

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**PREÂMBULO**

O Estado de Pernambuco, por intermédio da **SECRETARIA DE ADMINISTRAÇÃO**, através do Agente de Contratação/Pregoeira AC 10, Maria Fernanda de Carvalho Nunes, designada por meio da Portaria nº 4.061, publicada no Diário Oficial do Estado de Pernambuco, edição do dia 31/12/2024, torna público, para conhecimento dos interessados, em atendimento ao Documento de Abertura de Processo Licitatório do Secretário Executivo de Administração e Patrimônio, com a respectiva autorização, a abertura da licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL/POR LOTE**, a ser realizado por meio da utilização de recursos de tecnologia da informação – *Internet*, de acordo com a Lei Federal nº 14.133/21, a Lei Complementar nº 123/06 e o Decreto Estadual nº 54.142/2022 e respectivas alterações, aplicando-se subsidiariamente as demais normas regulamentares aplicáveis à espécie.

**1. DO OBJETO**

**1.1.** A presente licitação tem como objeto a prestação de serviços de rede corporativa segura com acesso à Internet, envolvendo implantação, operacionalização e melhoria contínua de serviços de acesso à Internet, conectividade de rede local e datacenter, voz, comunicação unificada, contact center, segurança e operação integrada de redes de computadores, visando atender as necessidades dos órgãos da Administração Direta, Indireta, Fundos Especiais, Autarquias e Fundações Públicas integrantes do Poder Executivo do Estado de Pernambuco, conforme especificações e quantitativos previstos no Termo de Referência (Anexo I).

**1.2.** O objeto desta licitação será dividido em lotes, conforme tabela constante do Termo de Referência (Anexo I), facultando-se à licitante a participação em quantos lotes forem de seu interesse.

**2. DA DESPESA E DOS RECURSOS ORÇAMENTÁRIOS**

2.1. A despesa total com a execução do objeto desta licitação é estimada **em R\$ 1.256.840.552,76 (um bilhão, duzentos e cinquenta e seis milhões, oitocentos e quarenta mil, quinhentos e cinquenta e dois reais e setenta e seis centavos)**, para os 48 meses, distribuídos em **lotes**, na forma indicada no Termo de Referência.

2.2. As despesas decorrentes desta licitação estão incluídas no orçamento do Estado de Pernambuco, para o presente exercício, e correrão por conta dos Órgãos ou Entidades (Órgãos Aderentes) que aderirem ao Contrato de Prestação de Serviços (Contrato-Mater) cujos Programas de Trabalho e Elementos de Despesas constarão nos respectivos termos de adesão e notas de empenho, observadas as condições estabelecidas no Edital, a saber:

2.2.1. As despesas decorrentes da instalação e operacionalização do Serviço Nova Rede Corporativa SEGURANÇA & CONECTIVIDADE, serão suportadas pelas DOTAÇÕES ORÇAMENTÁRIAS dos órgãos e entidades do Poder Executivo Estadual, no Elemento 3.3.90.39: Serviços de Terceiros – Pessoas Jurídicas, no elemento 3.3.90.39.27 para despesas relativas aos serviços despesas consumo de infraestrutura da rede, internet corporativa, serviço de operação, acesso dedicado; ou à conta das disponibilidades orçamentárias e financeiras das entidades que não dependem do Tesouro Estadual.

### 3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal ([www.gov.br/compras](http://www.gov.br/compras)).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

3.1.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

**3.2.** É obrigação do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. A não observância dessa obrigação poderá ensejar desclassificação no momento da habilitação.

**3.3** A participação no processo licitatório implica na aceitação, pelo licitante, do seu cadastro também no sistema PE-INTEGRADO, para fins de integração do Compras.gov.br com os sistemas utilizados pelo Poder Executivo Estadual.

**3.4.** Não poderão participar desta licitação:

**3.4.1.** Pessoa física ou jurídica impedida de licitar e contratar com a Administração Direta e Indireta do Estado de Pernambuco, nos termos do art. 156, III e § 4º, da Lei nº 14.133/2021, e do art. 7º da Lei Federal nº 10.520, de 17 de julho de 2002, durante o prazo da sanção aplicada ou até que seja promovida sua reabilitação;

**3.4.2.** Pessoa física ou jurídica suspensa temporariamente de participar em licitação e impedimento de contratar com a Administração, nos termos do art. 87, III, da Lei federal nº 8.666, de 1993;

**3.4.3.** Pessoa física ou jurídica declarada inidônea para licitar ou contratar com toda a Administração Pública, nos termos do art. 156, IV e §5º, da Lei 14.133/2021, e do art. 87, IV, da Lei Federal nº 8.666, de 1993, durante o prazo da sanção aplicada ou até que seja promovida sua reabilitação;

**3.4.4.** Pessoa física ou jurídica que tenha sido proibida de contratar com o Poder Público em razão de condenação por ato de improbidade administrativa, nos termos do artigo 12 da Lei Federal nº 8.429/1992;

**3.4.5.** Licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante;

**3.4.6.** Pessoa física ou jurídica enquadrada nas vedações previstas no art. 14 da Lei nº 14.133/21;

**3.4.7.** Pessoa jurídica cujo ramo de atividade previsto em estatuto ou contrato social não seja pertinente e compatível com o objeto desta licitação;

**3.4.8.** Agente público do órgão ou entidade licitante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133, de 2021;

**3.4.9.** Empresas sob a forma de consórcio para o LOTE 3, conforme previsto no item 2.6 do Termo de Referência (Anexo I);

**3.4.10.** Profissionais organizados em cooperativa, conforme previsto no item 2.7 do Termo de Referência (Anexo I do edital); e,

**3.4.11.** Pessoas físicas, conforme previsto no item 2.8 do Termo de Referência (Anexo I do edital).

## 4. DO CONSÓRCIO

**4.1.** Será permitida a participação de empresas reunidas em consórcio, atendidas as condições previstas no art. 15 da Lei nº 14.133/21 e no presente Edital, para os LOTES 1 e 2:

**4.2.** A apresentação do Termo de Compromisso público ou particular de constituição de Consórcio, subscrito pelas consorciadas, deverá prever:

**4.2.1.** Indicação da empresa líder, que será responsável pela representação do consórcio perante a Administração;

**4.2.2.** Declaração expressa de responsabilidade solidária, ativa e passiva, das consorciadas pelos atos praticados pelo consórcio, tanto na fase de licitação quanto na de execução do contrato;

**4.2.3.** Compromisso de que o consórcio não terá a sua composição ou constituição alterada até o final da execução do contrato, sem prévia e expressa anuência do contratante, ficando a substituição de consorciado condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos

valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do consórcio no processo licitatório que originou o contrato;

**4.2.4.** Compromisso de que o prazo de duração do consórcio deverá ser igual ou maior do que o prazo de vigência da contratação decorrente desta licitação;

**4.2.5.** Compromisso expresso de que o consórcio não se constitui, nem se constituirá, em pessoa jurídica distinta da de seus membros, bem como não terá denominação própria ou diferente das suas consorciadas;

**4.2.6.** Obrigações de cada uma das consorciadas, individualmente, bem como o percentual de participação de cada uma em relação ao serviço previsto.

**4.3.** A empresa consorciada fica impedida de participar isoladamente desta licitação, assim como de integrar mais de um consórcio.

**4.4.** O licitante vencedor é obrigado a promover, antes da celebração do contrato, a constituição e o registro do consórcio, nos termos do compromisso referido no item 4.2.

**4.5.** O consórcio deverá reunir, no máximo, 05 (cinco) empresas consorciadas, para o LOTE 1.

**4.6.** O consórcio deverá reunir, no máximo, 03 (três) empresas consorciadas, para o LOTE 2.

## 5. DA REFERÊNCIA DE TEMPO

**5.1.** Todas as referências de tempo previstas neste Edital, no Aviso e durante a sessão pública observarão obrigatoriamente o horário de Brasília – DF.

**5.2.** As sessões serão iniciadas em dias úteis.

**5.2.1.** Serão considerados como dias não úteis os sábados, domingos, feriados nacionais, estaduais e demais feriados e pontos facultativos publicados em Diário Oficial que influam no horário de funcionamento do órgão licitante.

**5.2.2.** Sessões já iniciadas poderão ser suspensas, cabendo ao Pregoeiro informar, através do Sistema, a data e horário para retomada do pregão.

**5.2.3.** Os prazos para encaminhamento da proposta e dos documentos de habilitação digitalizados serão computados em horas corridas.

**5.2.4.** Em caso de suspensão, quando da retomada da sessão, os prazos concedidos serão restituídos por tempo igual ao que faltava para sua complementação.

**5.3.** Havendo calamidade pública, fato relevante devidamente justificado ou necessidade de adequação de horário por motivos de administração interna, os horários previstos no item 5.2 poderão ser alterados, cabendo ao Pregoeiro informar previamente às licitantes a alteração e a nova data e horário para retomada do pregão, através do Sistema Compras.gov.

## 6. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

**6.1.** Qualquer pessoa é parte legítima para apresentar pedido de esclarecimento ou impugnar este Edital, devendo protocolar o pedido, por meio do e-mail indicado na folha de rosto anexa a este Edital, em até 3 (três) dias úteis antes da data fixada para a abertura da sessão pública.

**6.2.** As respostas aos pedidos de esclarecimento ou às impugnações vincularão os participantes e a Administração e serão divulgadas no Sistema pelo Pregoeiro no prazo de até 05 (cinco) dias úteis, limitado ao último dia útil anterior à data de abertura do certame.

**6.3.** A impugnação não possui efeito suspensivo, exceto em situações excepcionais devidamente motivadas pelo Pregoeiro.

**6.4.** Acolhida a impugnação, será republicado o Edital com as mesmas formalidades de sua publicação original e, conforme o caso, será definida nova data para realização do certame.

**6.5.** Não serão conhecidas impugnações apresentadas intempestivamente ou em desacordo com as regras estabelecidas neste Edital.

## 7. DA APRESENTAÇÃO DA PROPOSTA INICIAL

**7.1.** Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

**7.2.** No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

**7.2.1.** está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

**7.2.2.** não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

**7.2.3.** não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

**7.2.4.** cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

**7.3.** A licitante enquadrada Microempresa – ME, Empresa de Pequeno Porte – EPP Microempreendedor Individual (MEI) deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos nos artigos 3º e 18 -A da Lei Complementar nº 123, de 2006, e os requisitos de habilitação deste edital, mesmo que tenha restrição na documentação comprobatória da regularidade fiscal e trabalhista estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

**7.3.1.** nos itens exclusivos à participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

**7.3.2.** nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

**7.4.** A falsidade da declaração de que trata os itens 7.2 ou 7.3 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

**7.5.** Os licitantes poderão retirar ou substituir a proposta anteriormente inseridos no sistema, até a abertura da sessão pública.

**7.6.** Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

**7.7.** Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

**7.8.** Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

**7.8.1.** a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

**7.8.2.** os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

**7.9.** O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

**7.9.1.** valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e,

**7.9.2.** percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

**7.10.** O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 7.9 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

**7.11.** Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

**7.12.** O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

## 8. DA ABERTURA E DO PROCESSAMENTO DA LICITAÇÃO

**8.1.** A licitação será realizada em sessão pública, por meio da Internet, mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

**8.2.** Durante a sessão pública, a comunicação entre o Pregoeiro e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

**8.3.** Cabe à licitante acompanhar as operações no sistema eletrônico durante a sessão pública da licitação, ficando responsável por eventuais ônus decorrentes da perda de negócios causada pela inobservância de qualquer mensagem emitida pelo sistema ou por motivo de desconexão.

**8.4.** A abertura da sessão pública ocorrerá na data e horário indicados na folha de rosto anexa a este Edital, com a divulgação das propostas de preços recebidas, na forma prevista neste instrumento convocatório.

**8.5.** O Pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital.

**8.5.1.** O Pregoeiro poderá suspender a sessão pública para a análise dos documentos relativos às garantias de proposta apresentadas pelas licitantes.

**8.6.** Será desclassificada a proposta que contenha elementos que permitam a sua identificação.

**8.7.** A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

**8.8.** Somente as licitantes com propostas classificadas participarão da fase de lances.

## 9. DA FASE DE LANCES

**9.1.** Aberta a etapa competitiva, os representantes das licitantes classificadas deverão estar conectados ao sistema eletrônico e poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico.

**9.1.1.** O lance deverá ser ofertado pelo valor unitário total do item.

**9.1.2.** Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

**9.1.3.** O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,01% (zero vírgula zero um por cento), conforme previsto na Portaria SAD nº 2.293/2025.

**9.1.4** O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

**9.2.** Caso a licitante não apresente lances, concorrerá com o valor de sua proposta.

**9.3.** O sistema eletrônico não identificará o autor dos lances aos demais participantes.

**9.4.** A licitante somente poderá oferecer lance de valor inferior ao último por ela ofertado e registrado no sistema.

**9.5.** Durante o transcurso da sessão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado.

**9.6.** Não serão aceitos, durante a fase da disputa aberta, dois ou mais lances iguais provenientes de licitantes distintas, prevalecendo aquele que for recebido e registrado primeiro.

**9.7.** Salvo se houver evidente erro material, não poderá haver desistência dos lances ofertados, sujeitando-se a licitante desistente às penalidades estabelecidas neste Edital.

**9.8.** Durante a fase de lances, o Pregoeiro poderá, justificadamente e mediante comunicação via sistema, excluir lance oriundo de evidente erro material alegado pela respectiva licitante ou lance que possa comprometer, restringir ou frustrar o caráter competitivo do certame, implicando, nesta última hipótese, exclusão da licitante da disputa.

**9.9.** Se ocorrer a desconexão do Pregoeiro no decorrer da etapa de lances, e o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

**9.10.** No caso de a desconexão do Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa e terá reinício somente após comunicação expressa aos participantes no endereço [www.gov.br/compras](http://www.gov.br/compras), salvo na situação prevista no item 9.9.

**9.10.1.** Na situação acima, o reinício deve acontecer no turno seguinte ao da sessão suspensa, salvo em caso de impossibilidade, hipótese na qual a comunicação aos participantes deve ocorrer com antecedência mínima de 24 (vinte e quatro) horas.

**9.11.** O procedimento da etapa de lances seguirá de acordo com o modo de disputa aberto, conforme Termo de Referência.

**9.12.** A etapa de lances públicos e sucessivos terá duração de 10 (dez) minutos e, após esse prazo, será prorrogada automaticamente pelo sistema se houver oferta de lance nos últimos 02 (dois) minutos do período de duração.

**9.12.1.** A prorrogação automática de que trata o item 9.12 será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

**9.13.** Na hipótese de não haver novos lances na forma prevista nos itens 9.12.1, a sessão pública será encerrada automaticamente e o sistema ordenará e divulgará os lances em ordem crescente de classificação.

**9.14.** Definido o melhor lance, se a diferença em relação ao lance classificado em segundo lugar for de pelo menos 5%, o Pregoeiro poderá admitir, por uma única vez, o reinício da disputa aberta, para a definição das demais colocações.

**9.15.** Após o reinício previsto no item acima, as licitantes serão convocadas para apresentar lances intermediários, podendo optar por manter o seu último lance, ou por ofertar lance de valor inferior ou percentual de desconto superior.

**9.16.** Encerrada a etapa de que trata o item 9.15, o sistema ordenará e divulgará os lances em ordem crescente de vantajosidade, que se dará, conforme o critério de julgamento de **MENOR PREÇO GLOBAL POR LOTE**

## 10. DOS CRITÉRIOS DE DESEMPATE

**10.1.** Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, se houver, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

**10.1.1.** Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

**10.1.2.** A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

**10.1.3.** Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

**10.1.4.** No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

**10.2.** Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

**10.2.1.** Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

**10.2.1.1.** disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

**10.2.1.2.** avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei, conforme regulamento;

**10.2.1.3.** desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

**10.2.1.4.** desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

**10.2.2.** Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

**10.2.2.1.** empresas estabelecidas no território do Estado de Pernambuco;

**10.2.2.2.** empresas brasileiras;

**10.2.2.3.** empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

**10.2.2.4.** empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

**10.2.3.** Persistindo o empate, caso as regras previstas nos itens acima não solucionem o desempate, será realizado sorteio em sessão pública.

## 11. DA NEGOCIAÇÃO

**11.1.** Após o encerramento da fase de disputa, o Pregoeiro deverá negociar os preços apresentados pelas licitantes, podendo encaminhar contraproposta diretamente àquela que tenha apresentado o lance mais vantajoso, observado o critério de julgamento e o valor máximo estimado para a contratação.

**11.2.** A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelas demais licitantes.

**11.2.1.** O resultado da negociação será registrado na ata da sessão pública e divulgado a todos os licitantes.

**11.3.** Se, após a negociação, a licitante classificada provisoriamente em primeiro lugar não oferecer proposta compatível com o valor máximo do orçamento estimado, será desclassificada da licitação, sem prejuízo da aplicação da penalidade cabível.

**11.3.1.** Na hipótese acima, se a licitante, mesmo após a negociação, não oferecer proposta compatível com o orçamento estimado, será desclassificada da licitação, sem a aplicação de penalidade.

**11.4.** Os preços finais, unitários e totais, propostos pelos licitantes não poderão ultrapassar o preço unitário e global estimado pela Administração, sob pena de desclassificação da proposta.

**11.4.1.** No critério de julgamento pelo maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar o valor máximo do orçamento estimado.

**11.5.** No caso previsto no item 11.3, o Pregoeiro buscará negociar com as licitantes subsequentes, na ordem de classificação, buscando obter proposta com valor, no mínimo, igual ao previsto no orçamento estimado.

**11.6.** O sistema eletrônico informará a proposta de menor preço ou maior desconto imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação promovida pelo Pregoeiro.

## **12. DA CONVOCAÇÃO DA LICITANTE CLASSIFICADA PROVISORIAMENTE EM PRIMEIRO LUGAR**

**12.1.** Após a negociação e antes da convocação da licitante para apresentar a proposta adequada ao último lance, o Pregoeiro verificará se ela se enquadra em uma das vedações previstas no item 3.4 deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame, mediante consulta ao e-fisco, PE-Integrado, Compras.Gov.Br, Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e Cadastro Nacional de Empresas Punidas (CNEP).

**12.1.1.** A inscrição da licitante no Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS e no Cadastro Nacional de Empresas Punidas - CNEP será impeditiva apenas nos casos em que o efeito da sanção apontada no referido cadastro representar óbice à participação em licitações e contratações do Estado de Pernambuco.

**12.1.2.** A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, nos termos do art.12 da Lei nº 8.429, de 1992.

**12.1.3.** Caso reste configurada a ocorrência de alguma das vedações elencadas no item 3.4 deste edital, será declarado o impedimento de sua participação na presente licitação, devendo o Pregoeiro repetir este procedimento, convocando as licitantes subsequentes, de acordo com a ordem de classificação.

**12.2.** A licitante classificada provisoriamente em primeiro lugar será convocada para apresentar a PROPOSTA DE PREÇO ADEQUADA AO ÚLTIMO LANCE, devidamente preenchida na forma do Modelo de Proposta de Preços (Anexo B do TR), bem como os DOCUMENTOS

EXIGIDOS PARA A HABILITAÇÃO DIGITALIZADOS, para fins de exame de aceitabilidade do preço e de sua habilitação.

**12.3.** Os documentos deverão ser incluídos no Sistema no prazo de 04 (quatro) horas corridas, contado a partir da convocação do Pregoeiro.

**12.4.** O prazo de que trata o item 12.3 poderá ser prorrogado por igual período, antes do término do prazo originalmente previsto, mediante solicitação da licitante ou de ofício, a critério do Pregoeiro.

**12.5.** Recomenda-se que as licitantes iniciem a sessão de abertura da licitação com todos os documentos necessários à classificação/habilitação previamente digitalizados.

**12.6.** A licitante responsabilizar-se-á pela documentação encaminhada, assumindo como verdadeiras suas propostas, declarações e atestados.

**12.7.** Os arquivos encaminhados deverão estar legíveis.

**12.8.** Caberá à licitante confirmar o recebimento pelo Pregoeiro dos documentos encaminhados pelo sistema, responsabilizando-se pelo ônus decorrente da perda de negócios causada pela inobservância de quaisquer mensagens emitidas pelo Pregoeiro no sistema.

**12.9.** A licitante que abandonar o certame, deixando de encaminhar a proposta e/ou documentos de habilitação DIGITALIZADOS, no todo ou em parte, no prazo previsto no item 12.3, será desclassificada ou inabilitada do certame, conforme o caso, e sujeitar-se-á às sanções previstas neste Edital.

**12.10.** A sessão será suspensa para aguardo da proposta de preços e dos documentos de habilitação, cabendo ao Pregoeiro informar, através do sistema eletrônico, a data e o horário para retomada da licitação e divulgação da aceitabilidade da proposta e do resultado da habilitação.

## 13. DA ANÁLISE DA PROPOSTA

**13.1.** O Pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor estimado e à compatibilidade do objeto com as especificações técnicas do edital.

**13.1.1.** O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Estado de Pernambuco ou de pessoas físicas ou jurídicas com a expertise necessária, contratados para este fim.

**13.2.** Eventuais falhas formais ou materiais da proposta, como erros no preenchimento da planilha ou outros que não impedem a caracterização do objeto e a prestação dos serviços nos termos desta licitação, não constituem motivo para a desclassificação da proposta e deverão ser corrigidos pela licitante.

**13.2.1.** Os ajustes da proposta não poderão implicar alteração de sua substância nem aumento do seu valor global.

**13.2.2.** Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

**13.2.3.** O Pregoeiro poderá fixar prazo para o reenvio do anexo contendo a proposta ajustada quando o preço total ofertado for aceitável, mas os preços unitários que o compõem necessitem de ajustes para adequação aos valores estimados.

**13.2.4.** No caso de discrepância entre valores grafados em algarismos e por extenso, prevalecerá o valor por extenso

**13.2.5.** No caso de erro de multiplicação do preço unitário pela quantidade correspondente, o produto será retificado, mantendo-se inalterados o preço unitário e a quantidade.

**13.2.6.** No caso de erro de somatório, a adição será retificada, mantendo-se inalteradas as parcelas.

**13.2.7.** No caso de erros de transcrição das quantidades previstas para os serviços, o produto será corrigido devidamente, mantendo-se o preço unitário e se corrigindo a quantidade e o preço total.

**13.3.** Na análise da proposta não se considerará qualquer oferta de vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido.

**13.4.** Serão desclassificadas as propostas que:

- a) não obedeçam às especificações técnicas previstas neste Edital;
- b) permaneçam com valores unitários ou global superiores aos estimados, após a negociação de que trata o item 11;
- c) contenham preços manifestamente inexequíveis ou não tenham sua exequibilidade demonstrada, quando exigido pela Administração;
- d) apresentem vício ou desconformidade insanável com quaisquer outras exigências deste Edital;
- e) contenham falhas, apontadas pelo Pregoeiro, não corrigidas nem justificadas, mesmo após a oportunidade de saneamento de que trata o item 16 deste Edital;
- f) apresentem valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

**13.5.** Considerar-se-á indício de inexequibilidade de proposta valores inferiores a 50% do valor estimado para contratação.

**13.5.1.** Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, o Pregoeiro deverá, por meio de diligência, conferir à licitante a oportunidade de demonstrar a exequibilidade da sua proposta.

**13.5.2.** A inexequibilidade só ficará comprovada quando, cumulativamente, o custo da licitante ultrapassar o valor da proposta e inexistirem custos de oportunidade capazes de justificar o valor proposto.

**13.5.3.** A análise de exequibilidade da proposta não considerará materiais e instalações a serem fornecidos pela licitante em relação aos quais conste da proposta renúncia expressa à parcela ou à totalidade da remuneração.

**13.6.** Não se admitirá proposta que não observe a desoneração do ICMS quando se tratar de hipótese enquadrada na isenção prevista no Decreto Estadual nº 44.650/17 (Convênio ICMS 73/04).

**13.7.** Na proposta, não poderão ser incluídos pagamentos antecipados de quaisquer etapas ou serviços.

**13.8.** Se a proposta da licitante provisoriamente classificada em primeiro lugar não for aceita, o Pregoeiro retomará a sessão pública para convocar as licitantes subsequentes, obedecida a ordem de classificação, a fim de apresentarem proposta de preços e documentos de habilitação, no mesmo prazo e condições do item 12.3, e realizarem a negociação de que trata o item 11, até a apuração de uma que atenda às condições editalícias.

**13.9.** Quando todas as licitantes forem desclassificadas, o Pregoeiro poderá fixar o prazo de 8 (oito) dias úteis para a apresentação de novas propostas escoimadas das causas de desclassificação.

**13.10.** Classificada a proposta, o Pregoeiro dará início à fase de habilitação da licitante classificada em primeiro lugar, mediante a verificação da documentação exigida neste Edital.

**13.11.** Conforme item 5.2.2 do Termo de Referência (Anexo I do edital), a proposta comercial deverá estar acompanhada de:

**13.11.1.** Folders, catálogos e/ou prospectos técnicos dos produtos propostos, em português ou inglês, para fins de verificação da compatibilidade da solução apresentada com as especificações técnicas estabelecidas no Edital;

**13.11.2.** Documento contendo o detalhamento dos custos e a especificação dos produtos, softwares e serviços propostos - com os itens que compõem os lotes, fabricantes, modelos e códigos dos produtos - apresentando a matriz cruzada, quando couber, entre as especificações exigidas no termo de referência e a indicação da página do documento, folder, catálogo e/ou prospecto do fabricante onde se verifica a comprovação do atendimento; e,

**13.11.3.** A não apresentação dos documentos referidos nos itens 13.11.1 e 13.11.2 será causa de desclassificação da proposta do licitante, se não houver o saneamento hábil em sede de diligência.

**13.12. Do detalhamento dos itens de serviços da proposta:**

**13.12.1.** A Licitante, quando declarada vencedora provisória em seu lote, deverá apresentar o detalhamento dos itens de serviços, contendo todos os recursos necessários à prestação dos serviços, bem como as marcas, modelos, topologias e fornecedores das soluções (hardware e software) indicados na Proposta, de forma a atender integralmente aos requisitos obrigatórios e às especificações detalhadas deste Termo de Referência;

**13.12.2.** Para os itens de serviços indicados explicitamente na seção 5.2.3.1.6 do Termo de Referência (Anexo I do Edital), deverá ser apresentada uma Matriz Cruzada. Esta matriz demonstrará a correspondência detalhada entre cada requisito exigido neste Termo de Referência (seja de hardware, software ou serviço) e sua respectiva comprovação em documentação oficial do fabricante/fornecedor (como manuais, catálogos, páginas da internet, entre outros).

**13.12.3.** A matriz cruzada deverá ser apresentada em formato de tabela, estabelecendo referência direta entre cada requisito do Termo de Referência e a forma de atendimento pela solução proposta, contendo, no mínimo, os seguintes campos:

**13.12.3.1.** Item do TR

**13.12.3.2.** Especificação Exigida

**13.12.3.3.** Produto/Serviço

**13.12.3.4.** Fabricante/Modelo

**13.12.3.5.** Página de Referência no Documento

**13.12.3.6.** Empresa responsável pelo atendimento

**13.12.4.** Para fins de comprovação técnica, somente serão aceitos documentos oficiais do fabricante/fornecedor, publicados em seu domínio institucional e acessíveis a partir das páginas oficiais do produto ou do repositório oficial de documentação do fabricante.

**13.12.5.** Não serão aceitos datasheets obtidos por links diretos não referenciados nas páginas oficiais do fabricante (links órfãos), URLs temporárias, arquivos enviados por e-mail ou hospedados fora do domínio institucional do fabricante/fornecedor, ainda que contenham marca/identidade visual do fabricante.

**13.12.6.** Havendo duas ou mais versões de datasheets oficial para o mesmo produto/modelo, com valores de desempenho ou funcionalidades divergentes, prevalecerão, para fins de julgamento, os valores mais restritivos (menores) e o menor escopo funcional dentre as versões encontradas, salvo se for comprovado que a versão mais restritiva seja uma versão descontinuada.

**13.12.7.** Os itens da tabela da matriz cruzada deverão estar diretamente vinculados a cada serviço, conforme os itens e subitens correspondentes do Termo de Referência. O detalhamento da Proposta, em cada lote, deverá descrever claramente a solução adotada para:

**13.12.7.1. Lote 01**

**13.12.7.1.1.** ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO - Apresentar matriz cruzada para todos os serviços e recursos integrantes do Centro Integrado de Inteligência e Segurança Cibernética, com exceção do Serviço de disponibilização de ambiente de testes;

**13.12.7.1.2.** ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC) - Apresentar matriz cruzada para o Serviço de Comunicação Unificada;

**13.12.7.1.3.** ADENDO IV - SERVIÇO DE REDE SEM FIO - Apresentar matriz cruzada para os Serviços de Rede Sem Fio;

**13.12.7.1.4.** ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE - Apresentar matriz cruzada para os Serviços de Pontos de Voz Fixos e demais serviços e recursos integrantes desta solução, com exceção dos serviços de tráfego de voz e Serviço Adicional de Acesso SIP (SIP TRUNK);

**13.12.7.1.5.** ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER - Apresentar matriz cruzada para o serviço de Infraestrutura para Contact Center, com exceção dos serviços de Automatizações e Integrações - Consultoria Inicial e Implantação;

**13.12.7.1.6.** ADENDO III - SEGURANÇA DE REDE LOCAL - Apresentar matriz cruzada para o serviço de segurança de rede local;

**13.12.7.1.7. ADENDO VI - SEGURANÇA DE DATACENTER** - Apresentar matriz cruzada para o serviço de segurança de datacenter;

**13.12.7.1.8. A CONTRATADA** deverá apresentar desenho das soluções do ADENDO VI - SEGURANÇA DE DATACENTER, do ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO e ADENDO XI - INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM, mostrando sua integração, incluindo alta disponibilidade, para melhor visualização da proposta técnica da CONTRATADA, com indicação de correlação entre a solução apresentada na proposta (por meio de documentação oficial do fabricante) com os itens dos requisitos do Edital.

#### **13.12.7.2. Lote 02**

**13.12.7.2.1.** Apresentar topologia para os Links de Trânsito;

**13.12.7.2.2.** Apresentar matriz cruzada do serviço de proteção antiDDoS.

**13.12.7.2.3.** Deverá obrigatoriamente ser apresentada no detalhamento dos itens de serviços da Proposta Declaração da(s) licitante(s) informando o país/região/estado de seu mitigador (AntiDDoS), devendo esta localização atender às exigências da lei 12.965 de 23/04/2014 e regulamentada pelo decreto 8.771 de 11/05/2016;

## **14. DOS DOCUMENTOS DE HABILITAÇÃO**

**14.1.** A licitante classificada provisoriamente em primeiro lugar deverá apresentar os seguintes documentos, nos termos e prazo previstos neste Edital:

### **14.2. Habilitação Jurídica:**

**14.2.1.** Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

**14.2.2.** Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>.

**14.2.3.** Sociedade empresária, sociedade limitada unipessoal - SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo,

estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores.

**14.2.4.** Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

**14.2.4.1.** Sociedades estrangeiras que não funcionem no País devem apresentar documentos de habilitação equivalentes, na forma de regulamento emitido pelo Poder Executivo Federal, inicialmente em tradução livre.

**14.2.5.** Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores.

**14.2.6.** Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

**14.2.7.** Para os LOTES 1 e 2, Termo de autorização expedido pela Agência Nacional de Telecomunicações (Anatel) para explorar o Serviço de Comunicação Multimídia - SCM, conforme estabelecido no Regulamento do Serviço de Comunicação Multimídia, conforme Resolução Anatel nº 777, de 28 de abril de 2025, com direito/Delegação/Autorização/Concessão/ outorga de operação em Pernambuco.

**14.2.8.** Para os LOTES 1 e 2, no caso de formação de consórcio, as consorciadas que fornecerão os serviços de Conectividade deverão apresentar o Termo de autorização expedido pela Agência Nacional de Telecomunicações (Anatel) para explorar o Serviço de Comunicação Multimídia - SCM, conforme estabelecido no Regulamento do Serviço de Comunicação Multimídia, conforme Resolução Anatel nº 777, de 28 de abril de 2025.

**14.2.9.** Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

### **14.3. Regularidade Fiscal, Social e Trabalhista:**

**14.3.1.** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

**14.3.2.** Prova de regularidade fiscal perante a Fazenda Nacional, através da Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND), expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, ou Certidão Positiva com Efeitos de Negativa;

**14.3.3.** Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço – FGTS, comprovada através de apresentação de certidão fornecida pela Caixa Econômica Federal;

**14.3.4.** Prova de inscrição no Cadastro de Contribuintes Estadual relativo ao domicílio da licitante;

**14.3.5.** O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

**14.3.6.** Prova de regularidade para com a Fazenda Estadual do Estado de Pernambuco, mediante apresentação de Certidão de Regularidade Fiscal (CRF) emitida pela Secretaria da Fazenda do Estado (SEFAZ/PE).

**14.3.7.** Prova de regularidade para com a Fazenda Estadual, mediante apresentação de Certidão de Regularidade Fiscal (CRF) emitida pela Secretaria da Fazenda do domicílio do estabelecimento executor do contrato.

**14.3.8.** Prova de regularidade perante a Justiça do Trabalho, através de Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva com efeitos de Negativa, de acordo com a Lei nº 12.440/2011 e Resolução Administrativa nº 1.470/2011 do TST.

**14.3.9.** As microempresas, as empresas de pequeno porte e o Microempreendedor Individual (MEI) deverão apresentar toda a documentação exigida para fins de regularidade fiscal e trabalhista, mesmo que apresente alguma restrição, sendo a comprovação efetiva exigível

somente para efeito de contratação, nos termos dos arts. 42 e 43 da LC 123, de 2006 e art. 4º do Decreto Federal 8.538, de 2015.

**14.3.10.** Havendo alguma restrição na comprovação da regularidade fiscal ou trabalhista da Microempresa, da Empresa de Pequeno Porte ou do Microempreendedor Individual, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada vencedora do certame, prorrogável por igual período, a critério da administração, para regularização da documentação, para pagamento ou parcelamento do débito e para emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

**14.3.11.** A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital.

**14.3.12.** Caso a licitante esteja em recuperação judicial, estará dispensada da apresentação dos documentos de regularidade fiscal, social e trabalhista, com exceção da certidão de regularidade perante a Previdência Social, nos termos do artigo 52, inciso II, da Lei Federal nº 11.101/2005.

**14.3.12.1.** Para os fins do disposto no item acima, a licitante deverá apresentar decisão judicial em vigor que autorize o processamento do pedido de recuperação e dispense expressamente as certidões negativas, e comprovar que o respectivo plano de recuperação ainda não foi aprovado e homologado em Juízo.

**14.3.12.2.** Caso a licitante em recuperação judicial já tenha tido seu plano aprovado e homologado em juízo até a data de abertura da fase de habilitação do certame, a dispensa prevista acima não subsiste e a licitante deverá apresentar todas as certidões de regularidade requeridas neste Edital.

#### **14.4. Qualificação Técnica:**

**14.4.1.** A LICITANTE deverá comprovar aptidão para execução de serviços de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, mediante apresentação de atestados ou certidões de capacidade técnica emitidos por pessoa(s) jurídicas de direito público ou privado ou, quando aplicável, regularmente

emitidos pelo conselho profissional competente, observadas as condições previstas no Termo de Referência.

**14.4.1.1.** Para fins de comprovação da qualificação técnica, serão aceitos atestados emitidos em nome da própria LICITANTE, das empresas integrantes de consórcio formalmente constituído para participação neste certame, quando aplicável, ou de potencial subcontratado, exclusivamente nas hipóteses, limites e condições expressamente previstos no Termo de Referência, nos termos do art. 67, §9º, da Lei nº 14.133/2021.

**14.4.1.2.** Não serão aceitos atestados emitidos em nome de empresas pertencentes ao mesmo grupo econômico que não integrem formalmente o consórcio participante da licitação, ressalvada a hipótese de apresentação de atestado de potencial subcontratado, quando expressamente admitida no Termo de Referência.

**14.4.1.3.** Para a confirmação de informações contidas no(s) atestado(s) apresentado(s), poderá ser promovido diligência no intuito de esclarecer/complementar a instrução do processo, solicitando e obtendo cópias de contratos e outros documentos idôneos.

**14.4.1.4.** Será admitida, nos termos do art. 67, §9º da Lei nº 14.133/2021, a apresentação de atestados relativos a potencial subcontratado em relação à parcela do serviço de até 25% (vinte e cinco por cento), cuja subcontratação foi expressamente autorizada no Termo de Referência.

**14.4.1.5.** A apresentação de atestados de potencial subcontratado implicará a obrigatoriedade de sua efetiva contratação para execução das parcelas correspondentes, sendo vedada sua substituição sem prévia anuência da CONTRATANTE, mediante justificativa técnica devidamente fundamentada e reapresentação dos atestados.

**14.4.1.6.** Para fins de comprovação, os atestados/certidões devem dizer respeito a prestação dos serviços correlatos a cada lote:

**14.4.1.6.1. LOTE 01 - prestação de serviços de CONECTIVIDADE E SEGURANÇA**

**14.4.1.6.1.1.** 38.175 (trinta e oito mil cento e setenta e cinco) eventos por segundo de capacidade mínima de monitoramento e análise de eventos de segurança em um ambiente operacional;

**14.4.1.6.1.2.** 1.221 (mil duzentos e vinte e um) gerenciamento de acessos à rede local (NAC);

**14.4.1.6.1.3.** 611 (seiscentos e onze) fornecimentos e implantações de Solução unificada de segurança de rede de última milha (UTM);

**14.4.1.6.1.4.** 2.513 (dois mil quinhentos e treze) pontos de voz (PVF);

**14.4.1.6.1.5.** 1.289 (mil duzentos e oitenta e nove) pontos de rede sem fio interno ou externo (SRSF);

**14.4.1.6.1.6.** 820 (oitocentos e vinte) circuitos com acesso do tipo banda larga, dedicado, satelital ou 5G FWA;

**14.4.1.6.1.7.** 3.750 (três mil setecentos e cinquenta) itens de Solução de gerenciamento e monitoramento de ativos.

#### **14.4.1.6.2 LOTE 2 - prestação de serviços de CONECTIVIDADE DE DATACENTER**

**14.4.1.6.2.1** A LICITANTE deverá comprovar o fornecimento do Serviço de Internet Corporativa + AntiDDoS de no mínimo 1 (um) Gbps de Banda, sendo permitido a soma de no máximo 02 (dois) links, correspondendo a 50% da banda inicial a ser contratada, comprovando que ambas as infraestruturas de backbone disponibilizadas pela licitante possuam interligação direta a no mínimo 2 (dois) Sistemas Autônomos (AS - Autonomous Systems) distintos, conforme norma da RFC1930;

**14.4.1.6.2.2.** A LICITANTE deverá comprovar que está conectada diretamente a pelo menos um provedor de serviços de trânsito IP Internacional: Entenda-se por Provedor de Serviços de Trânsito Internacional aquele que se acha fora dos limites da jurisdição territorial brasileiro. A comprovação de que a empresa está conectada a uma fornecedora Internacional será feita através das ferramentas públicas, como bgp.he.net ou outra similar;

#### **14.4.1.6.3 LOTE 3 - prestação de serviços de AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS**

**14.4.1.6.3.1** A contratada deverá comprovar experiência prévia na prestação de serviços de gestão de vulnerabilidades, incluindo identificação, análise, priorização e mitigação de vulnerabilidades em ambientes tecnológicos. A comprovação deve ser realizada por meio de atestados de capacidade técnica emitidos por clientes que comprove a execução de serviços compatíveis

em características com o objeto licitado, especialmente envolvendo ao menos 420 (quatrocentos e vinte) ativos de tecnologia da informação.

**14.4.1.6.3.2** A contratada deverá comprovar que possui qualificação técnica e experiência prévia na execução de **serviços de análise forense digital**, contemplando a identificação, coleta, preservação, análise e apresentação de evidências digitais. A experiência deverá ser comprovada mediante atestados que evidenciem a execução de serviços compatíveis em características com o objeto licitado com carga horária acumulada igual ou superior a 677 (seiscentos e setenta e sete) horas realizadas a partir de 01/01/2020.

**14.4.1.6.3.3** A contratada deverá comprovar experiência na realização de **serviços de testes de intrusão (Pentest)**, abrangendo a identificação e exploração de vulnerabilidades em redes, sistemas e aplicações, com emissão de relatórios detalhados dos riscos e recomendações. A comprovação deverá ser realizada por meio de atestados emitidos por clientes que demonstrem a execução de serviços compatíveis com o objeto licitado, abrangendo ao menos 24 (vinte e quatro) aplicações.

**14.4.1.7.** Será considerado compatível com a quantidade os atestados ou certidões que apresentarem, no mínimo os quantitativos e/ou percentuais das quantidades estimadas na licitação para cada lote, constantes nos subitens do 14.4.1., exigindo-se a comprovação cumulativa quando da classificação provisória em primeiro lugar em mais de um lote;

**14.4.1.8.** Para fins de aferição do percentual e/ou quantitativo mínimo relativo à qualificação técnica, em sendo obtido resultado cujo número possua casas decimais, deverá ser realizado arredondamento para o primeiro menor número inteiro.

**14.4.1.9.** Será admitido, para fins de comprovação do quantitativo mínimo, o somatório das quantidades descritas em um ou mais atestados apresentados.

**14.4.1.10.** Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

**14.4.1.11.** Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial da licitante.

**14.4.1.12.** Não serão aceitos atestados emitidos pela licitante, em seu próprio nome, nem qualquer outro em desacordo com as exigências do Edital.

**14.4.1.13.** A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

**14.4.2. Documentação Técnica exigida para cada Lote além dos atestados referenciados acima:**

**14.4.2.1. Para o LOTE 02:**

**14.4.2.1.1.** A LICITANTE deverá comprovar que o somatório das larguras de banda de seu backbone, considerando as conexões com Sistemas Autônomos (ASs) nacionais, resulta em capacidade mínima equivalente ao dobro da banda máxima a ser contratada, estabelecida em 20 (vinte) Gbps.

**14.4.3. A Capacitação Técnico-profissional consistirá em:**

**14.4.3.1. Para os LOTES 01 e 02**

**14.4.3.1.1.** A LICITANTE deverá indicar Responsável(eis) Técnico(s), em conformidade com o artigo 67 da Lei nº 14.133/2021, que permite a exigência de qualificação técnico-profissional para assegurar a capacidade técnica da licitante na execução contratual. Essa exigência também está respaldada pela Resolução nº 1.137/2023 do CONFEA, a qual estabelece a necessidade de vínculo direto entre o profissional e a empresa contratada para serviços técnicos especializados, garantindo o compromisso e a responsabilidade técnica necessários ao cumprimento do Termo de Referência.

**14.4.3.1.2. Para o LOTE 01,** o(s) Responsável(eis) técnico(s), pertencente(s) ao seu quadro permanente, na data prevista para entrega da proposta, incluindo suas qualificações, sendo exigido profissionais de nível superior, detentores de certidões de responsabilidade técnica de ser-

viços técnicos especializados para implementação da infraestrutura de telecomunicação para acesso à Internet (ARTs/CAT) com registro emitido pelo CREA.

**14.4.3.1.3. Para o LOTE 02**, o(s) profissional(is) indicados devem possuir nível superior ou outro devidamente reconhecido pela entidade competente, detentor(es) de atestados de responsabilidade técnica por execução de Serviços de Comunicação Multimídia (SCM) de características semelhantes ao objeto da licitação, devidamente acompanhados da respectiva Certidão de Acervo Técnico (CAT) com registro no CREA e/ou CFT.

**14.4.3.1.4.** A comprovação de vinculação do profissional ao quadro da licitante poderá ser efetuada, no caso de empregado da licitante, por meio da Carteira de Trabalho e Previdência Social; no caso de sócio, através do contrato/estatuto social; no caso de prestador de serviços, mediante contrato escrito firmado com o licitante ou declaração de compromisso do profissional de vinculação futura, caso o licitante se sagre vencedor do certame.

**14.4.3.1.5.** No decorrer do contrato os profissionais de que trata esse item poderão ser substituídos por profissionais equivalentes ou superiores desde que haja anuência prévia do contratante.

**14.4.4.** Conforme justificativas constantes na NOTA TÉCNICA - SAD - Comissão Técnica de Telemática - COMTEC - TELEMATICA - Nº 5/2025 (doc. SEI 67013492), uma mesma empresa, isolada ou em forma de consórcio, não poderá ser declarada vencedora do LOTE 01 e LOTE 03 cumulativamente.

**14.4.4.1.** Conforme item 5.3.3.1 do Termo de Referência (Anexo I do edital), caso a licitante seja classificada provisoriamente em primeiro lugar, **SIMULTANEAMENTE NOS LOTES 1 e 3**, caberá a Administração especificar, considerando a maior economia obtida em valores absolutos de cada lote, para o qual a licitante será habilitada.

**14.4.5.** Declaração emitida pela licitante atestando que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação, conforme Anexo III, assegurado o direito de realização de vistoria prévia, por solicitação da licitante, mediante agendamento, na forma prevista no Termo de Referência.

**14.4.5.1** Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

**14.4.5.2.** Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

**14.4.5.3.** Caso a licitante opte por não realizar a vistoria, deverá apresentar declaração formal assinada por seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação, conforme Anexo IV.

#### **14.5. Qualificação Econômico-Financeira:**

**14.5.1.** Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de sociedade simples.

**14.5.2.** Certidão Negativa de Falência, expedida pelo distribuidor ou distribuidores (caso exista mais de um) da sede ou domicílio da licitante.

**14.5.2.1.** Certidão Negativa de Falência referente aos processos distribuídos pelo PJe (processos judiciais eletrônicos) da sede ou domicílio da licitante.

**14.5.2.2.** A certidão descrita no item 14.5.2.1 somente é exigível quando a certidão negativa de Falência da sede ou do domicílio da licitante contiver a **ressalva expressa** de que não abrange os processos judiciais eletrônicos.

**14.5.2.3.** No caso de Certidão Positiva de Falência, a licitante será inabilitada, salvo se restar comprovado que não houve decisão judicial válida e eficaz decretando a falência da empresa.

**14.5.3.** Comprovação de Capital Social ou Patrimônio Líquido Mínimo correspondente a 10% (dez por cento) do valor anual estimado da licitação para o respectivo lote, exigindo-se a comprovação cumulativa quando da classificação provisória em primeiro lugar em mais de um lote.

**14.5.4.** Para fins de comprovação de Patrimônio Líquido e dos índices contábeis, o licitante deverá apresentar Balanço Patrimonial e demonstrações contábeis dos últimos 2 (dois) exercícios sociais, exigíveis e apresentados na forma da lei (incluindo o termo de abertura e termo de encerramento), devendo cumprir a qualificação em ambos os exercícios, salvo

quando a licitante tiver sido constituída há menos de 02 (dois) anos, hipótese na qual tais documentos limitar-se-ão ao último exercício financeiro.

**14.5.5.** Os balanços e demonstrações devem conter os registros ou autenticação no órgão competente e estar devidamente assinados pelo administrador da empresa e pelo profissional habilitado junto ao Conselho Regional de Contabilidade – CRC, e vir acompanhados dos termos de abertura e de encerramento.

**14.5.6.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura, conforme art. 65, §1º, da Lei nº 14.133, de 2021.

#### **14.6. Documentos complementares**

**14.6.1.** Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, de acordo com o modelo estabelecido no Anexo II deste Edital.

**14.6.2.** Declaração de cumprimento das exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, de acordo com o modelo estabelecido no Anexo II deste Edital.

**14.6.3.** Declaração de que não possui em seu quadro societário ou de pessoal agente público do órgão ou entidade licitante ou contratante, nos termos do art. 9º, §1º da Lei 14.133/2021, de acordo com o modelo estabelecido no Anexo II deste Edital.

**14.6.4.** Declaração de que não incorre em qualquer uma das vedações impostas no art. 14 da Lei 14.133/2021 aplicáveis ao objeto da presente licitação, de acordo com o modelo estabelecido no Anexo II deste Edital.

**14.6.5.** Declaração de que atende às disposições da Lei Geral de Proteção de Dados (LGPD), conforme determinação da Lei Estadual nº 18.671/2024, de acordo com o modelo estabelecido no Anexo II deste Edital.

#### **14.7. Das regras gerais relativas aos documentos de habilitação**

**14.7.1.** A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

**14.7.1.1.** Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

**14.7.1.2.** A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

**14.7.1.3.** É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

**14.7.1.4.** A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

**14.7.1.5.** A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

**14.7.1.6.** Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

**14.7.1.7.** Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados por meio do sistema, em formato digital, no prazo de 04 (quatro) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

**14.7.2.** Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

**14.7.3.** Quando da convocação da licitante para apresentação dos documentos de habilitação, a qualquer tempo, os documentos relativos à habilitação jurídica, à qualificação técnica e à qualificação econômico-financeira deverão remontar à data da sessão de abertura do certame, demonstrando-se que, à época da licitação, a licitante reunia as condições de habilitação.

**14.7.3.1.** Se os documentos indicados no item 14.7.3, na data da convocação, encontrarem-se com prazo de validade expirado, ou tenham sofrido alterações, devem ser também apresentados novos documentos que comprovem a manutenção das condições de habilitação;

**14.7.4.** Os documentos de regularidade fiscal, social e trabalhista, previstos no item 14.3, devem encontrar-se válidos na data da convocação.

**14.7.5.** Inexistindo preceito legal ou prazo de validade fixado no próprio instrumento, os documentos/certidões serão considerados válidos por um período de 90 (noventa) dias contados da sua emissão, exceto quando se tratar de Certidão Negativa de Falência, que terá validade de 180 (cento e oitenta) dias da sua expedição.

**14.7.5.1.** Caso haja previsão de prazo diverso em lei ou em norma infralegal municipal, de outros estados da federação ou internacional, a licitante ficará responsável por juntar a respectiva comprovação.

**14.7.6.** Não será aceito qualquer protocolo de entrega ou de solicitação de documentos em substituição aos documentos relacionados neste Edital.

**14.7.7.** A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo Certificado de Registro de Fornecedor emitido pelo CADFOR-PE, desde que os documentos contemplados estejam dentro do prazo de validade, ou pelo certificado de registro cadastral unificado disponível no Portal Nacional de Contratações Públicas - PNCP, nos termos do regulamento próprio.

**14.7.8.** Para fins de habilitação, a verificação dos documentos pelo Pregoeiro nos sítios oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

**14.7.9.** Caso a licitante não logre comprovar o atendimento cumulativo dos requisitos de qualificação técnica e econômico-financeira para todos os lotes/itens em que seja classificada provisoriamente em primeiro lugar, caberá a Administração especificar, considerando a maior economia obtida em valores absolutos de cada lote/item, os respectivos lotes/itens para os quais a licitante será habilitada.

**14.7.9.1.** Na hipótese de o certame ser homologado de forma parcial, correspondente a determinados lotes ou itens, a aplicação da regra prevista no subitem 14.7.9 restringir-se-á aos lotes ou itens abrangidos pela respectiva homologação. A escolha dos lotes ou itens para os quais a licitante será habilitada, com base na maior

economia obtida em valores absolutos, deverá ocorrer exclusivamente dentre aqueles incluídos na etapa de homologação em curso.

**14.7.10.** Em caso de participação de licitantes estrangeiras que não funcionem no país, as exigências de habilitação serão atendidas mediante a apresentação de documentos equivalentes, inicialmente apresentados em tradução livre.

**14.7.10.1.** Caso seja vencedora a licitante estrangeira que não funcione no país, será exigido, como condição para assinatura do contrato, que os documentos apresentados sejam traduzidos por tradutor juramentado e consularizados pelos respectivos consulados ou embaixadas.

**14.7.10.2.** A autenticação consular ou em embaixada será dispensada quando se tratar de documento público e o respectivo país for signatário da Convenção de Haia, sendo, neste caso, necessário apenas o apostilamento do documento em cartório, nos termos do disposto no Decreto Federal nº 8.660/2016.

**14.7.11.** Será inabilitada a licitante que apresentar declaração ou documentação falsa, que deixar de apresentar quaisquer documentos exigidos ou apresentá-los em desacordo com as exigências deste Edital, ressalvadas as restrições relativas à regularidade fiscal e trabalhista das Microempresas, Empresas de Pequeno Porte, Microempreendedores Individuais ou equiparadas, nos termos da Lei Complementar nº 123/2006, e o disposto no subitem 14.7.7.

**14.7.12.** Habilitada a licitante, o Pregoeiro encaminhará todos os documentos apresentados para fins de inscrição da licitante no CADFOR ou de atualização do respectivo registro cadastral, se já houver.

**14.7.12.1.** É obrigação da licitante conferir a exatidão dos seus dados cadastrais e manter atualizados os documentos em seu registro no CADFOR até a homologação do certame, sob pena de decair do direito à contratação.

**14.7.13.** Em caso de participação de empresas em consórcio nos LOTES 1 e 2, o Termo de Compromisso de que trata o item 4.2 deverá ser apresentado em conjunto com os documentos de habilitação, observadas as seguintes disposições:

**14.7.13.1.** Cada empresa consorciada deve apresentar os documentos exigidos nos itens 14.2 e 14.3 deste Edital, para fins de comprovar a habilitação jurídica e a regularidade fiscal, social e trabalhista;

**14.7.13.2.** A fim de comprovar a qualificação econômico-financeira, exige-se que cada consorciado apresente a Certidão Negativa de Falência, prevista no item 14.5.2, e comprove o atendimento aos índices contábeis fixados no item 14.5.4.

**14.7.13.3.** Para a prova da qualificação técnica, quando exigida, será admitido o somatório dos quantitativos dos atestados fornecidos por cada consorciado e, para efeito de habilitação econômico-financeira, quando exigido capital social ou patrimônio líquido mínimo, será observado o somatório dos valores de cada consorciado.

**14.7.13.4.** A qualificação econômico-financeira relativa ao Capital Social ou Patrimônio Líquido Mínimo terá um acréscimo de 10% (dez por cento) do valor exigido para o licitante individual.

**14.7.13.4.1.** O acréscimo previsto não será exigido se o consórcio for formado integralmente por microempresa ou empresas de pequeno porte.

## 15. DA DECLARAÇÃO DA LICITANTE VENCEDORA

**15.1.** Verificado o atendimento das exigências de habilitação fixadas neste Edital, a(s) licitante(s) será(ão) declarada(s) vencedora(s) em sessão pública.

**15.3.** Na hipótese de a licitante não atender às exigências de habilitação, o Pregoeiro retornará o processo à fase de negociação para exame das ofertas subsequente assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital de licitação.

**15.4.** Após análise de todas as propostas, na hipótese de não haver licitante classificada que atenda às exigências de habilitação, o Pregoeiro poderá conceder o prazo de 8 (oito) dias úteis para que as licitantes classificadas apresentem nova documentação escoimada das causas da inabilitação, observada a ordem de classificação.

## 16. DO SANEAMENTO DA PROPOSTA E DA HABILITAÇÃO

**16.1.** Durante as fases de julgamento e de habilitação, o Pregoeiro, mediante decisão fundamentada, poderá realizar diligências para sanear erros ou falhas que não alterem a substância das propostas e a validade jurídica dos documentos de habilitação, devendo registrá-las em ata acessível aos licitantes.

**16.2.** Fica vedada a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

- a) complementação de informações ou esclarecimentos adicionais acerca dos documentos já apresentados pelos licitantes;
- b) atualização de documentos cuja validade tenha expirado;
- c) comprovação de situação fática preexistente à época da abertura do certame.

**16.2.1.** Para os fins do disposto na alínea “c”, é lícita a juntada de certidão ou atestado não anexados à documentação originalmente apresentada, desde que tenham data anterior à abertura do certame ou se refiram inequivocamente a condição adquirida pelo licitante antes da abertura do certame.

**16.2.2.** Na falta de documentos de habilitação que consistam em mera declaração da licitante sobre fato preexistente ou em simples compromisso por ela firmado, poderá ser concedido prazo para saneamento da falha.

**16.3.** A realização de diligências não confere à licitante novo prazo ou oportunidade de obter condição ou requisito que antes não detinha, nem autoriza o Pregoeiro a fazer exigências novas não previstas no edital.

**16.4.** Na hipótese de necessidade de envio de documentos complementares à proposta e à habilitação, os documentos deverão ser apresentados em formato digital, via sistema, no prazo de 01 (um) dia útil.

**16.5.** Sendo necessária a suspensão da sessão pública para a realização de diligências, o reinício se dará mediante aviso prévio no sistema COMPRAS.GOV, com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

## 17. DOS RECURSOS ADMINISTRATIVOS

**17.1.** Após a declaração do(s) vencedor(es), qualquer licitante inconformada com o resultado poderá manifestar, ao final da sessão pública, a intenção de recorrer contra o julgamento das propostas ou a habilitação ou inabilitação de licitantes, através de campo próprio do sistema eletrônico, sendo-lhes então concedido o prazo de 03 (três) dias úteis para anexar no sistema eletrônico memoriais contendo as razões recursais.

**17.1.1.** A intenção de recorrer deverá ser registrada no sistema em **até 10 (dez) minutos** após a declaração do vencedor.

**17.1.2.** A falta de manifestação imediata da intenção recursal importará preclusão e a adjudicação do objeto à licitante vencedora.

**17.2.** Os demais interessados ficam, desde logo, intimados a apresentar contrarrazões no prazo de 03 (três) dias úteis, que começarão a correr após o término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

**17.3.** As razões do recurso e das contrarrazões deverão ser anexadas em campo próprio do sistema eletrônico.

**17.4.** O recurso terá efeito suspensivo até a decisão final da autoridade competente e o seu acolhimento importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

**17.5.** As razões do recurso serão dirigidas ao Pregoeiro, que, no prazo de 03 (três) dias úteis, poderá reconsiderar sua decisão ou, nesse mesmo prazo, encaminhar o recurso à autoridade superior, devidamente motivado, para decisão final no prazo máximo de 10 (dez) dias úteis.

**17.6.** A decisão dos recursos deverá ser divulgada no sistema Compras.gov.br.

**17.7.** Não serão conhecidos recursos apresentados em desacordo com as regras estabelecidas neste item ou fora do prazo e horário legal ou, ainda, subscritos por representante não habilitado legalmente ou não identificado no processo para responder pelo proponente.

**17.8.** Decididos os recursos, a autoridade competente fará a adjudicação do objeto da licitação à licitante vencedora.

**17.9.** Verificada a regularidade dos procedimentos, o Pregoeiro encaminhará o processo à autoridade competente para a homologação.

## 18. DO CONTRATO

**18.1.** A contratação decorrente desta licitação será formalizada mediante a assinatura de termo de contrato, conforme modelo constante do Anexo V.

**18.2.** Após a homologação da licitação, a adjudicatária será convocada para assinatura do termo de contrato no prazo de **10 dias úteis**, contados a partir da convocação, sob pena de decair o direito à contratação.

**18.2.1.** O prazo para assinatura do termo de contrato poderá ser prorrogado uma única vez, por igual período, mediante solicitação da adjudicatária e desde que ocorra motivo justo, aceito pelo contratante, e que seja formulada antes do decurso do prazo assinalado.

**18.2.2.** Se o instrumento de contrato não for assinado pelo representante legal do contratado, deverá ser apresentada procuração, devidamente reconhecida em cartório, com poderes que habilitem o mandatário a assinar o instrumento.

**18.2.3.** Aplicar-se-á o prazo mencionado no item 18.2 para as assinaturas dos termos aditivos ao Contrato Mater

**18.2.4.** Após a assinatura do Contrato Mater, a contratada deverá assinar os termos de adesão e seus aditivos no prazo de **5 (cinco) dias úteis**, a contar da convocação pela contratante.

**18.3.** Por ocasião da convocação para assinatura do contrato, a contratante deverá consultar a regularidade da adjudicatária no CADFOR, no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep).

**18.3.1.** Se houver pendência documental no CADFOR e não for possível atualizá-lo por meio por meio de consulta aos sítios eletrônicos oficiais, a adjudicatária será notificada para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das respectivas certidões vigentes, sob pena de decair do direito à contratação.

**18.4.** O não comparecimento injustificado da adjudicatária, a não apresentação dos documentos exigidos como requisito de contratação e a desatualização de seus documentos de habilitação

no CADFOR importará na recusa à contratação, sujeita à aplicação das penalidades previstas neste Edital e à perda da garantia da proposta, quando houver, nos termos do item 19.1.2.

**18.4.1** Na hipótese do item 18.4, a adjudicação poderá ser anulada e retomado o procedimento licitatório, a fim de que o Pregoeiro retorne à fase de negociação para exame das ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda ao edital de licitação e seja declarada uma nova adjudicatária.

**18.5.** Poderá ser acrescentada ao contrato vantagem apresentada pela licitante vencedora em sua proposta, desde que seja pertinente e compatível com os termos deste Edital, não represente quaisquer ônus para a Administração e a respectiva aceitação esteja devidamente fundamentada.

## 19. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

**19.1.** Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133, de 2021, a licitante ou a adjudicatária que:

**19.1.1.** convocada dentro do prazo de validade da proposta, não comparecer para assinar a Ata de Registro de Preços ou o instrumento contratual;

**19.1.2.** deixar de entregar documentação exigida durante a licitação ou para fins de assinatura da Ata ou do contrato, inclusive a garantia da proposta ou de execução contratual;

**19.1.3.** Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

**19.1.3.1.** não enviar a proposta adequada ao último lance ofertado ou após a negociação;

**19.1.3.2.** recusar-se a enviar o detalhamento da proposta quando exigível;

**19.1.3.3.** desistir dos lances ofertados, a menos que haja erro material reconhecido;

**19.1.3.4.** desistir da proposta após encerrada a etapa competitiva ou der causa à sua desclassificação ao não oferecer, mesmo após negociação, proposta compatível com o valor máximo do orçamento estimado;

**19.1.3.5.** apresentar proposta em desacordo com as especificações do edital.

**19.1.4.** apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

**19.1.5.** fraudar a licitação;

**19.1.6.** praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

**19.1.7.** comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

**19.1.7.1.** agir em conluio ou em desconformidade com a lei;

**19.1.7.2.** induzir deliberadamente a erro no julgamento.

**19.1.8.** cometer fraude de qualquer natureza;

**19.1.9.** praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;

**19.2.** As licitantes ou adjudicatárias que incorram em infrações sujeitam-se às seguintes sanções administrativas, sem prejuízo das responsabilidades civil e criminal:

**19.2.1.** Multa;

**19.2.2.** Impedimento de Licitar e Contratar com a Administração Direta e Indireta do Estado de Pernambuco, pelo prazo de até 03 (três) anos;

**19.2.3.** Declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 03 (três) e máximo de 06 (seis) anos.

**19.3.** As sanções previstas nos itens 19.2.2 e 19.2.3 poderão ser aplicadas cumulativamente com a multa.

**19.4.** A penalidade de multa será aplicada de acordo com as seguintes regras:

**19.4.1.** Multa de 1% (um por cento) a 5% (cinco por cento) sobre o valor estimado para o item/lote do qual participou, observado o valor mínimo de 10.000,00 (dez mil reais) e o máximo de R\$ 100.000,00 (cem mil reais), a ser aplicada a quem cometer a infração prevista no item 19.1.1 deste edital;

**19.4.2.** Multa de 0,5% (zero vírgula cinco por cento) até 1% (um por cento) sobre o valor total do item/lote do qual participou, observado o valor mínimo de R\$ 2.000,00 (dois mil reais) e máximo de R\$ 50.000,00 (cinquenta mil reais), a ser aplicada a quem cometer a infração prevista nos itens 19.1.2 e 19.1.3. deste edital;

**19.4.3.** Multa de 10% (dez por cento) até 30% (trinta por cento) sobre o valor estimado para o item/lote do qual participou nos casos das infrações previstas nos itens 19.1.4. 19.1.5., 19.1.6., 19.1.7, 19.1.8 e 19.1.9 deste edital.

**19.5.** Além da multa, aplicada conforme os itens precedentes, será aplicável a penalidade de Impedimento de Licitar e Contratar com a Administração Direta e Indireta do Estado de Pernambuco, nos seguintes casos e condições:

**19.5.1.** No cometimento da infração prevista no item 19.1.1: de 6 a 12 meses;

**19.5.2.** No cometimento das infrações previstas nos itens 19.1.2 e 19.1.3: até 6 meses;

**19.6.** Além da multa, aplicada conforme os itens precedentes, será aplicável a penalidade de declaração de inidoneidade para licitar e contratar com a Administração Pública direta e indireta de todos os entes federativo, no cometimento das infrações previstas nos itens 19.1.4, 19.1.5, 19.1.6, 19.1.7, 19.1.8 e 19.1.9: de 03 a 6 anos;

**19.7.** Na fixação das penalidades, dentro das faixas de multa estabelecidas neste Edital, bem como dos prazos previstos nos itens 19.5 e 19.6. deverão ser observadas:

**19.7.1.** A natureza e a gravidade da infração cometida;

**19.7.2.** As peculiaridades do caso concreto;

**19.7.3.** Circunstâncias gerais agravantes ou atenuantes da infração

**19.7.4.** Os danos para a Administração Pública resultantes da infração;

**19.7.5.** A vantagem auferida em virtude da infração;

**19.7.6.** A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

**19.8.** Em caso de reincidência na prática de infração sancionada com a mesma penalidade objeto de condenação definitiva anterior, ocorrida no prazo igual ou inferior a 12 (dozes)

meses, contados da data de publicação da decisão definitiva da condenação anterior, as faixas de multa e os prazos previstos neste Edital poderão ser majorados em até 50% (cinquenta por cento), observados os limites máximos previstos em lei.

**19.9.** As penalidades deverão ser registradas no sistema e-fisco, no PE-integrado, no Compras.gov.br, no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), no prazo máximo de 15 (quinze) dias úteis, contados da data da decisão definitiva de aplicação da sanção.

**19.10.** Nenhuma penalidade será aplicada sem o devido Processo Administrativo de Aplicação de Penalidade - PAAP, disciplinado em Decreto Estadual.

**19.11.** Havendo indícios de cometimento das condutas previstas na Lei Federal nº 12.846/2013 (Lei Anticorrupção), a documentação pertinente será encaminhada às autoridades competentes para apuração da conduta típica em questão.

## 20. DAS DISPOSIÇÕES FINAIS

**20.1.** A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do pregão constarão de ata, sem prejuízo das demais formas de publicidade.

**20.2.** As decisões referentes a este processo licitatório poderão ser comunicadas às licitantes por qualquer meio de comunicação que comprove o seu recebimento ou, ainda, mediante publicação no Sistema Compras.gov ou no Diário Oficial do Estado de Pernambuco.

**20.3.** A presente licitação poderá ser revogada, por motivo de conveniência e oportunidade, em decorrência de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, ou será anulada, por ilegalidade insanável, de ofício ou por provocação de terceiros, mediante ato escrito e devidamente fundamentado, nos termos do art. 71 da Lei nº 14.133/2021.

**20.4.** Constatado vício insanável na licitação, a decisão sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será adotada na hipótese em que se revelar medida de interesse público, nos termos do art. 147 da Lei nº 14.133/2021.

**20.5.** Após a adjudicação do objeto, a revogação ou a anulação da licitação somente será efetivada depois de concedido à adjudicatária do prazo de 3 (três) dias úteis para exercício do direito ao contraditório e à ampla defesa.

**20.5.1.** Da decisão da autoridade de anular ou revogar o certame caberá recurso, no prazo de 03 (três) dias úteis para a autoridade máxima do órgão ou entidade responsável.

**20.6.** As licitantes não terão direito à indenização em decorrência da revogação, cabendo, em caso de anulação, o dever de indenizar o contratado pelo que houver executado até a data em que for declarada ou tornada eficaz, bem como por outros prejuízos regularmente comprovados, desde que não lhe seja imputável.

**20.7.** A participação das licitantes nesta licitação implica a aceitação de todos os termos deste Edital.

**20.8.** Em caso de divergência entre o Termo de Referência e o Edital de Licitação, prevalece o Edital.

**20.9.** Em caso de discordância existente entre as especificações do objeto a ser licitado descritas no Compras.gov.br e as especificações constantes deste Edital, prevalecerão as últimas.

**20.10.** Constituem anexos deste instrumento convocatório, dele fazendo parte integrante:

- a) Anexo I - Termo de Referência (com seus respectivos anexos, inclusive Modelo de Proposta);
- b) Anexo II - Declarações complementares;
- c) Anexo III - Declaração de conhecimento das condições locais para cumprimento das obrigações;
- d) Anexo IV - Declaração de conhecimento pleno das condições e peculiaridades da contratação;
- e) Anexo V - Minuta do Contrato (com seus respectivos anexos); e,
- f) Anexo VI - Modelo de Folha de Rosto.

**20.11.** Os casos omissos neste Edital serão decididos com base na Lei nº 14.133, de 2021, e demais normas que regem a matéria.

**20.12.** A data de abertura da sessão pública poderá ser adiada por conveniência do órgão licitante, sem prejuízo do disposto no art. 55, II, “a” e “b”, da Lei n.º 14.133, de 2021.

Recife, 05 de maio de 2026.

Maria Fernanda de Carvalho Nunes

Agente de Contratação/Pregoeira AC 10

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**ANEXO I**  
**TERMO DE REFERÊNCIA**

**1. DO OBJETO DA LICITAÇÃO**

1.1. O objeto da presente licitação é a contratação de prestações de serviços de rede corporativa segura com acesso à Internet, envolvendo implantação, operacionalização e melhoria contínua de serviços de acesso à Internet, conectividade de rede local e datacenter, voz, comunicação unificada, contact center, segurança e operação integrada de redes de computadores, visando atender as necessidades dos órgãos da Administração Direta, Indireta, Fundos Especiais, Autarquias e Fundações Públicas integrantes do Poder Executivo do Estado de Pernambuco, conforme as condições, especificações, quantidades e exigências contidas nos Estudos Técnicos Preliminares e neste Termo de Referência e seus adendos.

1.2. As especificações e os quantitativos do objeto desta licitação estão divididos em lotes e descritos conforme quadro abaixo:

LOTE 01										
Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
ADENDO III - SEGURANÇA DE REDE LOCAL										
1	598669-9	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1	UNIDADE	1759	48	R\$ 1.203,91	R\$ 2.117.677,69	R\$ 57.787,68	R\$ 101.648.529,12
2	598670-2	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2	UNIDADE	1299	48	R\$ 3.474,40	R\$ 4.513.245,60	R\$ 166.771,20	R\$ 216.635.788,80
3	598672-9	27014	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	193	48	R\$ 631,92	R\$ 121.960,56	R\$ 30.332,16	R\$ 5.854.106,88
4	598675-3	27014	Solução para gerenciamento de acessos à rede local - NAC	UNIDADE	24427	48	R\$ 4,34	R\$ 106.013,18	R\$ 208,32	R\$ 5.088.632,64
ADENDO IV - SERVIÇO DE REDE SEM FIO										
5	598692-3	27014	Serviço de Rede Sem Fio Interno com Segurança	UNIDADE	12892	48	R\$ 555,45	R\$ 7.160.861,40	R\$ 26.661,60	R\$ 343.721.347,20

6	598693-1	27014	Serviço de Rede Sem Fio Externo com Segurança	UNIDADE	500	48	R\$ 645,00	R\$ 322.500,00	R\$ 30.960,00	R\$ 15.480.000,00
7	598694-0	27014	Serviço de Rede Sem Fio Temporário com Segurança	UNIDADE	10	6	R\$ 819,01	R\$ 8.190,10	R\$ 4.914,06	R\$ 49.140,60
8	602034-8	27014	Serviço de fornecimento e implantação de Switch	UNIDADE	716	48	R\$ 705,03	R\$ 504.801,48	R\$ 33.841,44	R\$ 24.230.471,04
<b>ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL</b>										
9	598281-2	26174	Link de Acesso Permanente (LAP - Tipo 1)	UNIDADE	2968	48	R\$ 356,27	R\$ 1.057.409,36	R\$ 17.100,96	R\$ 50.755.649,28
10	598282-0	26174	Link de Acesso Permanente (LAP - Tipo 2)	UNIDADE	2212	48	R\$ 504,40	R\$ 1.115.732,80	R\$ 24.211,20	R\$ 53.555.174,40
11	598755-5	26174	Link Multitecnologia Especial (LME) - Tipo 1	UNIDADE	250	48	R\$ 1.011,99	R\$ 252.997,50	R\$ 48.575,52	R\$ 12.143.880,00
12	598757-1	26174	Link Multitecnologia Especial (LME) - Tipo 2	UNIDADE	20	48	R\$ 501,50	R\$ 10.030,00	R\$ 24.072,00	R\$ 481.440,00
13	598758-0	26174	Link Multitecnologia Especial (LME) - Tipo 3	UNIDADE	20	48	R\$ 870,16	R\$ 17.403,20	R\$ 41.767,68	R\$ 835.353,60
14	598761-0	26174	Link Acesso Temporário (LAT) - Tipo 1	UNIDADE	30	6	R\$ 612,00	R\$ 18.360,00	R\$ 3.672,00	R\$ 110.160,00
15	598762-8	26174	Link Acesso Temporário (LAT) - Tipo 2	UNIDADE	20	6	R\$ 1.273,00	R\$ 25.460,00	R\$ 7.638,00	R\$ 152.760,00
16	598763-6	26174	Link Acesso Temporário (LAT) - Tipo 3	UNIDADE	20	6	R\$ 1.500,00	R\$ 30.000,00	R\$ 9.000,00	R\$ 180.000,00
<b>ADENDO VI - SEGURANÇA DE DATACENTER</b>										
17	598673-7	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER	UNIDADE	6	48	R\$ 54.875,18	R\$ 329.251,08	R\$ 2.634.008,64	R\$ 15.804.051,84
18	598674-5	27014	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	3	48	R\$ 50.200,91	R\$ 150.602,73	R\$ 2.409.643,68	R\$ 7.228.931,04
19	598677-0	27014	Solução de segurança de confiança zero - ZTNA	UNIDADE	1.221	48	R\$ 21,17	R\$ 25.848,57	R\$ 1.016,16	R\$ 1.240.731,36
20	598678-8	27014	Solução de proteção, detecção e resposta para servidores - EDR	UNIDADE	4.200	48	R\$ 13,88	R\$ 58.296,00	R\$ 666,24	R\$ 2.798.208,00
21	598679-6	27014	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR	UNIDADE	3	48	R\$ 47.117,01	R\$ 141.351,03	R\$ 2.261.616,48	R\$ 6.784.849,44
22	598680-0	27014	Solução para gerenciamento de acessos à rede datacenter - NAC	UNIDADE	1.221	48	R\$ 6,53	R\$ 7.973,13	R\$ 313,44	R\$ 382.710,24
23	598681-8	27014	Solução de segurança de identidade privilegiada - PAM	UNIDADE	1.221	48	R\$ 305,53	R\$ 373.052,13	R\$ 14.665,44	R\$ 17.906.502,24
24	598682-6	27014	Solução de filtro de mensagens indesejadas - ANTISPAM	UNIDADE	129.058	48	R\$ 1,63	R\$ 210.364,54	R\$ 78,24	R\$ 10.097.497,92
25	598683-4	27014	Solução de Filtro de Aplicações WEB - WAF	UNIDADE	3	48	R\$ 51.924,09	R\$ 155.772,27	R\$ 2.492.356,32	R\$ 7.477.068,96
<b>ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO</b>										

26	598642-7	27014	Solução de gerenciamento e monitoramento de ativos - ITAM	UNIDADE	1	48	R\$ 246.050,00	R\$ 246.050,00	R\$ 11.810.400,00	R\$ 11.810.400,00
27	598685-0	27014	Solução de gerenciamento de identidade de acesso - IAM	UNIDADE	629.058	48	R\$ 0,61	R\$ 383.725,38	R\$ 29,28	R\$ 18.418.818,24
28	598686-9	27014	Solução de monitoramento e análise de eventos de segurança - SIEM	UNIDADE	477.186	48	R\$ 2,25	R\$ 1.073.668,50	R\$ 108,00	R\$ 51.536.088,00
29	598687-7	27014	Solução de automação de resposta a incidentes de segurança - SOAR	UNIDADE	1	48	R\$ 166.107,47	R\$ 166.107,47	R\$ 7.973.158,56	R\$ 7.973.158,56
30	598643-5	27014	Solução para guarda de LOGs	UNIDADE	1	48	R\$ 98.023,00	R\$ 98.023,00	R\$ 4.705.104,00	R\$ 4.705.104,00
31	598644-3	27014	Serviço de disponibilização de ambiente de testes	UNIDADE	1	48	R\$ 2.280,90	R\$ 2.280,90	R\$ 109.483,20	R\$ 109.483,20
32	598645-1	27014	Solução de gerenciamento de serviços de TI - ITSM	UNIDADE	1	48	R\$ 39.275,12	R\$ 39.275,12	R\$ 1.885.205,76	R\$ 1.885.205,76
<b>ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA</b>										
33	598688-5	26980	Serviço de resposta à incidentes de cibersegurança sob demanda	HORA	318	48	R\$ 580,00	R\$ 184.440,00	R\$ 27.840,00	R\$ 8.853.120,00
34	598646-0	26980	Serviço de análise de segurança de primeiro nível	UNIDADE	1	48	R\$ 84.855,26	R\$ 84.855,26	R\$ 4.073.052,48	R\$ 4.073.052,48
35	598647-8	26980	Serviço de análise de segurança especializada	UNIDADE	1	48	R\$ 340.980,00	R\$ 340.980,00	R\$ 16.367.040,00	R\$ 16.367.040,00
36	598648-6	26980	Serviço de acompanhamento de reparos	UNIDADE	1	48	R\$ 52.293,78	R\$ 52.293,78	R\$ 2.510.101,44	R\$ 2.510.101,44
37	598649-4	26980	Serviço de atenção especializada ao cliente	UNIDADE	1	48	R\$ 63.000,00	R\$ 63.000,00	R\$ 3.024.000,00	R\$ 3.024.000,00
38	598650-8	26980	Service Desk	UNIDADE	1	48	R\$ 91.292,00	R\$ 91.292,00	R\$ 4.382.016,00	R\$ 4.382.016,00
39	598651-6	26980	Serviço de operação da rede	UNIDADE	1	48	R\$ 86.240,00	R\$ 86.240,00	R\$ 4.139.520,00	R\$ 4.139.520,00
40	598653-2	26980	Serviço de análise de qualidade	UNIDADE	1	48	R\$ 69.576,00	R\$ 69.576,00	R\$ 3.339.648,00	R\$ 3.339.648,00
41	598654-0	26980	Serviço de Coordenação do CIISC	UNIDADE	1	48	R\$ 27.351,92	R\$ 27.351,92	R\$ 1.312.892,16	R\$ 1.312.892,16
42	598655-9	26980	Núcleo de Redes e Segurança Setorial	UNIDADE	5	48	R\$ 17.325,00	R\$ 86.625,00	R\$ 831.600,00	R\$ 4.158.000,00
43	602102-6	26980	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCs)	UNIDADE	22	48	R\$ 10.500,00	R\$ 231.000,00	R\$ 504.000,00	R\$ 11.088.000,00
44	598656-7	26980	Serviço de Evolução da Maturidade em Segurança da Informação	UNIDADE	1	48	R\$ 23.659,92	R\$ 23.659,92	R\$ 1.135.676,16	R\$ 1.135.676,16
<b>ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)</b>										
45	598691-5	1988	Serviço de Comunicação Unificada - SCU (Conta de usuário)	UNIDADE	500	48	R\$ 40,18	R\$ 20.090,00	R\$ 1.928,64	R\$ 964.320,00
<b>ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE</b>										
46	598696-6	1988	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)	UNIDADE	8199	48	R\$ 69,56	R\$ 570.322,44	R\$ 3.338,88	R\$ 27.375.477,12

47	598697-4	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	UNIDADE	8000	48	R\$ 58,98	R\$ 471.840,00	R\$ 2.831,04	R\$ 22.648.320,00
48	598698-2	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	UNIDADE	202	48	R\$ 91,90	R\$ 18.563,80	R\$ 4.411,20	R\$ 891.062,40
49	598699-0	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz DECT IP (PVF-DECT IP)	UNIDADE	354	48	R\$ 190,88	R\$ 67.571,52	R\$ 9.162,24	R\$ 3.243.432,96
50	598700-8	1988	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)	UNIDADE	3298	48	R\$ 35,00	R\$ 115.430,00	R\$ 1.680,00	R\$ 5.540.640,00
51	598701-6	1988	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)	UNIDADE	500	48	R\$ 22,65	R\$ 11.325,00	R\$ 1.087,20	R\$ 543.600,00
52	598703-2	1988	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)	UNIDADE	203	48	R\$ 103,17	R\$ 20.943,51	R\$ 4.952,16	R\$ 1.005.288,48
53	598704-0	1988	Serviço PVF-Fone-de-Cabeça	UNIDADE	1223	48	R\$ 27,33	R\$ 33.424,59	R\$ 1.311,84	R\$ 1.604.380,32
54	463377-6	1988	Serviço Fixo Inter Estadual	MINUTO	364	48	R\$ 0,03	R\$ 10,92	R\$ 1,44	R\$ 524,16
55	467295-0	1988	Serviço Fixo Intra Estadual	MINUTO	15.303	48	R\$ 0,03	R\$ 459,09	R\$ 1,44	R\$ 22.036,32
56	467296-8	1988	Serviço Fixo Local	MINUTO	84.960	48	R\$ 0,02	R\$ 1.699,20	R\$ 0,96	R\$ 81.561,60
57	467297-6	1988	Serviço Móvel Intra Estadual	MINUTO	137.450	48	R\$ 0,12	R\$ 16.494,00	R\$ 5,76	R\$ 791.712,00
58	467300-0	1988	Serviço Móvel Local	MINUTO	575.533	48	R\$ 0,06	R\$ 34.531,98	R\$ 2,88	R\$ 1.657.535,04
59	467302-6	1988	Serviço Móvel VC2	MINUTO	23.051	48	R\$ 0,20	R\$ 4.610,20	R\$ 9,60	R\$ 221.289,60
60	467303-4	1988	Serviço Móvel VC3	MINUTO	802	48	R\$ 0,20	R\$ 160,40	R\$ 9,60	R\$ 7.699,20
61	467304-2	1988	Serviço Longa Inter Regional Fixo	MINUTO	475	48	R\$ 0,13	R\$ 61,75	R\$ 6,24	R\$ 2.964,00
62	598664-8	1988	Serviço Adicional de Acesso SIP (SIP TRUNK)	UNIDADE	21	48	R\$ 850,00	R\$ 17.850,00	R\$ 40.800,00	R\$ 856.800,00
<b>ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER</b>										
63	598657-5	1988	Serviço de Contact Center com Recurso de Voz	UNIDADE	250	48	R\$ 800,31	R\$ 200.077,50	R\$ 38.414,88	R\$ 9.603.720,00
64	598658-3	1988	Serviço de Contact Center com recurso de Whatsapp	UNIDADE	400	48	R\$ 838,61	R\$ 335.444,00	R\$ 40.253,28	R\$ 16.101.312,00
65	598659-1	1988	Serviço de Contact Center com recurso de Redes Sociais	UNIDADE	50	48	R\$ 1.131,00	R\$ 56.550,00	R\$ 54.288,00	R\$ 2.714.400,00
67	598661-3	1988	Serviço de Comunicação por vídeo ou video-chamada	UNIDADE	60	48	R\$ 841,00	R\$ 50.460,00	R\$ 40.368,00	R\$ 2.422.080,00
68	598662-1	1988	Serviço de Automatizações e Integrações - Consultoria Inicial	UNIDADE	5	48	R\$ 1.462,25	R\$ 7.311,25	R\$ 70.188,00	R\$ 350.940,00
69	598663-0	1988	Serviço de Automatizações e Integrações -	UNIDADE	100	48	R\$ 1.551,80	R\$ 155.180,00	R\$ 74.486,40	R\$ 7.448.640,00

			Implantação							
<b>ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO DOS SERVIÇOS</b>										
70	598640-0	27120	Suporte de Manutenção (12h x 7d)	UNIDADE	600	48	R\$ 130,10	R\$ 78.060,00	R\$ 6.244,80	R\$ 3.746.880,00
71	598641-9	27120	Suporte de Manutenção (24h x 7d)	UNIDADE	500	48	R\$ 371,10	R\$ 185.550,00	R\$ 17.812,80	R\$ 8.906.400,00
									<b>TOTAL LOTE 01</b>	<b>R\$ 1.180.217.323,80</b>

<b>LOTE 02</b>										
Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
<b>ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER</b>										
72	598287-1	26506	Link de Fibra Lan To Lan (L2L)	UNIDADE	4	48	R\$ 23.180,24	R\$ 92.720,96	R\$ 1.112.651,52	R\$ 4.450.606,08
73	598288-0	26506	Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	12	R\$ 8.097,92	R\$ 24.293,76	R\$ 97.175,04	R\$ 194.350,08
74	598289-8	26506	Link para Data Center de 4GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	12	R\$ 17.677,10	R\$ 53.031,30	R\$ 212.125,20	R\$ 424.250,40
75	598290-1	26506	Link para Data Center de 6GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	12	R\$ 20.555,52	R\$ 61.666,56	R\$ 246.666,24	R\$ 493.332,48
76	598291-0	26506	Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	06	R\$ 17.653,76	R\$ 52.961,28	R\$ 105.922,56	R\$ 211.845,12
77	598292-8	26506	Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	06	R\$ 19.814,40	R\$ 59.443,20	R\$ 118.886,40	R\$ 237.772,80
									<b>TOTAL LOTE 02</b>	<b>R\$ 6.012.156,96</b>

<b>LOTE 03</b>										
Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
<b>ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS</b>										
78	598665-6	27324	Serviço de gestão de vulnerabilidades	UNIDADE	4.200	48	R\$ 89,00	R\$ 373.800,00	R\$ 4.272,00	R\$ 17.942.400,00
79	598666-4	27324	Serviço de análise forense	HORA	141	48	R\$ 798,00	R\$ 112.518,00	R\$ 38.304,00	R\$ 5.400.864,00
80	598667-2	27324	Serviço de análise de segurança ofensiva (Red Team)	UNIDADE	1	48	R\$ 194.986,00	R\$ 194.986,00	R\$ 9.359.328,00	R\$ 9.359.328,00

81	598668-0	27324	Serviço de testes de intrusão (Pentest)	UNIDADE	10	48	R\$ 78.976,00	R\$ 789.760,00	R\$ 3.790.848,00	R\$ 37.908.480,00
									<b>TOTAL LOTE 03</b>	R\$ 70.611.072,00

1.3. Em caso de discordância existente entre as especificações do objeto descritas no E-fisco/Termo de Referência e no CATSER, prevalecerá a descrição do E-fisco/Termo de Referência.

1.4. A tabela acima apresenta uma estimativa da execução contratual de cada item de serviço ao longo dos 48 (quarenta e oito) meses de vigência. Ressalta-se que a utilização dos itens poderá ser ajustada de acordo com a demanda real dos Contratantes Aderentes. Considerando tratar-se de um **Contrato Mater**, destaca-se que a execução dos quantitativos indicados não está condicionada às projeções iniciais aqui descritas, estando sujeita à variação conforme a necessidade efetivas da Administração, não constituindo obrigação de consumo mínimo por parte do Poder Público.

## 2. DAS JUSTIFICATIVAS

### 2.1. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

A Justificativa e objetivo da contratação encontram-se pormenorizadas em tópico específico dos Estudos Técnicos Preliminares (item 2 do ETP), anexo deste Termo de Referência.

**2.1.1.** Contratação de uma Nova Rede Corporativa é imperativa para o Estado de Pernambuco, uma vez que o atual contrato de serviços está em vias de expirar, e a continuidade dos serviços públicos, dependente dessa infraestrutura, deve ser assegurada sem interrupções. A falta de conectividade comprometeria o funcionamento dos sistemas governamentais, impedindo que os servidores públicos acessem as plataformas essenciais para suas atividades e afetando diretamente os cidadãos, que ficariam sem acesso aos serviços disponibilizados pelos *Datacenters* estaduais, de acordo com as especificações e quantidades constantes neste Termo de Referência.

**2.1.2. Análise do Cenário Atual:** A infraestrutura atual de conectividade e cibersegurança já não atende às crescentes demandas de tráfego e aos avanços das ameaças cibernéticas. Esse quadro expõe o Estado a riscos críticos, como vazamento de dados sensíveis e a interrupção dos serviços essenciais, além de aumentar a vulnerabilidade a ataques cibernéticos que poderiam comprometer operações governamentais.

#### 2.1.3. Principais Interesses e Benefícios

2.1.3.1. Essa contratação busca proteger informações sensíveis, manter a eficiência dos serviços e promover a inclusão digital. Os benefícios esperados incluem:

2.1.3.2. **Aumento da Segurança Cibernética:** Menor exposição a ciberataques, garantindo a integridade dos sistemas e proteção de dados sensíveis.

2.1.3.3. **Melhoria na Eficiência Operacional:** Modernização que minimiza riscos de interrupções e aumenta a rapidez nas comunicações internas e externas.

2.1.3.4. **Inclusão Digital e Acesso Público:** Expansão do Wi-Fi público e uma rede robusta que amplia o acesso cidadão.

**Confiança Pública e Inovação:** Investir na segurança e modernização da infraestrutura fortalece a confiança nas instituições e permite a adoção de novas tecnologias.

2.1.3.5. Este processo é essencial não apenas para a continuidade e segurança dos serviços, mas também para consolidar o Estado de Pernambuco como um modelo de inovação e proteção digital no setor público.

## 2.2. JUSTIFICATIVA DO QUANTITATIVO ESTIMADO

2.2.1. A Justificativa para o quantitativo necessário ao atendimento da necessidade pública encontra-se pormenorizada para cada item de serviço em tópico específico dos Estudos Técnicos Preliminares (**7 - ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS**), anexo deste Termo de Referência.

2.2.2. Cada quantidade estimada foi justificada a partir das necessidades identificadas no ambiente de TI do Governo do Estado de Pernambuco e das exigências regulatórias aplicáveis. Os quantitativos finais da contratação precisaram ser enquadrados ao orçamento previsto para o processo. A necessidade de contratação desses serviços é evidente pela crítica função que desempenham na proteção dos ativos informacionais e na manutenção da continuidade operacional da instituição.

2.2.3. O planejamento das quantidades CONTRATADAS visa assegurar que os serviços contratados estejam plenamente alinhados com as demandas reais e futuras, evitando tanto o Subdimensionamento quanto o superdimensionamento da contratação.

2.2.4. A estimativa dos serviços a serem contratados foi desenvolvida com base em uma análise rigorosa das necessidades do Governo do Estado de Pernambuco, sempre focando em garantir a adequação e a eficiência dos serviços de segurança cibernética, conectividade, voz, Wi-Fi, SOC e NOC. Os serviços de instalação, configuração, capacitação, e licenciamento de *software* foram considerados como partes integradas do escopo.

2.2.5. O quantitativo estimado para cada item de serviço está descrito no item **1 - DO OBJETO DA LICITAÇÃO** deste Termo de Referência.

## 2.3. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

2.3.1. A Justificativa da escolha da solução a ser licitada encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares ao longo dos itens **8 - ANÁLISE COMPARATIVA DAS SOLUÇÕES**, **9 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS**, **10 - ANÁLISE COMPARATIVA DE CUSTOS (TCO)** e **16 - DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**, anexo deste Termo de Referência.

2.3.2. De forma resumida, seguem as justificativas para a escolha da Solução de Rede Corporativa com Segurança e Banda Larga.

2.3.2.1. O Modelo de contratação é composto por links banda larga, solução de segurança centralizada com equipamento de última milha, solução de rede sem fio, solução de detecção e resposta à dispositivos finais, monitoramento das operações de segurança, gestão de qualidade e uso dos serviços, processos, pessoas e tecnologias de segurança providos por uma única empresa ou consórcio. Além destes, haverá também itens de serviço complementares, compostos por links multitecnologias redundantes e conectividade de *Datacenter* em lotes distintos.

2.3.2.2. A solução se destaca como a opção mais viável para atender às necessidades do Governo de Pernambuco. Esta escolha é fundamentada na sua agilidade no processo, maior capacidade de gestão e facilidade de implementação. Ao optar pela consolidação da prestação dos serviços, elimina-se a necessidade de aguardar a conclusão de outros processos licitatórios para sua implementação. Uma vez concluído o processo, o serviço pode ser imediatamente utilizado em sua totalidade, garantindo continuidade e integridade ao longo do processo. Além disso, é importante ressaltar que este modelo de contratação já é uma prática consolidada e bem-sucedida no estado de Pernambuco.

2.3.2.3. Dentre as soluções analisadas, a solução escolhida apresentou nível de atendimento máximo para todas as Necessidades de Negócio - NN e Necessidade Técnicas – NT, além de se demonstrar mais vantajoso economicamente para o Governo de Pernambuco.

## 2.4. JUSTIFICATIVA PARA O PARCELAMENTO DA CONTRATAÇÃO

2.4.1. A Justificativa para o parcelamento da contratação encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares ao longo do item **11 - JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO**, anexo deste Termo de Referência, de modo a permitir a ampliação da competitividade, diante das particularidades do caso concreto.

2.4.2. No caso concreto, em virtude da natureza do serviço a ser contratado, a opção pela divisão em LOTES é a mais vantajosa para a Administração, uma vez que cada LOTE é formado por itens de serviço tecnicamente específicos exigindo empresas com especialização técnica e expertise necessárias para cada um dos lotes. A divisão permite que empresas com competências específicas em cada área possam focar suas melhores práticas e soluções, aumentando a qualidade e eficácia de cada serviço prestado.

2.4.3. A decisão foi fundamentada em uma análise criteriosa que abrange aspectos técnicos, econômicos e estratégicos, sendo listados abaixo os principais argumentos:

### 2.4.3.1. 1º LOTE: Serviço de Segurança de Toda a Rede + Conectividade com Banda Larga (Link Principal + Redundância) + Comunicação de Voz

- **Integração Técnica e Operacional:** A segurança da rede e a conectividade principal são elementos críticos e interdependentes. Ao consolidar esses serviços em um único lote, garantimos que a implementação de soluções de segurança esteja diretamente alinhada com a gestão da conectividade principal, evitando incompatibilidades e simplificando a operação. Isso é vital para manter a integridade, a disponibilidade e a confidencialidade dos dados trafegados pela rede do governo.
- **Redução de Complexidade:** A gestão centralizada desses serviços por um único fornecedor ou consórcio reduz a complexidade administrativa e operacional, permitindo uma resposta mais rápida a incidentes e uma coordenação mais eficaz entre as equipes de segurança e de infraestrutura de rede.
- **Economia de Escala e Eficiência Operacional:** A unificação desses serviços permite ao fornecedor otimizar recursos e infraestrutura, resultando em uma redução significativa de custos operacionais. A economia de escala obtida através da centralização desses serviços também proporciona maior poder de negociação para o Estado, resultando em contratos mais vantajosos e eficientes.

### 2.4.3.2. 2º LOTE: Conectividade *Datacenter* com AntiDDoS

- **Especialização e Foco em Segurança Crítica:** A conectividade de *Datacenter*, com a proteção AntiDDoS, é um serviço altamente especializado, essencial para garantir a segurança e a continuidade das operações de TI do governo. A previsão deste serviço em um lote dedicado permite a contratação de fornecedores com expertise específica em mitigação de ataques DDoS e gestão de infraestruturas de alta disponibilidade. Isso reduz significativamente os riscos de indisponibilidade e violações de segurança, protegendo dados sensíveis e serviços críticos do Estado.
- **Adaptação às Inovações Tecnológicas:** O setor de segurança cibernética e infraestrutura de *Datacenter* é dinâmico, com constantes inovações tecnológicas. A especialização deste lote permite que o Estado aproveite as últimas inovações em proteção de rede e gestão de *Datacenter*, garantindo que as soluções contratadas sejam robustas, atualizadas e eficazes contra ameaças emergentes.
- **Aumento da Competitividade:** O serviço de *Datacenter* com AntiDDoS compoendo este lote atrai empresas especializadas que podem oferecer soluções inovadoras e economicamente competitivas. Isso não apenas melhora a qualidade das propostas recebidas, mas também amplia o leque de opções tecnológicas disponíveis para o governo.

### 2.4.3.3. 3º LOTE: Avaliação e Mitigação de Riscos Cibernéticos

- **Foco em segurança ofensiva:** Ao prever esses serviços neste lote, o estado pode contratar fornecedores com expertise avançada em segurança ofensiva e análise forense, garantindo a identificação de riscos antes que sejam explorados por agentes mal-intencionados, elevando a proteção da rede e dos dados governamentais.
- **Prevenção e análise a ameaças avançadas:** A gestão de vulnerabilidades, aliada aos testes de intrusão, permite ao governo antecipar falhas em suas infraestruturas críticas. A análise forense, por sua vez, assegura que, em caso de ataques, a origem e o impacto sejam investigados, aprimorando a segurança continuamente.
- **Flexibilidade e competitividade no mercado:** Quanto ao serviço de avaliação e mitigação de riscos cibernéticos compondo este lote, o estado atrai empresas especializadas, ampliando a competitividade no processo de contratação e obtendo soluções mais customizadas e adaptadas às necessidades de segurança, com maior qualidade dos serviços.

2.4.4. Conclui-se, portanto, que o modelo definido para esta contratação é o mais adequado tanto tecnicamente, quanto economicamente, sem restringir ou prejudicar a competitividade do certame e, consequentemente, o mais propício para promover maior vantagem para o Estado.

## 2.5. DA PREVISÃO DA PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO PARA OS LOTES 1 E 2

2.5.1. No caso vertente, é permitida a participação de empresas sob a forma de consórcio para o LOTE 01 e LOTE 02, na forma do art. 15, da Lei nº 14.133/2021. A justificativa da permissão de consórcio, deve-se à execução de serviços especiais, por envolverem objeto dotado de heterogeneidade e complexidade, onde pode demandar a conjugação de esforços de mais de uma empresa para viabilizar a participação no certame e aumento da concorrência, como delineado na NOTA TÉCNICA - Nº 4/2025 (doc. SEI 66422745);

2.5.2. O número máximo de empresas admitidas em cada consórcio para o LOTE 01 será de 5 (cinco) empresas por consórcio, que apresentem os requisitos de habilitação dispostos neste Edital e que satisfaçam integralmente as condições e exigências deste.

2.5.2.1. Esta limitação em 5 (cinco) empresas por consórcio, é justificada por ser este lote composto por serviços específicos e integrados entre si, podendo ser prestados por empresas (operadoras, integradores e provedores) cada uma delas com grau de maior ou menor expertise no âmbito de serviços de segurança de rede, conectividade e de comunicação de voz. A participação em consórcio das melhores expertises permitirá um maior benefício tecnológico, econômico e de gestão à rede governo, bem como amplia a condição de competitividade.

2.5.3. O número máximo de empresas admitidas em cada consórcio para o LOTE 02 será de 3 (três) empresas por consórcio, que apresentem os requisitos de habilitação dispostos neste TR e que satisfaçam integralmente as condições e exigências dele.

2.5.3.1. Esta limitação em 3 (três) empresas por consórcio, é justificada por ser este lote composto por serviços específicos e integrados entre si, podendo ser prestados por empresas (operadoras, integradores e provedores) cada uma delas com grau de maior ou menor expertise no âmbito de serviços de conectividade, serviço de trânsito e solução AntiDDoS.

2.5.3.2. A permissão para a formação de consórcios justifica-se pela necessidade de assegurar a ampla concorrência e a efetiva participação de empresas com especializações complementares, tendo em vista a complexidade e a abrangência dos serviços exigidos para a implantação e operação da Nova Rede Corporativa do Estado. Trata-se de uma contratação que reúne atividades técnicas diversificadas, incluindo fornecimento de links, instalação de equipamentos, suporte especializado, manutenção preventiva e corretiva, monitoramento, segurança cibernética, atendimento presencial e remoto, entre outros, que muitas vezes não se encontram integralmente no portfólio de uma única empresa prestadora. Dessa forma, a possibilidade de consorciamento visa garantir que o objeto licitado seja

plenamente atendido em seus aspectos técnicos e operacionais, permitindo que empresas com expertises distintas se unam para cumprir os requisitos do Termo de Referência com qualidade e cobertura territorial. Essa medida está alinhada ao interesse público na medida em que favorece a competitividade e a economicidade, ao mesmo tempo em que respeita a realidade do mercado local e nacional, em que é comum a especialização segmentada por tipo de serviço ou região de atuação. Além disso, a previsão de consórcios está de acordo com o disposto no art. 15 da Lei nº 14.133/2021, que admite a participação conjunta de empresas quando tal formato se mostra necessário à ampliação da competitividade e à execução eficiente do objeto licitado. A adoção dessa medida, portanto, não apenas atende a realidade do mercado, mas também busca garantir o atendimento integral da necessidade pública de implantação da nova rede corporativa nas localidades espalhadas pelo território estadual, com a qualidade e a capilaridade exigidas pelo projeto.

## 2.6. DA PREVISÃO DA VEDAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO PARA O LOTE 3

2.6.1. De acordo com o art. 15 da Lei nº 14.133/2021, a participação de empresas reunidas em consórcio poderá ser vedada, segundo discricionariedade da Administração, com base em justificativa técnica que leve em consideração as peculiaridades do caso concreto.

2.6.2. Assim, para o **LOTE 03**, não poderá participar desta licitação sob a forma de consórcio de empresa, qualquer que seja sua forma de constituição, visto que não se faz necessária a conjugação de esforços para a prestação do presente serviço contínuo.

2.6.3. Além disso, no caso vertente, não se faz presente a premissa da complexidade do objeto, uma vez que ao separar esses serviços, o Estado pode contratar fornecedores com expertise avançada em segurança ofensiva e análise forense, garantindo a identificação de riscos antes que sejam explorados por agentes mal-intencionados, elevando a proteção da rede e dos dados governamentais. Também não está presente o grande vulto da contratação, pois o Estado atrai empresas especializadas, ampliando a competitividade no processo de contratação e adaptada às necessidades de segurança, com maior qualidade dos serviços. Adicionalmente, ressalta-se que a natureza dos serviços previstos no Lote 03 exige domínio técnico específico e atualizado, o que é mais eficientemente atendido por empresas com atuação dedicada e estrutura já consolidada, o que torna desnecessária a união de empresas com competências distintas. A vedação à formação de consórcio, nesse contexto, visa ainda garantir maior clareza quanto à responsabilidade contratual e à prestação dos serviços, evitando eventuais conflitos de governança entre consorciadas que possam comprometer a execução dos serviços de segurança cibernética. Soma-se a isso o fato de que a contratação direta de empresas individualmente capacitadas facilita a fiscalização, o controle e a responsabilização administrativa, contribuindo para a efetividade da gestão pública e a mitigação de riscos operacionais, jurídicos e contratuais.

2.6.4. Por todo o exposto, conclui-se que a vedação da participação de empresas sob a forma de consórcio no LOTE 03 é a medida que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

## 2.7. DA VEDAÇÃO DE PROFISSIONAIS ORGANIZADOS EM COOPERATIVA NA LICITAÇÃO

2.7.1. É vedada a participação de profissionais organizados em cooperativas na presente licitação, uma vez que a estrutura de cooperativa prejudica a fiscalização direta sobre as obrigações contratuais, trabalhistas e previdenciárias, além de comprometer a continuidade e a uniformidade dos serviços, características fundamentais para o bom atendimento do objeto contratual.

## 2.8. DA VEDAÇÃO DE PESSOAS FÍSICAS NA LICITAÇÃO

2.8.1. É vedada a participação de pessoas físicas na presente licitação, uma vez que restrição visa garantir que as condições contratuais e operacionais exigidas para a execução do objeto da licitação sejam atendidas de forma plena, assegurando-se que a licitante possua estrutura organizacional, capacidade técnico-operacional e financeira adequadas para a realização dos serviços ou fornecimento de produtos.

### **3. DAS ESPECIFICAÇÕES DO OBJETO**

#### **3.1. CONCEITOS, INFORMAÇÕES GERAIS PARA A PRESTAÇÃO DOS SERVIÇOS INTEGRANTES DA Nova Rede Corporativa**

3.1.1. Inicialmente, visando uma melhor compreensão do modelo de prestação aqui requerido, serão descritos informações, conceitos e exigências a serem observadas e cumpridas pelas CONTRATADAS. Em seguida, cada serviço integrante desta solução será detalhado.

3.1.2. AS CONTRATADAS devem realizar a prestação de serviços da nova Rede dentro das especificações contidas nos itens e seus subitens deste Termo de Referência, considerando os conceitos definidos a seguir.

3.1.3. AS CONTRATADAS devem considerar todos os Órgãos e Entidades que aderirem ao Contrato de Prestação de Serviços referente ao objeto deste Termo de Referência, como Órgãos aderentes à Nova Rede Corporativa. Os Órgãos aderentes ao formalizar seus respectivos Contratos de Adesão serão considerados CONTRATANTES aderentes, passando a ter as responsabilidades previstas neste Termo de Referência, bem como, passarão a arcar com os pagamentos dos serviços contratados quando efetivamente prestados e atestados pelo Gestor dos serviços no Órgão.

3.1.4. Todos os equipamentos e dispositivos de Telemática, exclusivos e fornecidos para a prestação dos serviços da nova Rede como um todo, devem ser novos e sem uso.

3.1.5. O conceito de Operação Integrada passará a ser de um Centro Integrado de Inteligência e Segurança Cibernética (CIISC), englobando e enfatizando ainda mais o foco nos serviços de segurança para o Estado.

3.1.6. Poderão aderir ao Contrato dos serviços da Nova Rede Corporativa:

3.1.6.1. Todos os Órgãos e Entidades da Administração Direta e Indireta, inclusive Fundacional, do Poder Executivo Estadual, a seguir denominada CONTRATANTE aderente, mediante Contrato de Adesão ao Contrato Mater.

3.1.6.2. Os Poderes Judiciário e Legislativo Estadual, bem como, o Ministério Público Estadual e Tribunal de Contas do Estado, mediante convênios específicos celebrados com o Governo do Estado, e assinatura do Contrato de Adesão, assim como, as Organizações Sociais que mantenham ou venham a manter Contrato de Gestão com o Estado.

3.1.6.3. Todos os entes denominados CONTRATANTES aderentes arcarão com todas as despesas decorrentes dos Termos de Adesão firmados com a CONTRATADA.

3.1.6.4. A adesão das Organizações Sociais ao Contrato deverá ser devidamente consignada no Contrato de Gestão e contabilizada como aporte de recursos estaduais.

3.1.7. As CONTRATADAS devem atender a Área de Abrangência da Nova Rede Corporativa, assim definida: a capital Recife e todos os Municípios do Estado de Pernambuco, incluindo o arquipélago de Fernando de Noronha, Brasília, como também, em localidades de divisas territoriais do Estado de Pernambuco com os Estados vizinhos: Alagoas, Bahia, Piauí, Ceará e Paraíba no raio de até 30 Km, para atender as necessidades de conexão dos órgãos aderentes, incluindo todos os serviços integrantes deste Termo de Referência e seus adendos. A CONTRATADA deverá prover capacidade operacional suficiente para a plena prestação dos serviços de telecomunicações da Nova Rede Corporativa dentro da sua abrangência.

3.1.8. A abrangência da Nova Rede Corporativa está descrita neste Termo de Referência. Os dados do ANEXO C são exemplificativos e não taxativos, refletindo apenas aquelas localidades que se encontram atualmente instaladas,

podendo, assim, serem substituídos ou acrescidos a critério da Administração antes ou durante a execução do contrato da Nova Rede Corporativa, sem que isso represente qualquer ônus para esta.

3.1.9. A CONTRATADA deve adotar o Protocolo TCP/IP para o tráfego de dados e voz em toda da Nova Rede Corporativa, bem como a tecnologia VoIP para o tráfego de voz entre os usuários dos serviços de telefonia fixa da rede.

3.1.10. A CONTRATADA deve adotar o Protocolo IPv6 em toda Nova Rede Corporativa e para todos os serviços desta. Garantir a coexistência, bem como a interoperabilidade, entre IPv6 e IPv4 nos equipamentos conectados via Rede e aos produtos que suportam ambos os protocolos, respeitando a RFC 3531, mantendo as conexões entre eles, não devendo isolar redes por versão de protocolo IPs.

3.1.11. Suportar tráfego (*upload e download*) entre provedores. Os endereçamentos IPv6 a serem implantados nos Pontos Conectados Seguros (PCSs) devem ser realizados pela CONTRATADA, incluindo os respectivos equipamentos integrantes do PCS, tais como roteadores, UTMs, pontos de acesso sem fio interno/externo (Wi-Fi) e demais equipamentos integrantes da prestação de serviços contratados e operacionalizados pela Nova Rede Corporativa.

3.1.12. **Ponto Conectado Seguro - PCS**, também conhecido como SITE, é o local designado pela CONTRATANTE, onde a conexão com a Nova Rede Corporativa é feita com os serviços contratados pelos aderentes. Os PCSs são as unidades administrativas e organizacionais públicas, tais como Hospitais, Delegacias, Sedes dos Órgãos, Escolas, Anexos, Unidades de Atendimento ao Cidadão, Postos para atividades de Fiscalização etc. Os PCSs são ambientes operacionais onde serão providos os diversos serviços de conectividade e segurança previstos neste TR. Os PCSs não serão precificados como itens de prestação de serviço, mas apenas os itens dos serviços pertinentes e contidos neste Termo e operacionalizados em um PCS. As especificações detalhadas para prestação dos serviços estão descritas nos ADENDOS, contidos neste Termo.

3.1.13. Serviços de conectividade e operação

3.1.13.1. **Links de Acesso (LA)**, são circuitos de dados, conhecidos como links ou conexões de última milha, que serão utilizados para acesso à Internet partindo do PCS, podendo ser de três tipos (Links de Acesso Permanente (LAP), Links Multitecnologia Especial (LME) e Link de Acesso Temporário (LAT)), cujas características e funcionalidades básicas estão apresentadas abaixo e as especificações detalhadas descritas no ADENDO V.

3.1.13.2. **Links de Acesso Permanente (LAP)**, são os circuitos destinados às conexões dos Pontos Conectados Seguros (PCSs) da Nova Rede Corporativa serão disponibilizados em dois tipos: Links de Acesso Permanente Tipo 1 (LAP Tipo 1) e Links de Acesso Permanente Tipo 2 (LAP Tipo 2).

3.1.13.2.1. Os circuitos **LAP Tipo 1** correspondem aos Links de Banda Larga (LBL) com velocidade de 500 Mbps, sendo facultado à CONTRATADA optar pela entrega de Links Dedicados (LD) com velocidade de 300 Mbps.

3.1.13.2.2. Os circuitos **LAP Tipo 2** correspondem aos Links de Banda Larga (LBL) com velocidade de 1 Gbps, sendo facultado à CONTRATADA optar pela entrega de Links Dedicados (LD) com velocidade de 500 Mbps.

3.1.13.2.3. Os links denominados **Link Banda Larga (LBL)** são usados nas conexões dos PCSs da Nova Rede Corporativa para acesso Internet. Esses LBLs podem ser fornecidos a partir de tecnologias e recursos diversos da área de telecomunicações, as quais devem ser apropriadas para tais finalidades, garantindo as especificações descritos no Regulamento de Qualidade dos Serviços de Telecomunicações (RQUAL), aprovado pela Resolução nº 717/2019 (Fonte: - <https://informacoes.anatel.gov.br/legislacao/resolucoes/2019/1371-resolucao-717> - em 01/07/2024).

3.1.13.2.4. Os links denominados **Link Dedicado (LD)** são usados nas conexões dos PCSs da Nova Rede Corporativa para acesso Internet com acesso determinístico, conexão simétrica, e garantia de banda. Esses LDs podem ser fornecidos a partir de tecnologias e recursos diversos da área de telecomunicações, as quais devem ser apropriadas para tais finalidades, garantindo as especificações descritos no Termo de Referência.

3.1.13.3. Os links denominados **Link Acesso Temporário (LAT)** são usados nas conexões dos PCSs da Nova Rede Corporativa, para as unidades administrativas que precisam ter acesso à internet durante eventos sazonais e/ou es-

peciais, podendo ser providos a partir de tecnologias e recursos diversos da área de telecomunicações, as quais devem ser apropriadas para tais finalidades, mas a banda larga deverá ser o tipo de acesso preferencial.

3.1.13.4. Os links denominados **Link Multitecnologia Especial (LME)** são usados nas conexões com os PCSs da Nova Rede Corporativa, específicas para aplicações especiais, tais como: Conexões redundantes, Interconexões ponto-a-ponto e outras aplicações consideradas especiais pela CONTRATANTE. Esses LMEs podem ser fornecidos a partir de tecnologias e recursos diversos da área de telecomunicações, as quais devem ser apropriadas para tais finalidades, podendo ter QoS (Quality of Service) específico.

3.1.13.5. Conectividade **Lan To Lan (L2L)**, são infraestruturas físicas de conectividade em fibra ótica, com origem e destino determinados. As especificações detalhadas estão descritas no ADENDO VII, contido neste Termo.

3.1.13.6. **Link de Internet Trânsito para Datacenter com AntiDDoS (LIT)**, são circuitos de dados, conhecidos como links ou conexões de última milha, que proverão acesso à Internet especializado e com proteção de forma dedicada e simétrica, partindo do PCS onde o *Datacenter* da CONTRATANTE está localizado. As especificações detalhadas estão descritas no ADENDO VII, contido neste Termo.

3.1.13.7. Prover o serviço de **Rede Sem Fio Wi-Fi (SRSF)**. A CONTRATADA deve disponibilizar uma Infraestrutura de comunicações de rede sem fio padrão IEEE 802.11, que também são conhecidas como redes Wi-Fi ou *wireless*, que permita a transmissão de informações entre dispositivos, sem a necessidade de uso de meios físicos. Será usada nas conexões com tecnologia sem fio, nas modalidades Aberta e Fechada. As especificações detalhadas estão descritas no ADENDO IV, contido neste Termo.

3.1.13.8. Prover o serviço de **Operação da Segurança da Nova Rede Corporativa**. A CONTRATADA deve identificar, proteger, detectar, responder e recuperar contra diversos tipos de ameaças contra a Nova Rede Corporativa e seus respectivos clientes e ativos (dados trafegados, informações, equipamentos, serviços etc.). Estas ações visam garantir a disponibilidade, integridade, confidencialidade e autenticidade destes ativos, empregando processos maduros e modernas soluções de segurança de mercado, através de controles que devem ser aplicados de acordo com políticas definidas pela ATI.

3.1.13.9. Prover o serviço de **Centro Integrado de Inteligência e Segurança Cibernética**, que conterà os times de Grupo de especialistas, Analista de suporte residente, Especialistas de atenção, *Service desk*, Analistas de primeiro nível, Técnicos de dados e voz, Analistas de qualidade, Liderança do primeiro nível, Liderança dos especialistas e Coordenação, conforme especificado no ADENDO IX deste Termo.

3.1.13.10. Prover o serviço de **Núcleo de Redes e Segurança Setorial**. A CONTRATADA deve disponibilizar os recursos tecnológicos necessários para permitir a realização do serviço de segurança, que deverá ser instalado na CONTRATANTE aderente, para monitoração, análise, emissão de relatórios, e acionamento para reparação dos serviços, seja da CONTRATADA para prestação destes serviços da Nova Rede Corporativa ou de responsabilidade da CONTRATANTE aderente, através de outros contratos para reparação dos serviços monitorados.

3.1.13.11. Todas as especificações detalhadas estão descritas nos ADENDOS contidos neste Termo.

## 3.2. DA EXECUÇÃO DOS SERVIÇOS

3.2.1. Os serviços descritos neste termo de referência serão prestados nos locais e horários indicados pela contratante aderente mediante envio de ordem de serviço.

3.2.2. A Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho estabelecidos nos Adendos deste Termo de Referência.

3.2.3. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas nos Adendos deste Termo de Referência.

3.2.4. O objeto será recebido mensalmente:

- a. Provisoriamente, pelo fiscal do CONTRATO no prazo de 5 (cinco) dias mediante termo detalhado que ateste o cumprimento das exigências de caráter técnico e administrativo e a comprovação da prestação dos serviços;
- b. Definitivamente, por servidor ou comissão designada pela autoridade competente, no prazo de 2 (dois) dias úteis, contados do recebimento provisório.

3.2.5. O termo detalhado do recebimento provisório, com a análise das ocorrências registradas na execução do CONTRATO será encaminhado ao gestor para fins de apuração dos descontos e glosas cabíveis na fatura correspondente, em virtude de serviços total ou parcialmente não executados ou, se for o caso, da pontuação obtida na avaliação da qualidade dos serviços em consonância com os indicadores previstos no Instrumento de Medição de Resultado (IMR), descritos no Adendo II – Níveis Mínimos de Serviço.

3.2.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade ético-profissional da contratada pela perfeita execução da contratação, nem a responsabilidade pelos prejuízos resultantes da sua incorreta execução;

3.2.7. Condições gerais e específicas para a prestação do serviço:

- a) O prazo de execução dos serviços de Link Internet Trânsito (LIT) referentes ao Lote 02 é de 48 (quarenta e oito) meses. A velocidade do Link Internet Trânsito (LIT) será inicialmente contratada em 2GB, podendo ser ampliada para 4GB, 6GB, 8GB ou 10GB a qualquer momento, conforme a necessidade da CONTRATADA, desde que não ultrapasse o valor máximo contratado para os serviços LIT.

#### 4. DO VALOR ESTIMADO DA CONTRATAÇÃO, CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA E DO BENEFÍCIO PREVISTO NA LEI COMPLEMENTAR Nº 123/2006.

##### 4.1. VALOR ESTIMADO DA CONTRATAÇÃO

4.1.1. O valor estimado mensal para a contratação é de **R\$ 26.474.800,81 (vinte e seis milhões, quatrocentos e setenta e quatro mil, oitocentos reais e oitenta e um centavos)**, perfazendo o valor estimado global de **R\$ 1.256.840.552,76 (um bilhão, duzentos e cinquenta e seis milhões, oitocentos e quarenta mil, quinhentos e cinquenta e dois reais e setenta e seis centavos)**, para 48 (quarenta e oito) meses, sendo assim distribuídos:

- a. Lote I (ampla concorrência) – R\$ 1.180.217.323,80 (um bilhão, cento e oitenta milhões, duzentos e dezessete mil, trezentos e vinte e três reais e oitenta centavos);
- b. Lote II (ampla concorrência) – Valor estimado total - R\$ 6.012.156,96 (seis milhões, doze mil, cento e cinquenta e seis reais e noventa e seis centavos);
- c. Lote III (ampla concorrência) – Valor estimado total - R\$ 70.611.072,00 (setenta milhões, seiscentos e onze mil e setenta e dois reais).

4.1.2 No preço total do objeto deverão estar inclusos todos os tributos (impostos, taxas e contribuições), sejam federais, estaduais e municipais, bem como frete, comissões, pessoal, embalagem, seguros, encargos sociais e trabalhistas, assim como demais insumos inerentes que incidam ou venham a incidir sobre o objeto, sejam de que naturezas forem, excetuando o tributo do ICMS (Imposto sobre Circulação de Mercadorias e Serviços), sendo a CONTRATANTE isenta desta contribuição, conforme DECRETO Nº 44.650, de 30 de junho de 2017 Art. 101. inciso IV;

4.1.3. Os preços finais unitários e totais propostos pelos LICITANTES não poderão ultrapassar o preço unitário e total estimado pela Administração, sob pena de desclassificação da proposta.

## 4.2. CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA

4.2.1 *Os recursos financeiros para fazer face às despesas da contratação do objeto desta licitação correrão por conta dos Órgãos ou Entidades (Órgãos Aderentes) que aderirem ao Contrato de Prestação de Serviços (Contrato-Mater) cujos Programas de Trabalho e Elementos de Despesas constarão nos respectivos termos de adesão e notas de empenho, observadas as condições estabelecidas no Edital, a saber:*

4.2.1.1 *As despesas decorrentes da instalação e operacionalização do Serviço Nova Rede Corporativa SEGURANÇA & CONECTIVIDADE, serão suportadas pelas DOTAÇÕES ORÇAMENTÁRIAS dos órgãos e entidades do Poder Executivo Estadual, no Elemento 3.3.90.39: Serviços de Terceiros – Pessoas Jurídicas, no elemento 3.3.90.39.27 para despesas relativas aos serviços despesas consumo de infraestrutura da rede, internet corporativa, serviço de operação, acesso dedicado; ou à conta das disponibilidades orçamentárias e financeiras das entidades que não dependem do Tesouro Estadual.:*

## 4.3 JUSTIFICATIVA PARA NÃO APLICAÇÃO DO BENEFÍCIO PREVISTO NA LEI COMPLEMENTAR Nº 123/2006

4.3.1. Em regra, contratação de serviços com itens ou lotes de valores estimados iguais ou inferiores a R\$ 80.000,00 (oitenta) mil reais devem ser objeto de licitações exclusivas para ME, EPP e MEI (cota exclusiva), nos termos do art. 48, inciso I, da LC nº 123/2006.

4.3.2 Considerando que o presente Termo de Referência não possui itens ou lotes de valor igual ou inferior a R\$ 80.000,00 (oitenta mil reais), a presente licitação não possui itens ou lotes exclusivo à participação de Microempresa (ME), Empresa de Pequeno Porte (EPP) ou Microempreendedor Individual (MEI).

## 5 DA LICITAÇÃO

### 5.1 MODALIDADE DE LICITAÇÃO, CRITÉRIO DE JULGAMENTO, REGIME DE EXECUÇÃO E MODO DE DISPUTA

5.1.1 A licitação será processada na modalidade **PREGÃO ELETRÔNICO**, tendo como critério de julgamento o **MENOR PREÇO POR LOTE**.

5.1.1.1 O objeto será executado por meio do regime de **EMPREITADA POR PREÇO UNITÁRIO**.

5.1.1.2 O modo de disputa a ser utilizado é o **ABERTO**.

5.1.1.3 A combinação dos parâmetros modalidade de licitação, critério de julgamento e modo de disputa descritos neste Termo de Referência se mostram adequadas e eficientes para seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, com base nas argumentações abaixo:

5.1.1.3.1 **Modalidade de Pregão Eletrônico com Critério de Menor Preço por Lote:** O **pregão eletrônico** visa garantir transparência, competitividade e eficiência, já que o ambiente eletrônico permite a participação de um número maior de fornecedores, independentemente da localização geográfica, ampliando a concorrência. Enquanto o critério de **menor preço por lote** visa a busca por uma contratação econômica e vantajosa para a administração pública, incentivando que fornecedores apresentem propostas competitivas para cada lote de serviço, o que gera uma maior eficiência orçamentária.

**Regime de Empreitada por Preço Unitário:** é indicada para serviços cuja quantidade exata de itens ou unidades necessárias ainda não está completamente definida. Esse modelo possibilita maior flexibilidade, pois o contratante paga apenas pelo quantitativo de serviços efetivamente executado, permitindo ajustes de acordo com a demanda real durante a execução do contrato. Esse regime reduz o risco financeiro e proporciona melhor controle sobre os gastos, evitando aditivos contratuais para cobrir diferenças nas quantidades executadas.

5.1.1.3.2 **Modo de Disputa Aberto:** proporciona maior transparência e competitividade ao processo, uma vez que todas as ofertas e lances dos fornecedores são visíveis em tempo real, o que estimula a competição saudável e a redução de preços. A administração pública se beneficia ao obter uma visão clara do processo de lances, promovendo um ambiente de igualdade e integridade, e incentivando os licitantes a apresentarem suas melhores propostas.

## 5.2 PROPOSTA

5.2.1 As propostas deverão ter validade de, **no mínimo, 180 (cento e oitenta) dias**, contados da data de abertura da sessão pública, independente de declaração da licitante.

### 5.2.2 CONDIÇÕES DA PROPOSTA

5.2.2.1 A licitante, quando declarada vencedora provisória em seu lote, deve apresentar a Proposta de Preço de acordo com o modelo presente em **ANEXO B - MODELO DE PROPOSTA** deste TR, respeitando os quantitativos estabelecidos e de acordo com as especificações contidas neste Termo de Referência;

5.2.2.2 A proposta comercial deverá estar acompanhada de:

5.2.2.2.1. Folders, catálogos e/ou prospectos técnicos dos produtos propostos, em português ou inglês, para fins de verificação da compatibilidade da solução apresentada com as especificações técnicas estabelecidas no Edital;

5.2.2.2.2. Documento contendo o detalhamento dos custos e a especificação dos produtos, softwares e serviços propostos - com os itens que compõem os lotes, fabricantes, modelos e códigos dos produtos - apresentando a matriz cruzada, quando couber, entre as especificações exigidas no termo de referência e a indicação da página do documento, folder, catálogo e/ou prospecto do fabricante onde se verifica a comprovação do atendimento; e,

5.2.2.3. A não apresentação dos documentos referidos nos itens 5.2.2.2.1 e 5.2.2.2.2 será causa de desclassificação da proposta do licitante, se não houver o saneamento hábil em sede de diligência.

### 5.2.3 DO DETALHAMENTO DOS ITENS DE SERVIÇOS DA PROPOSTA

5.2.3.1 A Licitante, quando declarada vencedora provisória em seu lote, deverá apresentar o detalhamento dos itens de serviços, contendo todos os recursos necessários à prestação dos serviços, bem como as marcas, modelos, topologias e fornecedores das soluções (hardware e software) indicados na Proposta, de forma a atender integralmente aos requisitos obrigatórios e às especificações detalhadas deste Termo de Referência;

5.2.3.1.1 Para os itens de serviços indicados explicitamente na seção 5.2.3.1.6 abaixo, deverá ser apresentada uma Matriz Cruzada. Esta matriz demonstrará a correspondência detalhada entre cada requisito exigido neste Termo de Referência (seja de hardware, software ou serviço) e sua respectiva comprovação em documentação oficial do fabricante/fornecedor (como manuais, catálogos, páginas da internet, entre outros).

5.2.3.1.2 A matriz cruzada deverá ser apresentada em formato de tabela, estabelecendo referência direta entre cada requisito deste Termo de Referência e a forma de atendimento pela solução proposta, contendo, no mínimo, os seguintes campos:

5.2.3.1.2.1 Item do TR

5.2.3.1.2.2 Especificação Exigida

5.2.3.1.2.3 Produto/Serviço

5.2.3.1.2.4 Fabricante/Modelo

5.2.3.1.2.5 Página de Referência no Documento

5.2.3.1.2.6 Empresa responsável pelo atendimento

5.2.3.1.3 Para fins de comprovação técnica, somente serão aceitos documentos oficiais do fabricante/fornecedor, publicados em seu domínio institucional e acessíveis a partir das páginas oficiais do produto ou do repositório oficial

de documentação do fabricante.

5.2.3.1.4 Não serão aceitos datasheets obtidos por links diretos não referenciados nas páginas oficiais do fabricante (links órfãos), URLs temporárias, arquivos enviados por e-mail ou hospedados fora do domínio institucional do fabricante/fornecedor, ainda que contenham marca/identidade visual do fabricante.

5.2.3.1.5 Havendo duas ou mais versões de datasheets oficial para o mesmo produto/modelo, com valores de desempenho ou funcionalidades divergentes, prevalecerão, para fins de julgamento, os valores mais restritivos (menores) e o menor escopo funcional dentre as versões encontradas, salvo se for comprovado que a versão mais restritiva seja uma versão descontinuada.

5.2.3.1.6 Os itens da tabela da matriz cruzada deverão estar diretamente vinculados a cada serviço, conforme os itens e subitens correspondentes deste Termo de Referência. O detalhamento da Proposta, em cada lote, deverá descrever claramente a solução adotada para:

#### **5.2.3.1.6.1 Lote 01**

5.2.3.1.6.1.1 ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO - Apresentar matriz cruzada para todos os serviços e recursos integrantes do Centro Integrado de Inteligência e Segurança Cibernética, com exceção do Serviço de disponibilização de ambiente de testes;

5.2.3.1.6.1.2 ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC) - Apresentar matriz cruzada para o Serviço de Comunicação Unificada;

5.2.3.1.6.1.3 ADENDO IV - SERVIÇO DE REDE SEM FIO - Apresentar matriz cruzada para os Serviços de Rede Sem Fio;

5.2.3.1.6.1.4 ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE - Apresentar matriz cruzada para os Serviços de Pontos de Voz Fixos e demais serviços e recursos integrantes desta solução, com exceção dos serviços de tráfego de voz e Serviço Adicional de Acesso SIP (SIP TRUNK);

5.2.3.1.6.1.5 ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER - Apresentar matriz cruzada para o serviço de Infraestrutura para Contact Center, com exceção dos serviços de Automações e Integrações - Consultoria Inicial e Implantação;

5.2.3.1.6.1.6 ADENDO III - SEGURANÇA DE REDE LOCAL - Apresentar matriz cruzada para o serviço de segurança de rede local;

5.2.3.1.6.1.7 ADENDO VI - SEGURANÇA DE DATACENTER - Apresentar matriz cruzada para o serviço de segurança de datacenter;

5.2.3.1.6.1.8 A CONTRATADA deverá apresentar desenho das soluções do ADENDO VI - SEGURANÇA DE DATACENTER, do ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO e ADENDO XI - INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM, mostrando sua integração, incluindo alta disponibilidade, para melhor visualização da proposta técnica da CONTRATADA, com indicação de correlação entre a solução apresentada na proposta (por meio de documentação oficial do fabricante) com os itens dos requisitos do Edital.

#### **5.2.3.1.6.2 Lote 02**

5.2.3.1.6.2.1 Apresentar topologia para os Links de Trânsito;

5.2.3.1.6.2.2 Apresentar matriz cruzada do serviço de proteção antiDDoS.

5.2.3.1.6.2.3 Deverá obrigatoriamente ser apresentada no detalhamento dos itens de serviços da Proposta Declaração da(s) licitante(s) informando o país/região/estado de seu mitigador (AntiDDoS), devendo esta localização atender às exigências da lei 12.965 de 23/04/2014 e regulamentada pelo decreto 8.771 de 11/05/2016;

### 5.3 REQUISITOS ESPECÍFICOS DE HABILITAÇÃO

#### 5.3.1 HABILITAÇÃO JURÍDICA

##### 5.3.1.1 LOTE 1 e LOTE 2

5.3.1.1.1. Termo de autorização expedido pela Agência Nacional de Telecomunicações (Anatel) para explorar o Serviço de Comunicação Multimídia - SCM, conforme estabelecido no Regulamento do Serviço de Comunicação Multimídia, conforme Resolução Anatel nº 777, de 28 de abril de 2025, com direito/Delegação/Autorização/Concessão/outorga de operação em Pernambuco.

5.3.1.1.2. No caso de formação de consórcio, as consorciadas que fornecerão os serviços de Conectividade deverão apresentar o Termo de autorização expedido pela Agência Nacional de Telecomunicações (Anatel) para explorar o Serviço de Comunicação Multimídia – SCM, conforme estabelecido no Regulamento do Serviço de Comunicação Multimídia, conforme Resolução Anatel nº 777, de 28 de abril de 2025.

5.3.1.1.2.1. Justifica-se esta exigência por tratar-se de prestação de serviços de telecomunicações regulamentadas pela ANATEL e exigida às empresas do setor de telecomunicações. Notória é a justificativa que a continuidade da prestação dos serviços deve sempre nortear a decisão do gestor público, cabendo a ele estabelecer regras e condições para proteger o estado de um desfecho que venha a gerar prejuízo ao erário público, para tal estabelece a obrigatoriedade de que quando em consórcio, todas estas empresas devem ser detentoras da outorga do SCM - Serviço Comunicação Multimídia.

#### 5.3.2 REQUISITOS DE QUALIFICAÇÃO TÉCNICA

5.3.2.1. A LICITANTE deverá comprovar aptidão para execução de serviços de complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação, ou ao item pertinente, mediante apresentação de atestados ou certidões de capacidade técnica emitidos por pessoa(s) jurídicas de direito público ou privado ou, quando aplicável, regularmente emitidos pelo conselho profissional competente, observadas as condições previstas neste Termo de Referência.

5.3.2.2. Para fins de comprovação da qualificação técnica, serão aceitos atestados emitidos em nome da própria LICITANTE, das empresas integrantes de consórcio formalmente constituído para participação neste certame, quando aplicável, ou de potencial subcontratado, exclusivamente nas hipóteses, limites e condições expressamente previstos neste Termo de Referência, nos termos do art. 67, §9º, da Lei nº 14.133/2021.

5.3.2.2.1. Não serão aceitos atestados emitidos em nome de empresas pertencentes ao mesmo grupo econômico que não integrem formalmente o consórcio participante da licitação, ressalvada a hipótese de apresentação de atestado de potencial subcontratado, quando expressamente admitida neste Termo de Referência.

5.3.2.2.2. Para a confirmação de informações contidas no(s) atestado(s) apresentado(s), poderá ser promovido diligência no intuito de esclarecer/complementar a instrução do processo, solicitando e obtendo cópias de contratos e outros documentos idôneos.

5.3.2.2.3. Será admitida, nos termos do art. 67, §9º da Lei nº 14.133/2021, a apresentação de atestados relativos a potencial subcontratado em relação à parcela do serviço de até 25% (vinte e cinco por cento), cuja subcontratação foi expressamente autorizada no presente termo de referência.

5.3.2.2.4. A apresentação de atestados de potencial subcontratado implicará a obrigatoriedade de sua efetiva contratação para execução das parcelas correspondentes, sendo vedada sua substituição sem prévia anuência da CONTRATANTE, mediante justificativa técnica devidamente fundamentada e reapresentação dos atestados.

5.3.2.3. Para fins de comprovação, os atestados/certidões devem dizer respeito a prestação dos serviços correlatos a cada lote:

#### 5.3.2.3.1. LOTE 01 - prestação de serviços de CONECTIVIDADE E SEGURANÇA

5.3.2.3.1.1 38.175 (trinta e oito mil cento e setenta e cinco) eventos por segundo de capacidade mínima de monitoramento e análise de eventos de segurança em um ambiente operacional;

5.3.2.3.1.2 1.221 (mil duzentos e vinte e um) gerenciamento de acessos à rede local (NAC);

5.3.2.3.1.3 611 (seiscentos e onze) fornecimentos e implantações de Solução unificada de segurança de rede de última milha (UTM);

5.3.2.3.1.4 2.513 (dois mil quinhentos e treze) pontos de voz (PVF);

5.3.2.3.1.5 1.289 (mil duzentos e oitenta e nove) pontos de rede sem fio interno ou externo (SRSF);

5.3.2.3.1.6 820 (oitocentos e vinte) circuitos com acesso do tipo banda larga, dedicado, satelital ou 5G FWA;

5.3.2.3.1.7 3.750 (três mil setecentos e cinquenta) itens de Solução de gerenciamento e monitoramento de ativos.

#### 5.3.2.3.2. LOTE 2 - prestação de serviços de CONECTIVIDADE DE DATACENTER

5.3.2.3.2.1 A LICITANTE deverá comprovar o fornecimento do Serviço de Internet Corporativa + AntiDDoS de no mínimo 1 (um) Gbps de Banda, sendo permitido a soma de no máximo 02 (dois) links, correspondendo a 50% da banda inicial a ser contratada, comprovando que ambas as infraestruturas de backbone disponibilizadas pela licitante possuam interligação direta a no mínimo 2 (dois) Sistemas Autônomos (AS - Autonomous Systems) distintos, conforme norma da RFC1930;

5.3.2.3.2.2. A LICITANTE deverá comprovar que está conectada diretamente a pelo menos um provedor de serviços de trânsito IP Internacional: Entenda-se por Provedor de Serviços de Trânsito Internacional aquele que se acha fora dos limites da jurisdição territorial brasileiro. A comprovação de que a empresa está conectada a uma fornecedora Internacional será feita através das ferramentas públicas, como bgp.he.net ou outra similar;

#### 5.3.2.3.3. LOTE 3 - prestação de serviços de AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS

5.3.2.3.3.1 A contratada deverá comprovar experiência prévia na prestação de **serviços de gestão de vulnerabilidades**, incluindo identificação, análise, priorização e mitigação de vulnerabilidades em ambientes tecnológicos. A comprovação deve ser realizada por meio de atestados de capacidade técnica emitidos por clientes que comprove a execução de serviços compatíveis em características com o objeto licitado, especialmente envolvendo ao menos 420 (quatrocentos e vinte) ativos de tecnologia da informação.

5.3.2.3.3.2 A contratada deverá comprovar que possui qualificação técnica e experiência prévia na execução de **serviços de análise forense digital**, contemplando a identificação, coleta, preservação, análise e apresentação de evidências digitais. A experiência deverá ser comprovada mediante atestados que evidenciem a execução de serviços compatíveis em características com o objeto licitado com carga horária acumulada igual ou superior a 677 (seiscentos e setenta e sete) horas realizadas a partir de 01/01/2020.

5.3.2.3.3.3 A contratada deverá comprovar experiência na realização de **serviços de testes de intrusão (Pentest)**, abrangendo a identificação e exploração de vulnerabilidades em redes, sistemas e aplicações, com emissão de relatórios detalhados dos riscos e recomendações. A comprovação deverá ser realizada por meio de atestados emitidos por clientes que demonstrem a execução de serviços compatíveis com o objeto licitado, abrangendo ao menos 24 (vinte e quatro) aplicações.

5.3.2.3.4 Será considerado compatível com a quantidade os atestados ou certidões que apresentarem, no mínimo os seguintes quantitativos e/ou percentuais das quantidades estimadas na licitação para cada lote, exigindo-se a comprovação cumulativa quando da classificação provisória em primeiro lugar em mais de um lote;

5.3.2.3.5. Para fins de aferição do percentual e/ou quantitativo mínimo relativo à qualificação técnica, em sendo obtido resultado cujo número possua casas decimais, deverá ser realizado arredondamento para o primeiro menor número inteiro.

5.3.2.3.6. Justifica-se o quantitativo fixado para fins de qualificação técnica, no que se refere à comprovação das quantidades a serem indicadas em atestados/certidões, por se tratar de contratação de alta complexidade tecnológica e operacional, envolvendo serviços críticos à segurança da informação, conectividade e continuidade das atividades institucionais dos órgãos da administração pública. Os quantitativos citados nos itens **5.3.2.3.1.**, **5.3.2.3.2** e **5.3.2.3.3.** asseguram que a licitante detém experiência compatível com a dimensão e os desafios da execução contratual, sem, contudo, restringir indevidamente a competitividade, em consonância com os princípios da razoabilidade e da proporcionalidade previstos na Lei nº 14.133/2021.

#### **5.3.2.4. Documentação Técnica exigida para cada Lote além dos atestados referenciados acima:**

##### **5.3.2.4.1. LOTE 02**

5.3.2.4.1.1. A LICITANTE deverá comprovar que o somatório das larguras de banda de seu backbone, considerando as conexões com Sistemas Autônomos (ASs) nacionais, resulta em capacidade mínima equivalente ao dobro da banda máxima a ser contratada, estabelecida em 20 (vinte) Gbps.

#### **5.3.2.5. A Capacitação Técnico-profissional consistirá em:**

##### **5.3.2.5.1. Para os LOTES 01 e 02**

5.3.2.5.1.1. A LICITANTE deverá indicar Responsável(eis) Técnico(s), em conformidade com o artigo 67 da Lei nº 14.133/2021, que permite a exigência de qualificação técnico-profissional para assegurar a capacidade técnica da licitante na execução contratual. Essa exigência também está respaldada pela Resolução nº 1.137/2023 do CONFEA, a qual estabelece a necessidade de vínculo direto entre o profissional e a empresa contratada para serviços técnicos especializados, garantindo o compromisso e a responsabilidade técnica necessários ao cumprimento do presente Termo de Referência.

5.3.2.5.1.1.1. **Para o LOTE 01**, o(s) Responsável(eis) técnico(s), pertencente(s) ao seu quadro permanente, na data prevista para entrega da proposta, incluindo suas qualificações, sendo exigido profissionais de nível superior, detentores de certidões de responsabilidade técnica de serviços técnicos especializados para implementação da infraestrutura de telecomunicação para acesso à Internet (ARTs/CAT) com registro emitido pelo CREA.

5.3.2.5.1.1.2. **Para o LOTE 02**, o(s) profissional(is) indicados devem possuir nível superior ou outro devidamente reconhecido pela entidade competente, detentor(es) de atestados de responsabilidade técnica por execução de Serviços de Comunicação Multimídia (SCM) de características semelhantes ao objeto da licitação, devidamente acompanhados da respectiva Certidão de Acervo Técnico (CAT) com registro no CREA e/ou CFT.

5.3.2.5.1.2. A comprovação de vinculação do profissional ao quadro da licitante poderá ser efetuada, no caso de empregado da licitante, por meio da Carteira de Trabalho e Previdência Social; no caso de sócio, através do contrato/estatuto social; no caso de prestador de serviços, mediante contrato escrito firmado com o licitante ou declaração de compromisso do profissional de vinculação futura, caso o licitante se sagre vencedor do certame.

5.3.2.5.1.3. No decorrer do contrato os profissionais de que trata esse item poderão ser substituídos por profissionais equivalentes ou superiores desde que haja anuência prévia do contratante.

#### 5.3.2.6. VISTORIA PRÉVIA

5.3.2.6.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, pois os LOTES 1 e 2 possuem itens de serviços que serão prestados localmente e endereços específicos incluindo a SEDE da ATI, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim.

5.3.2.6.2. A vistoria deverá ocorrer até o dia anterior à data da abertura do certame, no horário das 09:00 às 16:00, de segunda a sexta-feira, por representante legal da empresa participante ou responsável técnico, por meio de agendamento prévio, a ser realizado em dias úteis, no horário de 09:00 às 16:00hrs, com o setor GRC – Gerência de Rede e Conectividade pelo telefone (81) 3181-8100 ou por pelo e-mail comtectelematica@ati.pe.gov.br ou outro colaborador indicado pela GRC – Gerência de Rede Corporativa da ATI.

5.3.2.6.3. Durante a vistoria, a LICITANTE deverá observar, entre outros aspectos, o grau de dificuldade para execução dos serviços, diagnóstico dos requisitos necessários para prestação desses, não se admitindo, posteriormente, qualquer alegação de desconhecimento deles.

5.3.2.6.4. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia, de modo que seu agendamento não coincida com o agendamento de outros LICITANTES.

5.3.2.6.5. O LICITANTE deverá atestar, sob pena de inabilitação, que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação, conforme modelo de declaração constante no edital.

5.3.2.6.6. Caso a LICITANTE opte por não realizar a vistoria, deverá apresentar declaração formal assinada por seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação, conforme modelo de declaração constante no edital.

5.3.2.6.7. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

**5.3.3.** Conforme justificativas constantes na NOTA TÉCNICA - SAD - Comissão Técnica de Telemática - COMTEC - TELEMATICA - Nº 5/2025 (doc. SEI 67013492), uma mesma empresa, isoladamente, em consórcio ou por meio de empresas pertencentes ao mesmo grupo econômico, não poderá ser declarada vencedora simultaneamente dos LOTES 01 e 03 deste certame.

5.3.3.1. Caso a licitante seja classificada provisoriamente em primeiro lugar, **SIMULTANEAMENTE NOS LOTES 1 e 3**, caberá a Administração especificar, considerando a maior economia obtida em valores absolutos de cada lote, para o qual a licitante será habilitada.

#### 5.3.4 REQUISITOS DE QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

5.3.4.1 Os requisitos de qualificação econômico-financeira serão descritos no Edital da presente contratação.

5.3.4.2 **Patrimônio Líquido** OU **Capital Social** mínimo correspondente a 10% (dez por cento) do valor anual estimado para a contratação do respectivo lote, exigindo-se a comprovação cumulativa quando da classificação provisória em primeiro lugar em mais de um lote

5.3.4.3 **Quando** a participação na licitação de pessoas jurídicas organizadas em consórcio, este deve apresentar o somatório dos valores Capital Social ou Patrimônio Líquido Mínimo de cada consorciado, constituindo-se de um **acréscimo de 10 % (dez por cento)** sobre o valor exigido de licitante individual, não sendo tal acréscimo aplicável aos consórcios compostos, em sua totalidade, por microempresas e empresas de pequeno porte.

## 6. DO CONTRATO

### 6.1 PRAZO DE VIGÊNCIA CONTRATUAL E PRORROGAÇÃO

6.1.1 O prazo de vigência do contrato para os **LOTES 01, 02 e 03** é de 48 (quarenta e oito) meses, contados a partir da data de sua assinatura, prorrogável por 2 (dois) períodos iguais de 36 (trinta e seis), até o limite de 120 (cento e vinte) meses, na forma dos arts. 106 e 107 da Lei nº 14.133, de 2021, observadas as condições de vantajosidade, interesse público e disponibilidade orçamentária.

6.1.2 Os serviços dos **LOTES 01 e 02** são enquadrados como continuados tendo em vista que são essenciais para a operação ininterrupta e segura das atividades da administração pública, conforme descrito para os principais macro serviços listados a seguir:

6.1.2.1 **Serviço de Conectividade de Rede:** Este serviço é indispensável para a comunicação interna e externa da instituição, permitindo o acesso a sistemas administrativos, plataformas de atendimento ao público e comunicação entre setores e com outros órgãos públicos. A continuidade da conectividade é fundamental para que a administração possa desempenhar suas funções sem interrupções, uma vez que a falta de conectividade impacta diretamente a produtividade e a capacidade de resposta do órgão. Sendo assim, a execução constante e ininterrupta deste serviço é necessária para o pleno funcionamento das atividades institucionais.

6.1.2.2 **Serviço de Segurança Cibernética:** Em um cenário de crescente número de ameaças digitais, a segurança cibernética é um aspecto essencial para proteger dados e sistemas críticos do órgão, além de garantir a confidencialidade, integridade e disponibilidade das informações. A proteção contínua é necessária para evitar interrupções por ataques cibernéticos, minimizar riscos de vazamento de dados e atender às normativas de segurança da informação. Interrupções no serviço de segurança cibernética expõem o órgão a riscos de segurança significativos, justificando a necessidade de um contrato de execução continuada.

6.1.2.3 **Serviço de Rede sem Fio (Wi-Fi):** A rede Wi-Fi é fundamental para o funcionamento de dispositivos móveis e o atendimento de demandas específicas de comunicação em diferentes áreas do órgão. Esse serviço permite agilidade e flexibilidade nas operações, contribuindo para a eficiência dos processos. A descontinuidade no serviço de Wi-Fi poderia impactar negativamente a comunicação interna, o atendimento ao público e a utilização de ferramentas digitais, evidenciando a necessidade de um serviço que atenda a um regime continuado.

6.1.2.4 **Serviço de Telefonia Fixa:** A telefonia fixa ainda é um meio de comunicação essencial para a administração pública, especialmente em áreas de suporte, atendimento ao cidadão e comunicação institucional. Esse serviço deve estar continuamente disponível para garantir que o órgão mantenha seus canais de atendimento e comunicação com o público e outros órgãos governamentais. A descontinuidade no serviço de telefonia comprometeria o atendimento direto ao cidadão e a comunicação interna, o que justifica a necessidade de um contrato que garanta sua prestação contínua.

6.1.3 Os serviços do **LOTE 03** são enquadrados como serviços por demanda, tendo em vista que são atividades ou operações realizadas conforme a necessidade expressa do CONTRATANTE podendo ser prestado de forma contínua após contratação como são os casos dos **Serviços de Gestão de Vulnerabilidades** e o **Serviço de Análise de Segurança Ofensiva**, já os **Serviços de Testes de Intrusão** e o **Serviço Análise Forense** não possuem uma frequência fixa, atendendo a requisitos específicos e objetivos de cada solicitação.

6.1.3.1 **Serviços de Avaliação e Mitigação de Riscos Cibernéticos:** Conjunto de atividades em segurança ofensiva, voltadas para identificar, analisar e corrigir vulnerabilidades em redes, sistemas e aplicações, com o objetivo de antecipar e minimizar o impacto de possíveis ataques cibernéticos. Esses serviços incluem a simulação controlada de ataques (*Red Team*) para testar a resiliência dos controles de segurança, bem como a execução de análises forenses para investigar e compreender incidentes ocorridos, identificar sua origem, rastrear vetores de ataque e coletar evidências.

6.1.4 Portanto, dado o caráter essencial, a necessidade de execução contínua e os impactos negativos que a interrupção dos serviços causaria, justificamos o enquadramento do contrato de prestação de serviços de conectividade, segurança cibernética, rede Wi-Fi e telefonia fixa como serviços continuados.

6.1.5 O início da vigência da adesão está condicionada à assinatura do respectivo Termo pelos representantes do Contratante Principal, órgão Aderente e Contratada.

6.1.6 Os Termos de Adesão terão sua vigência subordinada à do Contrato Corporativo.

6.1.7 Haverá prorrogação automática da vigência dos Termos de Adesão quando da prorrogação do Contrato Corporativo condicionada sua eficácia ao apostilamento de empenhos correspondentes ao período prorrogado.

## 6.2 PRAZO PARA ASSINATURA DO CONTRATO OU RETIRADA DO INSTRUMENTO EQUIVALENTE

6.2.1 Após a homologação da licitação, a adjudicatária será convocada para assinatura do termo de contrato no prazo de **10 (dez) dias úteis**, contados a partir da convocação, sob pena de decair o direito à contratação.

6.2.1.1 Aplicar-se-á o prazo acima para a assinaturas dos termos aditivos ao Contrato Mater.

6.2.2 O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

6.2.3 Após a assinatura do Contrato Mater, a contratada deverá assinar os termos de adesão e seus aditivos no prazo de **5 (cinco) dias úteis**, a contar da convocação pela contratante.

## 6.3 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

6.3.1 Além das obrigações que serão dispostas na minuta do contrato anexa ao Edital da presente licitação, são requeridas as obrigações específicas dispostas no **ADENDO I - OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE**.

## 6.4 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

6.4.1 Além das obrigações que serão dispostas na minuta do contrato anexa ao Edital da presente licitação, são requeridas as obrigações específicas dispostas no **ADENDO I - OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE**.

## 6.5 DO PLANO DE ASSUNÇÃO

6.5.1 Considerando que o Governo do Estado de Pernambuco possui atualmente um serviço de rede convergente integrando dados, segurança e voz onde é necessário implementar um Plano de Assunção dos serviços em operação para a nova solução descrita neste Termo e seus adendos. Este plano visa assegurar a continuidade dos serviços prestados às unidades administrativas públicas, evitando qualquer interrupção das atividades atualmente atendidas.

6.5.2 O Plano de Assunção dos Serviços será estabelecido formalmente após a conclusão do processo licitatório e a assinatura do Contrato Mater. Este plano conterá todas as etapas de transição necessárias e deverá ser integralmente seguido pela CONTRATADA conforme estipulado.

6.5.3 O Plano de Assunção se aplica exclusivamente ao LOTE 01. Para os LOTE 02 e LOTE 03, deverão ser seguidos os prazos de entrega definidos no item **LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDE-REÇO E ENTREGA** de cada lote.

6.5.4 A CONTRATADA deverá, após a conclusão do processo licitatório e assinatura do Contrato Mater, submeter à Secretaria de Administração (SAD) e à Agência de Tecnologia da Informação (ATI) um cronograma detalhado de assunção dos serviços no prazo máximo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão das Ordem de Serviço (OS) de instalação do Centro Integrado de Inteligência e Segurança Cibernética – CIISC (Serviços e Soluções, Adendos VIII e IX). O prazo máximo para execução dos serviços deste cronograma não deverá superar 365 (trezentos e sessenta e cinco) dias corridos e deverão ser cumpridos os seguintes marcos:

6.5.4.1. O início do prazo de execução da assunção contará a partir da emissão das Ordem de Serviço (OS) de instalação do Centro Integrado de Inteligência e Segurança Cibernética – CIISC (Serviços e Soluções, Adendos VIII e IX);

6.5.4.2. O plano de assunção será considerado encerrado após 365 dias da emissão das OSs citadas acima do CIISC (Serviços e Soluções);

6.5.4.3. A CONTRATADA deverá concluir a entrega dos Serviços e Soluções do CIISC em até 90 dias corridos a partir da data de emissão das respectivas Ordens de Serviço (OS);

6.5.4.4. A CONTRATADA deverá realizar a migração dos Links de Acesso (LAs), Serviços de Rede Sem Fio (SRSFs) e Pontos de Voz (PVFs) da Região Metropolitana do Recife, que abrange 15 municípios, no prazo máximo de 210 dias corridos contados a partir da emissão das Ordens de Serviço (OSs) para a instalação dos Serviços e Soluções do CIISC;

6.6.4.5. A CONTRATADA deverá realizar a migração dos Links de Acesso (LAs), Serviços de Rede Sem Fio (SRSFs) e Pontos de Voz (PVFs) situados fora da Região Metropolitana do Recife (Interior) no prazo máximo de 365 dias corridos a partir da emissão da Ordem de Serviço (OS) para a instalação dos Serviços e Soluções do CIISC;

6.5.4.6. Os prazos não serão prorrogados devido a atrasos imputáveis à CONTRATADA. Em caso de atraso na entrega do CIISC, os demais prazos vinculados deverão ser cumpridos independentemente da conclusão dos Serviços e Soluções do CIISC;

6.5.4.7. Deve-se observar as seguintes situações quanto a emissão das OSs de migração por parte do CONTRATANTE aderente:

6.5.4.7.1. OSs Emitidas Após o Prazo de Assunção: Caso a OS seja emitida pelo CONTRATANTE ADERENTE após o término do período de assunção (365 dias), o prazo de entrega deverá seguir os especificados no **item LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA**, conforme cada serviço contratado;

6.5.4.7.2. OSs Emitidas Dentro do Prazo de Assunção: As OSs emitidas pela CONTRATANTE ADERENTE durante o prazo de assunção deverão seguir o maior prazo de entrega entre o prazo de Assunção e o prazo especificado no **item LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA**;

6.5.5 A CONTRATADA deve instalar e operacionalizar todos os serviços da Nova Rede Corporativa, conjuntamente com a CONTRATADA dos serviços ofertados na solução do PE-CONECTADO II, até a completa finalização da assunção de todos os serviços para Nova Rede Corporativa.

## 6.6 LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA

6.6.1. A CONTRATADA deverá atender nos prazos elencados na tabela abaixo, de **LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA**, os itens de serviços descritos neste Termo para nova Rede.

### LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA

#### LOTE 01

Seq.	Descrição do Serviço	Limites do tempo de Entrega (dias corridos)
ADENDO III - SEGURANÇA DE REDE LOCAL		
1	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1 e Tipo 2 <sup>(1)</sup>	Com LAP e LME: 30 dias Com LAT: 15 dias
2	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço	30
3	Solução para gerenciamento de acessos à rede local - NAC	30
ADENDO IV - SERVIÇO DE REDE SEM FIO		
4	Serviço de Rede Sem Fio Interno e Externo com Segurança <sup>(2)</sup> (Tempo do Serviço de fornecimento e implantação de Switch está incluso neste tempo)	Para PCSs que NÃO possuam o serviço: Até 30 dias.  Para PCSs que já possuam o serviço: Até 07 dias.
5	Site Survey do Serviço de Rede Sem Fio Interno e Externo com Segurança <sup>(2)</sup>	7
6	Serviço de Rede Sem Fio Temporário com Segurança (dispensado a realização do survey) <sup>(2)</sup>	15
7	Serviço de fornecimento e implantação de Switch <sup>(2)</sup>	Para PCSs que NÃO possuam o serviço: Até 30 dias.  Para PCSs que já possuam o serviço: Até 07 dias.
ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL		
8	Link de Acesso Permanente (LAP) - Tipo 1 e Tipo 2 <sup>(1)</sup>	Instalação: 30 dias Ampliação de banda (upgrade): 5 dias
9	Link Multitecnologia Especial (LME) - Tipo 1, Tipo 2 e Tipo 3 <sup>(1)</sup>	
10	Link Acesso Temporário (LAT) - Tipo 1, Tipo 2 e Tipo 3 <sup>(1)</sup>	15
ADENDO VI - SEGURANÇA DE DATACENTER		
11	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER	90
12	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço	
13	Solução de segurança de confiança zero - ZTNA	
14	Solução de proteção, detecção e resposta para servidores - EDR	
15	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR	
16	Solução para gerenciamento de acessos à rede datacenter - NAC	
17	Solução de segurança de identidade privilegiada - PAM	
18	Solução de filtro de mensagens indesejadas - ANTISPAM	
19	Solução de Filtro de Aplicações WEB - WAF	
ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO		

20	Solução de gerenciamento e monitoramento de ativos - ITAM	90
21	Solução de gerenciamento de identidade de acesso - IAM	
22	Solução de monitoramento e análise de eventos de segurança - SIEM	
23	Solução de automação de resposta a incidentes de segurança - SOAR	
24	Solução para guarda de LOGs	
25	Serviço de disponibilização de ambiente de testes	
26	Solução de gerenciamento de serviços de TI - ITSM	
ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA		
27	Serviço de resposta à incidentes de cibersegurança sob demanda	90
28	Serviço de análise de segurança de primeiro nível	
29	Serviço de análise de segurança especializada	
30	Serviço de acompanhamento de reparos	
31	Serviço de atenção especializada ao cliente	
32	Service Desk	
33	Serviço de operação da rede	
34	Serviço de análise de qualidade	
35	Serviço de Coordenação do CIISC	
36	Núcleo de Redes e Segurança Setorial	
37	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setori- al (pacotes 50 PCSs)	
38	Serviço de Evolução da Maturidade em Segurança da Informação	
ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)		
39	Serviço de Comunicação Unificada - SCU (Conta de usuário)	10
ADENDO XIII – SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE		
40	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)	Até 50 PVFs: 20 dias  Acrescido 1 dia útil a cada 50 Pontos.
41	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	
42	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	
43	Serviço de Ponto de Voz Fixo com Aparelho de Voz DECT IP (PVF-DECT IP)	
44	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)	
45	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)	
46	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)	
47	Serviço PVF-Fone-de-Cabeça	

48	Serviço Tráfego Telefônico Extrarede Reverso, do tipo DISCAGEM DIRETA GRATUITA (DDG)	15
49	Serviço Adicional de Acesso SIP (SIP TRUNK)	15
<b>ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER</b>		
50	Serviço de Contact Center com Recurso de Voz	30
51	Serviço de Contact Center com recurso de Whatsapp	30
52	Serviço de Contact Center com recurso de Redes Sociais	30
53	Serviço de Unidade de Resposta Audível (Porta de URA)	30
54	Serviço de Comunicação por vídeo ou vídeo-chamada	30
55	Serviço de Automatizações e Integrações - Consultoria Inicial	10
56	Serviço de Automatizações e Integrações - Implantação	60
<b>ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO</b>		
57	Suporte de Manutenção (12h x 7d)	1
58	Suporte de Manutenção (24h x 7d)	1

**Nota (1):** Os tempos limites para preparação, instalação, homologação, mudança de endereço e entrega dos serviços de Solução Unificada de Segurança de Rede (UTM) e conectividade (LAs) deverão ser únicos e vinculados, considerando sua interdependência operacional. Essa regra se aplica aos seguintes serviços:

- Serviço de fornecimento e implantação de Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 e Tipo 2;
- Link de Acesso Permanente (LAP) – Tipo 1 e Tipo 2;
- Link Multitecnologia Especial (LME) – Tipo 1, Tipo 2 e Tipo 3;
- Link de Acesso Temporário (LAT) – Tipo 1, Tipo 2 e Tipo 3.

Dessa forma, qualquer alteração, instalação ou mudança que envolva mais de um desses serviços deverá ser tratada como um único evento, respeitando os prazos máximos estabelecidos para sua ativação.

Em caso de descumprimento dos prazos, as penalidades e glosas serão aplicadas a todos os itens impactados, conforme as regras contratuais.

**Nota (2):** O tempo de fornecimento e implantação do Switch para o Serviço de Rede Sem Fio deverá ser sempre contabilizado dentro dos prazos estabelecidos para os seguintes itens de serviço:

- Serviço de Rede Sem Fio Interno e Externo com Segurança;
- Site Survey do Serviço de Rede Sem Fio Interno e Externo com Segurança (quando aplicável);
- Serviço de Rede Sem Fio Temporário com Segurança (quando aplicável).

Em caso de descumprimento dos prazos, as penalidades e glosas serão aplicadas a todos os itens impactados, conforme as regras contratuais.

**LOTE 02**

Seq.	Descrição do Serviço	Limites do tempo de Entrega (dias corridos)
<b>ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER</b>		
1	Link de Fibra Lan To Lan 100GB (L2L)	60
2	Link para Data Center de 2GB, 4GB, 6GB, 8GB e 10 GB com AntiDDoS - Link Internet Trânsito (LIT)	Instalação: 60 dias Ampliação de banda (upgrade): 5 dias

<b>LOTE 03</b>		
Seq.	Descrição do Serviço	Limites do tempo de Entrega (dias corridos)
<b>ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS</b>		
1	Serviço de gestão de vulnerabilidades	30
2	Serviço de análise forense	30
3	Serviço de análise de segurança ofensiva (Red Team)	30
4	Serviço de testes de intrusão (Pentest)	30

6.6.2. Considera-se como Ordem de Serviço (OS) válida para início da contagem de tempo de entrega dos itens de serviço da nova Rede, a emissão da OS por parte da CONTRATANTE.

## 6.7 MUDANÇA DE ENDEREÇO

6.7.1 A CONTRATANTE poderá solicitar, via Ordem de Serviço, a mudança de endereço dos serviços instalados em um PCS. Os prazos para realização desta atividade e disponibilização de todos os serviços de forma plena serão iguais aos prazos da tabela “**LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA**” de cada serviço envolvido.

6.7.2 Apenas serão consideradas como mudança de endereço dos serviços da instalados em um PCS, quando o logradouro de origem, estiver localizado no mesmo município do logradouro de destino, para onde serão reinstalados estes serviços.

## 6.8 RETIRADA DE SERVIÇOS

6.8.1 A retirada do(s) serviço(s), consiste na sua total desinstalação, retirada dos equipamentos e suspensão de cobrança do(s) referido(s) serviço(s). Para efeito do cumprimento do prazo de atendimento da retirada de serviço, será suficiente a interrupção da cobrança do valor do serviço retirado, cuja data de interrupção da cobrança será considerada a data da retirada.

6.8.2 A CONTRATANTE aderente não será responsabilizada por equipamentos que não forem coletados pela CONTRATADA em até 30 (trinta) dias da data da emissão da Ordem de Serviço de retirada.

6.8.3 O prazo máximo para a retirada de todos os serviços é de até 5 (cinco) dias, após a emissão da Ordem de Serviço.

6.8.4 Será concedido um período de carência mínima de 6 (seis) meses para qualquer item de serviço dos LOTES 1 e 2, exceto para serviços temporários, contados a partir da data de ativação do serviço. Durante o período de carência, não será permitida a solicitação de retirada do serviço.

## 6.9 PREVISÃO E CONDIÇÕES DE PRESTAÇÃO DA GARANTIA CONTRATUAL

6.9.1 A CONTRATADA prestará garantia de execução contratual, no percentual de **5% (cinco por cento) do valor anual do contrato**, nos termos dos artigos 96 a 98 da Lei nº 14.133, de 2021.

6.9.2 As demais disposições sobre o tema serão detalhadas na minuta do contrato, anexo do Edital do presente certame.

## 6.10 DA PREVISÃO DE SUBCONTRATAÇÃO

6.10.1. Será permitida a subcontratação de parte do objeto ou de atividades acessórias e complementares, desde que isso não comprometa a economicidade ou a qualidade do serviço.

6.10.2. Entende-se como atividade acessória ou complementar aquelas atividades de apoio para montagem, manutenção, transporte do item de serviço. A subcontratação não exime a CONTRATADA de suas responsabilidades, devendo ser observadas a qualidade, a fidelidade ao objeto e a garantia da totalidade dos serviços prestados. Cabe ainda à CONTRATADA supervisionar e coordenar adequadamente essas atividades;

6.10.3. **Para o LOTE 1, será permitida a subcontratação de até 25% (vinte e cinco por cento) do valor total do contrato.**

6.10.3.1. **NÃO será permitida a subcontratação do Serviço CIISC – Centro Integrado de Inteligência e Segurança Cibernética (serviços do ADENDO IX)**, exceto para o **serviço de acompanhamento de reparos**, que poderá ser subcontratado. A subcontratação das demais atividades relacionadas ao CIISC não se mostra técnica nem economicamente vantajosa para a Administração Pública, permanecendo vedada.

6.10.4. **Para o LOTE 2, será permitida a subcontratação de até 50% (cinquenta por cento) do valor total do contrato**, da parcela do objeto do presente certame correspondente à execução de serviços técnicos especializados de configuração, monitoramento e mitigação de ataques Anti-DDoS, garantia de alta disponibilidade, resiliência operacional e redundância de acesso à internet, por meio de rotas, sistemas autônomos (AS) e estações geograficamente distintas, tendo em vista que se trata de aspectos técnicos específicos do serviço, cuja adequada implementação é determinante para a continuidade dos serviços críticos da Administração Pública, conforme detalhado na Nota Técnica 5 (SEI nº 83630624) e os subitens 6.10.4.1 e 6.10.4.2.

6.10.4.1. Será permitida a subcontratação de outro provedor para a prestação do serviço de Solução de Internet Corporativa com Proteção Anti-DDoS em alta disponibilidade. Esta subcontratação se justifica por ser tecnicamente vantajosa e benéfica para a Administração Pública.

6.10.4.2. Será permitida a subcontratação de um AS (Autonomous Systems) para fornecimento do segundo link internet com dupla abordagem, sem que isso implique transferência da prestação do serviço contratado, em perda de economicidade ou em detrimento de sua qualidade;

6.10.5. **Para o LOTE 3**, será permitida a subcontratação do objeto do presente certame, tendo em vista que se trata de aspectos técnicos específicos do serviço, **até o limite de 25% (vinte e cinco por cento) do valor total do contrato**.

6.10.6. A subcontratação do objeto principal fica condicionada à expressa anuência da CONTRATANTE PRINCIPAL.

6.10.7. Não se caracteriza como subcontratação a utilização, pela CONTRATADA, de redes, circuitos, postes, dutos, fibras ópticas, enlaces, infraestrutura passiva ou ativa pertencentes a outras prestadoras de serviços de telecomunicações, quando admitido pela legislação setorial vigente, especialmente nos termos da Lei nº 9.472/1997 (Lei Geral de Telecomunicações) e da regulamentação expedida pela ANATEL.

6.10.8. A subcontratação não exime a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados, cabendo-lhe também a devida supervisão e coordenação dessas atividades.

## 6.11 MODELO DE GESTÃO DO CONTRATO

6.11.1 As obrigações dos agentes responsáveis pela gestão e fiscalização da presente contratação estão detalhadas no Decreto Estadual nº 51.651/2021, bem como, serão dispostas na minuta do contrato, anexo ao Edital deste certame.

6.11.2 A comunicação entre a Contratante e a Contratada se dará por meio do Preposto Indicado pela Contratada Através de mensagem eletrônica via e-mail, sem prejuízo de outros meios disponíveis.

6.11.3 A contratada deverá apresentar a Nota Fiscal ou fatura para atesto da Administração nos endereços dos CONTRATANTES ADERENTES.

6.11.4 A gestão do contrato ficará a cargo da Contratante do Contrato Mater (SAD) e dos CONTRATANTES ADERENTES dos seus contratos específicos.

6.11.5 A Fiscalização do Contrato Mater ficará a cargo da (SAD), e a Fiscalização dos Contratos dos CONTRATANTES ADERENTES ficará a cargo dos Gestores de Telemática dos Órgãos CONTRATANTES ADERENTES.

6.11.6 A Contratada deverá manter um Preposto em todo período do contrato, para ser o contato entre a contratada e a Contratante Mater e os Órgãos CONTRATANTES ADERENTES, para tratar sobre qualquer eventualidade sobre a execução do Contratos e dos itens do Termo de Referência.

## 7 DOS CRITÉRIOS E PRAZOS PARA PAGAMENTO

7.1 As disposições sobre o tema serão detalhadas na minuta do contrato, anexo do Edital do presente certame.

## 8 DOS INSTRUMENTOS DE MEDIÇÃO DE RESULTADOS

8.1 O Instrumento de Medição dos Resultados é o mecanismo que define, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento.

8.2 Os indicadores descritos no **ADENDO II - NÍVEIS MÍNIMOS DE SERVIÇO** serão utilizados para avaliação dos serviços prestados, conforme constante nos Níveis Mínimos de Serviço.

8.3 O pagamento poderá ser parcialmente glosado, de acordo com os indicadores descritos no **ADENDO II - NÍVEIS MÍNIMOS DE SERVIÇO** quando a CONTRATADA não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas ou quando deixar de utilizar materiais e recursos huma-

nos exigidos para a execução do serviço, ou, ainda, quando os utilizar com qualidade ou quantidade inferior à demandada.

8.4 Após a conferência dos quantitativos e valores apresentados, a CONTRATANTE, através do fiscal do CONTRATO, atestará a medição mensal comunicando à CONTRATADA o valor aprovado e autorizando a emissão da correspondente Nota fiscal ou documento de cobrança equivalente.

## 9 DAS SANÇÕES GERAIS E ESPECÍFICAS

### 9.1 SANÇÕES A SEREM APLICADAS NA FASE DE LICITAÇÃO

9.1.1 As disposições sobre sanções administrativas aplicáveis durante a licitação e aquelas praticadas no período situado entre a adjudicação e a assinatura do instrumento contratual serão previstas no Edital do presente certame.

### 9.2 SANÇÕES A SEREM APLICADAS DURANTE A CONTRATAÇÃO

9.2.1. Além das sanções previstas na minuta do contrato, são requeridas as seguintes sanções específicas na presente contratação:

I. Advertência;

a) Será aplicável a sanção de advertência quando a CONTRATADA descumprir deveres instrumentais ou der causa à inexecução parcial do CONTRATO que não acarrete dano à Administração e que não justifique a imposição de penalidade mais grave, em especial pelo descumprimento das obrigações previstas no Termo de Referência;

II. Multa, de acordo com as seguintes regras:

a) Pelo atraso na entrega do Plano de Assunção ou de Ordens de Serviço, cujos prazos previstos estão na tabela LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA deste Termo, multa de 3% (três por cento) do valor do referido serviço, por dia decorrido;

## ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A - ESTUDO TÉCNICO PRELIMINAR (ETP) (85887625)

ANEXO B - MODELO DE PROPOSTA (82202421)

ANEXO C - SITES GOVERNAMENTAIS COM LINKS INSTALADO (82245312)

ANEXO D - QUANTITATIVO DE TRAFÉGO EXTRARREDE E ESPECIFICAÇÕES TÉCNICAS PARA DIMENSIONAMENTO DE SOLUÇÃO DE VOZ EM CLOUD (63307901)

ANEXO E - MATRIZ DE RISCOS (76511527)

ANEXO F - ARQUITETURA E TOPOLOGIA DO SISTEMA SISTEMA DE GESTÃO DE ORDEM DE SERVIÇO (SGOS) (83454823)

## ADENDOS DO TERMO DE REFERÊNCIA

ADENDO I - OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE (81234512)

ADENDO II - NÍVEIS MÍNIMOS DE SERVIÇO (82680045)

ADENDO III - SEGURANÇA DE REDE LOCAL (81140873)

ADENDO IV - SERVIÇO DE REDE SEM FIO (SRSF) MODALIDADE INTERNO (INDOOR) E EXTERNO (OUTDOOR) (81869033)

ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL (84508855)

ADENDO VI - SEGURANÇA DE DATACENTER (81150718)

ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER (82021304)

ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO (84469512)

ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA DA NOVA REDE CORPORATIVA (81592361)

ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS (67492772)

ADENDO XI - INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM (81435047)

ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC) (74784614)

ADENDO XIII – SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE (84377531)

ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER (84668874)

ADENDO XV – GESTÃO DO PROJETO, SERVIÇOS, CONTINUIDADE E RESPOSTA A INCIDENTES (66905646)

ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO DOS SERVIÇOS (68946172)

Recife, data da assinatura digital.

---

FREDERICO DE VASCONCELOS PEREIRA

Presidente da ATI

Matrícula: 18187714/02

Observação: Este Termo de Referência foi elaborado de acordo com os instrumentos padronizados da PGE: Edital de Serviço (Atualizado em 25/06/2024), Minuta do Contrato de Serviço (Atualizada em 16/05/2024) e Minuta da Ata de Registro de Preços (Atualizada em 04/06/2024).

DATA DE VERSÃO DO TR SAD 30/07/2024

**ANEXO A - ESTUDO TÉCNICO PRELIMINAR (ETP)**

**ESTUDO TÉCNICO PRELIMINAR (ETP) DE TIC**

**Planejamento de Contratações de Soluções de TIC**

**Licitação**

**Processo Administrativo nº SEI 0001200180.000817/2023-36**

**Nova Rede Corporativa Segurança e Conectividade**

**Histórico de Revisões**

Data	Versão	Descrição	Autor
09/01/2024	0.1	Primeira versão do documento	Wesley Melo
16/04/2024	0.2	Segunda versão do documento	Samara Brych
05/06/2024	0.3	Terceira versão do documento	Leandro Silveira
07/06/2024	0.4	Quarta versão documento	Jeová Barros
16/08/2024	0.5	Quinta versão do documento	Samara Brych
26/08/2024	0.6	Sexta versão do documento	Wesley Melo / Samara Brych / Navarro Júnior
03/09/2024	0.7	Sétima versão do documento	Samara Brych / Navarro Júnior
30/10/2024	0.8	Revisão	Navarro Júnior / Samara Brych
08/11/2024	1.0	Revisão Final	Ítalo Sivini / Joseilson França
20/05/2025	1.1	Atualização e justificativa das quantidades	Navarro Júnior
11/09/2025	1.2	Atualização e justificativa das quantidades	Samara Brych
07/11/2025	1.3	Atualização e justificativa das quantidades	Navarro Júnior/ Samara Brych
14/04/2026	1.4	Atualização de justificativas	Italo Sivini/ Navarro

**ESTUDO TÉCNICO PRELIMINAR DE TIC**

**1. PREÂMBULO**

Este Estudo Técnico Preliminar (ETP) é o documento inicial e fundamental no planejamento de contratação de uma nova rede corporativa para o Governo de Pernambuco. Ele tem como objetivo identificar e analisar as soluções mais adequadas para atender às necessidades registradas no Documento de Formalização da Demanda (DFD), demonstrando a viabilidade técnica e econômica das opções levantadas. Além disso, este estudo se preocupa em assegurar que todas as soluções consideradas atendam aos mais elevados padrões de proteção e segurança da informação, essenciais para a preservação da integridade dos dados e da privacidade dos cidadãos. Através deste estudo, busca-se garantir que a decisão pela continuidade do processo de contratação seja embasada em critérios sólidos e alinhados com o interesse público.

Em um contexto onde a internet se tornou essencial para a governança moderna, o Governo de Pernambuco reconhece a importância de uma infraestrutura digital robusta e segura. Esta rede corporativa é crucial para sustentar o Governo Digital, assegurando que os serviços públicos estejam disponíveis de forma segura, protegendo informações sensíveis contra ameaças cibernéticas e garantindo a eficiência no atendimento aos cidadãos.

Este ETP não apenas orienta a elaboração do Termo de Referência (TR) e outros artefatos necessários ao processo licitatório, mas também reflete o compromisso do Governo de Pernambuco com a inovação contínua e a proteção dos dados. A substituição da atual rede PE-CONECTADO por uma nova rede de telemática exemplifica a busca por soluções que possam se adaptar rapidamente às novas tecnologias, garantindo a segurança da informação, a transparência e a eficiência dos serviços digitais prestados.

Elaborado em colaboração entre representantes das áreas técnica e requisitante, este estudo incorpora uma visão multidisciplinar, contemplando todas as facetas da contratação proposta. Com isso, o Governo de Pernambuco reafirma seu compromisso com o desenvolvimento sustentável, a inclusão digital e a melhoria contínua dos serviços públicos, promovendo um ambiente de confiança e transparência com a população, onde a segurança da informação é um pilar central na proteção dos dados e na garantia de serviços confiáveis.

#### Fundamentação:

- Art. 6º, XX, da Lei nº 14.133, de 01 de abril de 2021;
- Lei nº 14.804, de 29 de outubro de 2012;
- Art. 6º, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Art. 7º, §§ 3º, 4º, 5º, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Art. 9º, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Art. 2º, XII, da Portaria ATI nº 15 de 31 de março de 2023;

## 2. DESCRIÇÃO DA NECESSIDADE

### 2.1. Qual é o problema que se pretende resolver?

O problema central a ser resolvido é a insuficiência da atual infraestrutura de conectividade e cibersegurança dos órgãos públicos do Estado de Pernambuco. Com o crescente volume de dados trafegados nas redes governamentais e a sofisticação das ameaças cibernéticas, a infraestrutura existente mostra-se inadequada para garantir a segurança, a eficiência e a disponibilidade contínua dos serviços públicos. Essa deficiência expõe o estado a riscos significativos, como vazamento de dados sensíveis, interrupções nos serviços essenciais, e a vulnerabilidade a ciberataques que podem comprometer a integridade das operações governamentais.

## 2.2. Quais são os atores interessados na solução desse problema e quais as perspectivas desses atores sobre o problema?

Os principais atores interessados na solução deste problema incluem:

- **Órgãos Públicos Estaduais:** Os gestores e funcionários desses órgãos dependem de uma infraestrutura de rede robusta e segura para executar suas funções diárias e prestar serviços à população. Sua perspectiva é que a melhoria na conectividade e na cibersegurança resultará em maior eficiência operacional e redução de riscos.
- **Cidadãos:** Como principais beneficiários dos serviços públicos, os cidadãos esperam um serviço contínuo, seguro e acessível, incluindo o acesso à internet pública. Eles veem a melhoria na infraestrutura como uma forma de garantir seus direitos digitais, proteção de seus dados pessoais, e maior inclusão digital.
- **Governo do Estado de Pernambuco:** O governo tem o interesse de modernizar suas operações e assegurar a continuidade e a segurança dos serviços públicos, além de fortalecer sua posição como um estado inovador em termos de políticas digitais e de segurança cibernética.
- **Empresas Privadas e Fornecedores de Tecnologia:** Envolvidas diretamente na execução dos serviços e fornecimento das soluções tecnológicas, essas empresas têm o interesse de colaborar em um ambiente que valorize a segurança, a inovação e a eficiência.

## 2.3. Qual é o interesse público a ser atendido?

O interesse público a ser atendido envolve a proteção dos dados pessoais e das informações sensíveis da administração pública, a continuidade e eficiência dos serviços públicos, e a promoção da inclusão digital. Ao assegurar que os sistemas de comunicação do governo sejam resilientes contra ciberameaças, o Estado de Pernambuco estará garantindo que a população tenha acesso confiável e seguro aos serviços públicos, ao mesmo tempo que protege o patrimônio digital do estado.

## 2.4. Quais os resultados e os benefícios que serão alcançados ao resolvê-lo?

Os resultados e benefícios esperados com a solução deste problema incluem:

- **Aumento da Segurança Cibernética:** Redução significativa das vulnerabilidades a ciberataques, o que protegerá os dados sensíveis da administração pública e dos cidadãos, além de garantir a integridade dos sistemas governamentais.
- **Melhoria na Eficiência Operacional:** A modernização da infraestrutura de conectividade permitirá que os órgãos públicos operem de maneira mais eficiente, com menor risco de interrupções e maior velocidade na comunicação interna e externa.
- **Maior Inclusão Digital:** Com a expansão de pontos de Wi-Fi gratuitos e uma infraestrutura de rede mais robusta, mais cidadãos terão acesso à internet, o que promove a inclusão digital e facilita o acesso a serviços e informações online.
- **Fortalecimento da Confiança Pública:** Ao investir em segurança cibernética e na modernização da infraestrutura, o governo de Pernambuco demonstrará seu compromisso com a proteção dos dados e a melhoria dos serviços, aumentando a confiança da população nas instituições públicas.
- **Fomento à Inovação:** A contratação permitirá que o estado continue a inovar em suas operações digitais, adotando novas tecnologias que podem transformar a forma como os serviços públicos são prestados.

### Fundamentação:

- Art. 18º, § 1º c/c § 2º, inciso I, da Lei nº 14.133, de 01 de abril de 2021;

- Art. 8º, inciso I, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;

### 3. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A secretária de administração, no uso das atribuições sob a PORTARIA SAD N° 2.934 DO DIA 04 DE JULHO DE 2023:

Identificação da Área requisitante	Nome do responsável
SAD	Ana Maraíza Sousa Silva

Considerando a competência institucional da Secretaria de Administração, conforme previsto no Decreto nº 42.907, de 13 de abril de 2016, que dispõe sobre a gestão e o uso dos serviços de telemática do âmbito do Poder Executivo Estadual;

Considerando a indispensabilidade de iniciar os estudos e os procedimentos decorrentes para a contratação dos serviços de telemática, com a especificação técnica precisa, clara e suficiente para subsidiar sua aquisição, de modo a atender as necessidades da Administração Pública em termos de qualidade, eficiência e economicidade, a qual permitirá a continuidade dos serviços de informática fornecidos através de rede de telecomunicações; RE-SOLVE:

Art. 1º Designar os membros abaixo relacionados para compor a Comissão Técnica da Rede Corporativa de Telemática, sob a coordenação conjunta do primeiro e do segundo:

Identificação da Área técnica	Nome do responsável
SAD	Joseilson Albuquerque de França
ATI	Ítalo Fernando Vasconcelos Sivini Filho
ATI	Jeová Menezes de Barros
ATI	Wesley Davison Braga Melo
SAD	Henrique Sales de Oliveira
SAD	Isabele Carolina Pessoa Martins
SECTI	Leandro José da Silveira

#### Fundamentação:

- Art. 4º, § 5, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Art. 13º, da Portaria ATI nº 15 de 31 de março de 2023;

### 4. ALINHAMENTO DA CONTRATAÇÃO COM O PLANEJAMENTO DO ÓRGÃO/ENTIDADE

## INTRODUÇÃO À CONECTIVIDADE CORPORATIVA, CIBERSEGURANÇA E POLÍTICAS PÚBLICAS

A conectividade corporativa e a cibersegurança são fundamentais no cenário contemporâneo, onde a digitalização transforma profundamente as operações governamentais e empresariais. Este é um desafio reconhecido mesmo antes da pandemia global, que exige das equipes executivas proteger suas instituições de ciberataques sem prejudicar a inovação e a capacidade de gerar valor a partir de investimentos tecnológicos (MCKINSEY & COMPANY, 2021a).

A infraestrutura de redes não apenas facilita a comunicação e a troca de dados, mas também sustenta o desenvolvimento socioeconômico e a eficiência administrativa (WORLD BANK BLOGS, 2021 e MCKINSEY & COMPANY, 2021b) tornando-se um pilar essencial para a governança moderna e a prestação de serviços públicos. A World Bank destaca que os investimentos em infraestrutura, como energia, telecomunicações e redes de transporte, têm um impacto direto no crescimento, pois são insumos essenciais na produção de bens e serviços. Eles também podem reduzir custos, facilitar a mobilidade física de pessoas e produtos, remover restrições de produtividade e aumentar a competitividade. Além disso, a disponibilidade de internet de linha fixa, mesmo em velocidades básicas, tem um impacto forte no crescimento econômico local, como mostrado na África Subsaariana.

A McKinsey também ressalta a importância de se considerar os efeitos em rede ao selecionar projetos de infraestrutura, pois isso pode levar a benefícios mais amplos, especialmente em redes em desenvolvimento, como as de transporte ou energia. Além disso, o alinhamento e a coordenação de investimentos em infraestrutura podem levar a benefícios sociais e econômicos mais inclusivos.

No Estado de Pernambuco, a iniciativa PE-CONECTADO exemplifica o esforço para superar desafios de conectividade e segurança através de soluções inovadoras. O PE-Conectado II é uma iniciativa do governo de Pernambuco que visa melhorar a infraestrutura de telecomunicações do estado. O objetivo do programa é fornecer uma rede mais robusta e segura, que possa apoiar os órgãos públicos estaduais, melhorando assim a prestação de serviços ao cidadão. Além disso, o PE-Conectado buscou fomentar a expansão do acesso à internet por meio de pontos de WiFi gratuitos, que são uma parte importante da estratégia de inclusão digital do governo. Esses pontos permitiriam que os cidadãos acessem a internet em locais públicos, facilitando o acesso à informação e a serviços online.

A implementação do PE-Conectado II foi um passo significativo em direção ao avanço tecnológico e ao desenvolvimento econômico do estado, pois uma infraestrutura de comunicações eficiente é fundamental para o crescimento em diversas áreas, incluindo educação, saúde e negócios.

Sobre parcerias público-privadas (PPPs), várias fontes destacam a importância e eficácia das PPPs em contextos similares. A McKinsey & Company argumenta que, ao definir um nível ótimo de participação do setor privado e transferência de risco, é possível concluir mais projetos no prazo e dentro do orçamento, maximizando o uso de recursos governamentais e beneficiando a sociedade em geral. Essa abordagem de gerenciamento de risco é crucial para o sucesso de projetos de infraestrutura complexos e pode ajudar a alinhar as capacidades de gerenciamento de risco do setor privado com as necessidades do setor público (MCKINSEY & COMPANY, 2021c). Além disso, de acordo com o Blackridge Research & Consulting, os contratos de PPP geralmente têm duração de 20 a 30 anos ou mais, com financiamento parcial fornecido pelo setor privado, enquanto pagamentos são esperados pelo setor público e/ou clientes ao longo do projeto. Isso permite que o setor privado assuma a responsabilidade pelo planejamento, design, implementação e financiamento do projeto, enquanto o parceiro público define e supervisiona a conformidade do projeto, garantindo que as aprovações regulatórias sejam atendidas. Este modelo de

PPP pode ser ajustado para alcançar o desenvolvimento sustentável de instalações públicas, abordando necessidades financeiras e garantindo eficiência, disponibilidade, qualidade, desempenho e segurança ambiental (BLACKRIDGE RESEARCH & CONSULTING, 2022).

A governança e as políticas públicas desempenham um papel fundamental na criação de um ambiente digital seguro, estabelecendo padrões de segurança, promovendo práticas responsáveis e protegendo contra ameaças cibernéticas. Uma estratégia nacional de cibersegurança abrangente, conforme identificado por mais de 100 governos, geralmente inclui elementos como uma agência nacional dedicada à cibersegurança, um programa de proteção de infraestrutura crítica nacional, um plano de resposta e recuperação de incidentes nacionais, leis definidas relacionadas a todos os crimes cibernéticos e um ecossistema vibrante de cibersegurança (MCKINSEY & COMPANY, 2020). A Cybersecurity & Infrastructure Security Agency (CISA) dos EUA também destaca a importância da governança de cibersegurança, que envolvem quadros de responsabilidade, hierarquias de tomada de decisão, riscos definidos relacionados aos objetivos de negócios, planos e estratégias de mitigação e processos e procedimentos de supervisão (CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, s.d.).

Além da infraestrutura física, a governança e as políticas públicas desempenham um papel crucial em moldar um ambiente digital seguro. Políticas bem definidas e uma governança eficaz são essenciais para estabelecer padrões de segurança, promover práticas responsáveis e proteger contra ameaças cibernéticas. Nesse sentido, a Política Estadual de Segurança da Informação de Pernambuco (PESI) e a Política Estadual de Proteção de Dados Pessoais (PEPDP), também de Pernambuco, são exemplos de como os princípios e diretrizes podem orientar a ação governamental, enfatizando a confidencialidade, integridade, disponibilidade e autenticidade das informações.

A adoção das normas técnicas ISO 27000 é reconhecida como um quadro de referência fundamental para a gestão de segurança da informação e privacidade. Estas normas são projetadas para ser aplicáveis a todos os tipos e tamanhos de organizações, oferecendo uma estrutura flexível de segurança da informação que abrange desde a gestão de riscos até a implementação de controles de segurança específicos. A série ISO 27000, incluindo as normas principais ISO 27001 e 27002, estabelece requisitos e procedimentos para criar um Sistema de Gestão de Segurança da Informação (ISMS), sendo a ISO 27001 a única norma da série contra a qual as organizações podem ser auditadas e certificadas. Esta certificação é obtida através de processos de auditoria, normalmente realizados por organizações terceirizadas aprovadas pela ISO, que comprovam a conformidade da organização com as normas estabelecidas (TECHTARGET, 2023) (SECUREFRAME, 2023) (ITGOVERNANCE, 2020).

Além disso, normas suplementares como ISO 27017 e ISO 27018 fornecem controles adicionais para a proteção de dados armazenados na nuvem, refletindo a crescente importância da segurança em ambientes de cloud computing. A ISO 27701, a mais recente adição à série, aborda especificamente a gestão da privacidade, oferecendo orientações sobre como as organizações devem proteger as informações pessoais em conformidade com regulamentos internacionais como a equivalente europeia à nossa LGPD, a General Data Protection Regulation (GDPR).

O Marco Civil da Internet (MCI), promulgado no Brasil em 2014, e o Plano Estrutural de Redes de Telecomunicações (PERT) da Anatel são iniciativas chave que destacam o esforço do país em fortalecer sua infraestrutura digital, promover o acesso à internet e assegurar os direitos fundamentais dos usuários na esfera digital.

O MCI estabeleceu um marco regulatório para os direitos dos usuários da internet no Brasil, abordando temas como liberdade de expressão, privacidade, neutralidade da rede e responsabilidade dos provedores. Essa legislação foi resultado de um processo inovador de consulta pública, que envolveu ampla participação social e debate sobre os princípios que deveriam nortear a regulação da internet no país. A Lei Federal N° 12.965 reflete um compromisso com a promoção de um ambiente digital que respeita os direitos fundamentais e fomenta o desenvolvimento tecnológico e social (POLITIZE, 2021) (PLANALTO, 2014) (IGARAPÉ INSTITUTE, s.d.). Além disso, o Marco Civil estabelece direitos importantes para os usuários, como a inviolabilidade da intimidade e da vida privada, o sigilo das comunicações, a não suspensão da conexão à internet, exceto por débito diretamente decorrente de sua utilização, e a exclusão definitiva dos dados pessoais a pedido do usuário ao término da relação entre as partes. Esses direitos são essenciais para assegurar a privacidade e a liberdade dos usuários na internet. Com a sua criação, o Brasil tornou-se referência mundial na elaboração de princípios-chave para a formulação da internet livre e aberta, garantindo os direitos dos usuários. A legislação foi reconhecida e elogiada por figuras importantes no contexto digital, como Tim Berners-Lee, e serviu de inspiração para iniciativas semelhantes em outros países.

O Plano Estrutural de Redes de Telecomunicações (PERT), elaborado pela Agência Nacional de Telecomunicações (Anatel), é uma iniciativa fundamental para o desenvolvimento das telecomunicações no Brasil. Este plano tem como objetivo principal ampliar o acesso à banda larga no país, coordenando esforços e investimentos entre os setores público e privado. O PERT oferece um diagnóstico detalhado da infraestrutura de telecomunicações do Brasil, destacando as deficiências estruturais nas redes de transporte e de acesso que suportam a oferta dos serviços de banda larga. Através deste diagnóstico, é possível identificar as lacunas existentes e planejar ações efetivas para melhorar a qualidade e ampliar o acesso aos serviços de telecomunicações (GOV.BR, 2019 e GOV.BR, 2023). Além de apresentar um panorama geral da infraestrutura, o PERT também propõe uma série de projetos de investimentos destinados a suprir as deficiências identificadas, além de sugerir possíveis fontes de financiamento que o Poder Público pode utilizar para a execução desses projetos. A atualização anual do PERT é uma parte integrante das atividades da Anatel, servindo como um instrumento de planejamento setorial e de controle dos resultados alcançados, garantindo que as ações sejam ajustadas periodicamente para serem mais efetivas (GOV.BR, 2019).

O MCI e o PERT são iniciativas chave que destacam o esforço do país em fortalecer sua infraestrutura digital, promover o acesso à internet e assegurar os direitos fundamentais dos usuários na esfera digital.

Além disso, o Brasil tem se destacado na governança da internet com a criação de pontos de troca de tráfego internet (IXPs) administrados pelo NIC.br, fortalecendo a infraestrutura de rede do país e promovendo uma maior eficiência na distribuição do tráfego de internet. São Paulo, por exemplo, abriga um dos IXPs mais significativos, direcionando uma quantidade substancial de tráfego diariamente. O país também está investindo na expansão de sua conectividade global, com a construção de novos cabos submarinos de fibra óptica que ligam o Brasil a outras partes do mundo, melhorando a capacidade e a resiliência da rede. Essas iniciativas são fundamentais para abordar a crescente demanda por serviços de telecomunicações e para expandir a conectividade em regiões menos desenvolvidas do Brasil, garantindo que o acesso à internet e os benefícios da digitalização sejam mais equitativamente distribuídos entre a população.

Portanto, a introdução à conectividade corporativa, cibersegurança e políticas públicas abrange uma gama de elementos interconectados, desde a infraestrutura física e tecnológica até o quadro regulatório

e normativo. Juntos, esses elementos formam a base para um ambiente digital seguro, resiliente e inclusivo, capaz de suportar as operações governamentais e empresariais no século XXI.

## PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

A segurança cibernética no contexto atual é marcada por um dinamismo constante, com ameaças evoluindo em complexidade e sofisticação. A crescente digitalização dos serviços governamentais e financeiros amplia o escopo de vulnerabilidades, expondo infraestruturas críticas a riscos significativos. A proteção dessas infraestruturas contra interrupções, vazamentos de dados e outros tipos de ciberataques se torna imperativa, enfatizando a necessidade de uma segurança cibernética robusta e de uma governança eficaz.

Neste capítulo, serão detalhados alguns ataques cibernéticos e como eles exploram vulnerabilidades conhecidas, afetando tanto o setor privado quanto o público. As ameaças digitais são variadas e exigem uma abordagem estratégica e cautelosa para a cibersegurança, a fim de minimizar riscos e proteger os dados organizacionais de influências externas como vírus, invasões, e outras formas de ataques cibernéticos.

Entre as principais ameaças identificadas estão o roubo de dados, a espionagem industrial, ataques de ransomware, phishing, e a exploração de softwares vulneráveis. O roubo de dados, por exemplo, é facilitado pela exfiltração de dados, que envolve a extração não autorizada de informações confidenciais como nomes de usuários, senhas e e-mails, muitas vezes por meio de credenciais de funcionários vazadas. Essa ameaça pode ocorrer em qualquer etapa do armazenamento de dados da empresa, representando um grande potencial de dano e prejuízo (ESCOLA SUPERIOR DE REDES, 2023). Além disso, os erros humanos, como o acesso a links maliciosos ou o uso inadequado de dados sigilosos, são frequentemente explorados por atacantes. A falta de treinamento adequado dos colaboradores em práticas de segurança digital pode deixar a empresa vulnerável a ataques, pois os comportamentos inadequados podem inadvertidamente comprometer informações valiosas (ENG22).

As principais ameaças à segurança da informação têm evoluído de forma significativa, com os ataques e atacantes explorando uma gama diversificada de vulnerabilidades. Em 2022, foram registrados 2,8 bilhões de ataques de malware e 236,1 milhões de ataques de ransomware em todo o mundo, demonstrando a magnitude e a frequência dessas ameaças. A expectativa é que esses números continuem a crescer, tornando imperativo para organizações públicas e privadas desenvolverem estratégias robustas de defesa cibernética (ODATA, 2023). Entre as principais ameaças identificadas para 2023 e além, estão os ataques de ransomware, que não apenas criptografam dados, mas também os roubam, elevando o nível de ameaça e complicando a decisão de pagar ou não o resgate. O aumento do uso de criptomoe-das como o Bitcoin tem facilitado o anonimato dessas transações, incentivando ainda mais esses ataques. Além disso, o criptojacking, que sequestra sistemas para minerar criptomoedas, tem causado problemas significativos de desempenho e segurança para empresas e indivíduos (DEFENSE LIFE CYCLE, 2023).

Outras ameaças notáveis incluem ataques ciberfísicos a cadeias de produção e infraestruturas críticas, como redes elétricas, sistemas de transporte e saúde, bem como ataques patrocinados por governos, que visam tanto outros governos quanto o setor privado. A crescente prevalência de dispositivos IoT (Internet das Coisas) também aumenta o risco de invasões e infecções cibernéticas, com um número estimado de 75 bilhões de dispositivos conectados esperados até 2025. Esses dispositivos, quando comprometidos, podem ser usados para criar confusão, sobrecarregar redes ou bloquear equipamentos es-

senciais (DEFENSE LIFE CYCLE, 2023). Além disso, a saúde digital está se tornando uma área de preocupação crescente, com dispositivos médicos inteligentes e registros médicos eletrônicos (EMRs) tornando-se alvos atraentes para hackers devido às informações confidenciais que contêm. A interconectividade desses dispositivos com redes hospitalares aumenta o risco de comprometimento remoto, o que pode ter consequências diretas na segurança do paciente (DEFENSE LIFE CYCLE, 2023).

Para entender a mente do atacante, alguns modelos foram elaborados por especialistas. O Cyber Kill Chain e o MITRE ATT&CK são modelos conceituais que se destacam no contexto da segurança cibernética por suas abordagens estruturadas para entender e neutralizar ameaças digitais.

O Cyber Kill Chain foi criado pela empresa de defesa Lockheed Martin e delinea as etapas sequenciais que um atacante cibernético realiza para penetrar e eventualmente comprometer sistemas de informação. Estas etapas são: Reconhecimento, Armamentização, Entrega, Exploração, Instalação, Comando e Controle (C2), e Execução de Objetivos. A ideia por trás do modelo é que, interrompendo o ataque em qualquer ponto dessa "cadeia", é possível evitar que os atacantes atinjam seus objetivos finais. Este modelo é amplamente citado em literatura especializada como uma metodologia eficaz para o planejamento de defesas cibernéticas proativas e reativas (Hutchins, Cloppert, & Amin, 2011).

Em detalhes, as fases típicas incluem:

1. Reconhecimento: O adversário coleta informações sobre o alvo;
2. Armamentização: O adversário cria malware para explorar vulnerabilidades no alvo;
3. Entrega: O malware é entregue ao sistema do alvo;
4. Exploração: O malware explora uma vulnerabilidade para entrar no sistema;
5. Instalação: O malware estabelece presença no sistema;
6. Comando e Controle (C2): O adversário estabelece um canal para controlar o malware remotamente;
7. Ações sobre os objetivos: O adversário executa ações para alcançar seus objetivos, como extração de dados ou dano ao sistema.

Por outro lado, o framework ATT&CK, desenvolvido pelo MITRE Corporation, é um repositório detalhado de táticas e técnicas que adversários podem usar contra sistemas de TI. Ao contrário da linearidade do Cyber Kill Chain, o ATT&CK é representado por uma matriz que cruza táticas (os "objetivos" dos adversários) com técnicas (os "métodos" usados para alcançar esses objetivos). Ele é constantemente atualizado com novas informações baseadas em análises reais de ameaças e é empregado para compreender o comportamento dos adversários, melhorar as estratégias de defesa e criar modelos de ameaça adaptativos. O framework é reconhecido por sua aplicabilidade em diversos ambientes operacionais, incluindo sistemas empresariais e infraestrutura crítica (Strom, et al., 2018).

As TTPs, um acrônimo para Táticas, Técnicas e Procedimentos, são elementos centrais do framework MITRE ATT&CK, que é uma ferramenta utilizada para entender e classificar o comportamento de atores de ameaças cibernéticas. Vamos detalhar cada um deles:

- Táticas: Correspondem ao "o quê" da ação do adversário, ou seja, o objetivo imediato que ele deseja alcançar. No MITRE ATT&CK, as táticas são categorizadas em uma matriz que representa as diferentes fases de um ataque cibernético, como Reconhecimento, Acesso Inicial, Execução, Persis-

tência, entre outras. Cada tática é uma coluna na matriz e descreve uma categoria de intenções do adversário durante um ataque.

- **Técnicas:** São o "como" do processo, detalhando os métodos específicos que os adversários usam para alcançar seus objetivos táticos. Cada técnica pode ser empregada em várias táticas diferentes. Por exemplo, a técnica de "Phishing" pode ser usada tanto para o Acesso Inicial quanto para a Execução, dependendo do contexto do ataque.
- **Procedimentos:** São o "detalhe" do "como", representando as implementações específicas das técnicas, incluindo os comandos exatos, as ferramentas utilizadas e as atividades operacionais. Os procedimentos são exemplos do mundo real de como uma técnica é aplicada.

O MITRE ATT&CK é útil porque permite aos defensores visualizar e explorar as relações entre táticas e técnicas, ajudando-os a compreender como um adversário opera e como se pode defender contra suas ações. Além disso, o ATT&CK inclui uma variedade de grupos de ameaças que são conhecidos por usar certas técnicas, o que ajuda os defensores a prever e preparar-se contra ataques que ainda não ocorreram, mas são característicos de um grupo de ameaça conhecido.

A biblioteca de conhecimento do MITRE ATT&CK é constantemente atualizada com novas informações obtidas através da colaboração com especialistas em segurança cibernética e através da análise de incidentes reais de segurança, o que a torna uma fonte viva e adaptável de inteligência sobre ameaças.

A aplicação prática das TTPs dentro do framework pode incluir o mapeamento de logs de segurança a técnicas específicas para identificar atividades suspeitas, a criação de cenários de simulação de ataque para treinamento e testes de defesa, e a priorização de controles de segurança com base em quais técnicas são mais relevantes para a organização em questão.

Voltando ao comparativo dos modelos, eles são ferramentas fundamentais para especialistas em segurança cibernética. O Cyber Kill Chain é uma ferramenta estratégica para identificar e mitigar ataques em progresso, enquanto o MITRE ATT&CK serve como um guia abrangente para o desenvolvimento de defesas robustas contra uma ampla gama de atividades maliciosas. A utilização conjunta desses modelos pode proporcionar uma visão holística e aprofundada das ameaças, facilitando a criação de um ecossistema digital mais seguro e resiliente.

## PROTEGENDO CONTRA AMEAÇAS

Para se proteger contra essas ameaças, é crucial estabelecer uma política robusta de segurança da informação, que inclua a implementação de métodos e ferramentas para proteção de dados, controle de acesso e monitoramento constante da infraestrutura digital. Investir em tecnologias específicas para a proteção de dados, como antivírus, antispam e firewall, e manter os sistemas atualizados são medidas essenciais para combater as ameaças online e oriundas de dispositivos portáteis. A criptografia de arquivos sensíveis e a realização regular de backups, preferencialmente na nuvem, são práticas recomendadas para garantir a resiliência dos dados empresariais frente a potenciais ataques cibernéticos (ENGINEERING BRASIL, 2022) (Junior & da Silva, 2023). Além disso, é crucial que as organizações adotem estratégias de defesa cibernética abrangentes, como a implementação de soluções de segurança integradas, a adoção do modelo de confiança zero e a avaliação do risco de segurança cibernética em transações e compromissos comerciais com terceiros. Além disso, é importante que os líderes empresariais desenvolvam uma cultura de resiliência organizacional para sobreviver a crimes cibernéticos e outras interrupções (GARTNER, 2022).

Para reforçar a segurança em ambientes de Integração Contínua e Entrega Contínua (CI/CD), a CISA e a NSA lançaram orientações conjuntas, enfatizando a importância de reconhecer os vários tipos de ameaças de segurança que podem afetar as operações de CI/CD e tomar medidas para se defender contra cada uma delas. Este guia fornece uma lista de riscos comuns encontrados em pipelines de CI/CD e superfícies de ataque que podem ser exploradas e ameaçar a segurança da rede (CYBERSECURITY & INFRASTRUCTURE, 2023).

No Brasil, a estratégia nacional de segurança cibernética, conhecida como E-Ciber, orienta a sociedade sobre as principais ações do governo federal em termos nacionais e internacionais no quadriênio 2020-2023. Esta estratégia representa o compromisso do país em se tornar uma referência em segurança cibernética, destacando a importância de uma abordagem multifacetada para enfrentar desafios cibernéticos. Isso inclui a prevenção e mitigação de ameaças, a proteção de infraestruturas críticas e a promoção da inovação por meio de pesquisa e desenvolvimento (GOV.BR, 2021a) (GOV.BR, 2021b) (GOV.BR, 2022). Um dos focos da E-Ciber é o reforço dos instrumentos de cooperação internacional, crucial para a aplicação da lei no ambiente digital, especialmente quando as ameaças cibernéticas possuem natureza transnacional. A estratégia também ressalta a necessidade de uma governança eficaz de segurança cibernética, que abrange desde a gestão de riscos até a segurança de certificados digitais, e enfatiza a importância de uma resposta rápida e eficaz a incidentes cibernéticos (GOV.BR, 2021b).

Adicionalmente, a segurança de infraestruturas críticas é tratada como uma prioridade, reconhecendo a importância estratégica de setores como comunicações, energia, transportes e finanças. A Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) define as diretrizes para preservar a prestação de serviços essenciais e estabelece a segurança dessas infraestruturas como uma atividade de Estado, indicando a alta prioridade dada pelo governo brasileiro a essa área (GOV.BR, 2022). Essa estratégia abrangente reflete a compreensão de que a segurança cibernética não é apenas uma questão técnica, mas também um elemento vital para a segurança nacional, desenvolvimento econômico e bem-estar social.

A educação e capacitação em práticas de segurança cibernética também são fundamentais, tanto para a população em geral quanto para profissionais da área. A consciência sobre segurança cibernética vai além da mera questão técnica; é também uma questão de comportamento humano e conscientização. A educação em segurança cibernética equipa indivíduos com o conhecimento necessário para reconhecer e prevenir ameaças, ensina boas práticas de segurança e promove a proteção de dados sensíveis (NET CONSULTING, s.d.). A necessidade de treinamento contínuo é ressaltada, considerando a evolução rápida da tecnologia e das táticas dos atacantes. Uma cultura organizacional de segurança, onde todos estão cientes de seus papéis na proteção dos ativos digitais, é crucial para criar um ambiente cibernético resiliente (GO CACHE, 2023).

A integração da segurança cibernética na educação formal é debatida globalmente, com a percepção de que muitos jovens terminam sua educação sem as habilidades necessárias para navegar com segurança no mundo digital. Projetos educacionais específicos, como o da Universidade Nacional de Córdoba na Argentina, que capacita estudantes para ministrar palestras sobre segurança cibernética, mostram a necessidade de informações e capacitação sobre proteção de dados, identidade digital, e prevenção de ataques (WE LIVE SECURITY, 2019). A inclusão da educação em segurança cibernética nas bases curriculares de países como a Inglaterra e a Espanha destaca a crescente importância deste tema. A Espanha, por exemplo, adaptou seu ordenamento jurídico para incluir a educação digital e a segurança cibernética como parte da educação formal, reconhecendo a necessidade de navegar de forma segura e proteger a privacidade e os dados pessoais desde a infância (WE LIVE SECURITY, 2019). Essas iniciativas refletem a

compreensão de que a segurança cibernética é uma responsabilidade compartilhada e que a educação desempenha um papel fundamental na preparação de indivíduos para enfrentar os desafios do mundo digital.

Além disso, a segurança holística no contexto corporativo enfatiza a integração de medidas passivas e ativas de segurança, o envolvimento das pessoas através da conscientização e treinamento, a consideração de aspectos humanos e culturais, e a coordenação entre diferentes departamentos. A segurança deve ser vista como um componente integrado a todos os aspectos da operação empresarial, abrangendo segurança física, cibernética, humana e organizacional. A inovação responsável e a criação de uma cultura de segurança são fundamentais para o sucesso de qualquer estratégia de segurança (EVEO, s.d.) (BLOG GESTÃO DE SEGURANÇA PRIVADA, 2023).

Estas abordagens refletem a necessidade de uma estratégia de segurança que vá além da implementação de controles técnicos, reconhecendo que as pessoas, processos e a cultura organizacional desempenham papéis cruciais na proteção contra ameaças à segurança da informação. Uma cooperação efetiva entre o setor público, o setor privado e a sociedade civil é essencial para enfrentar esses desafios de forma abrangente.

## DESAFIOS E PERSPECTIVAS FUTURAS NA CIBERSEGURANÇA

A evolução constante do cenário de cibersegurança ressalta a importância da vigilância e inovação contínuas, especialmente com o advento de tecnologias emergentes como a Inteligência Artificial (IA) e a Internet das Coisas (IoT). Estas tecnologias, embora ofereçam novas possibilidades para aumentar a eficiência e funcionalidade dos sistemas, também introduzem complexidades adicionais e vetores de ataque que os agentes de ameaças podem explorar.

A IA, por exemplo, tem o potencial de acelerar e otimizar os processos de detecção e resposta a ameaças cibernéticas, reduzindo o tempo e esforço requerido pelos analistas de segurança através de automação e orquestração. Além disso, pode prever cenários de risco cibernético e sugerir medidas preventivas ou corretivas, adaptando-se às mudanças no ambiente e às novas ameaças para melhorar sua eficácia ao longo do tempo. No entanto, a IA também enfrenta limitações, como a dependência da qualidade e quantidade dos dados, vulnerabilidade a ataques ou manipulações e dificuldades em lidar com situações complexas ou incertas (MANAGE ENGINE, 2023). No contexto da Tecnologia Operacional (OT), a IA é uma faca de dois gumes. Embora possibilite a detecção e resposta proativa a ameaças, ampliando os limites da automação em tecnologias que protegem dados, dispositivos e redes essenciais, sua suscetibilidade a ataques adversários e o potencial de uso indevido por agentes mal-intencionados podem transformá-la em uma nova superfície de ataque. Isso representa um risco significativo para a infraestrutura crítica e sistemas de OT. A colaboração entre analistas de segurança humanos e sistemas de IA é crucial para alcançar um alto nível de resiliência cibernética, permitindo que os operadores humanos se concentrem em tarefas mais estratégicas e de alto nível (INTERNATIONAL IT, 2023). Portanto, à medida que adotamos essas tecnologias inovadoras, é vital abordar os desafios associados à sua implementação, garantindo a segurança, a confiança e a ética na cibersegurança.

A evolução das ameaças cibernéticas destaca-se especialmente com o uso crescente da Inteligência Artificial (IA) pelos cibercriminosos, tornando os ataques mais sofisticados e difíceis de detectar. Técnicas como personificação via IA e a criação de deepfakes estão se tornando ferramentas comuns em golpes de vishing e na disseminação de informações falsas, dificultando a detecção dessas ameaças pelos agentes da lei e sistemas de segurança tradicionais (KEEPER SECURITY, 2023). Além disso, a IA generativa tem

sido utilizada para tornar e-mails de phishing mais convincentes, explorando vulnerabilidades humanas através de engenharia social agressiva. Essa tendência sugere que as ameaças futuras se concentrarão mais nas pessoas, exigindo uma abordagem diferenciada em cibersegurança para quebrar a cadeia de ataques (CISO ADVISOR, 2023).

No contexto de Ransomware como Serviço (RaaS), essa modalidade transformou o ransomware em uma indústria, permitindo até mesmo a indivíduos sem experiência técnica lançar ataques significativos. O modelo de Crimeware-as-a-service (CaaS) facilita o acesso a uma variedade de ferramentas e serviços de hacking, aumentando a sofisticação e a frequência dos ataques cibernéticos. Esse modelo de negócios tem contribuído para o crescimento exponencial dos ataques de ransomware, representando um desafio significativo para a segurança cibernética (MANAGE ENGINE, 2023).

As entidades governamentais enfrentam desafios adicionais devido a orçamentos restritos e falta de pessoal especializado, dificultando a implementação de medidas de segurança robustas e a resposta rápida a incidentes de segurança. A rápida evolução do cenário de ameaças e a necessidade de acesso a grandes volumes de dados para detectar novas ameaças podem levar a altas taxas de falsos positivos, desperdiçando tempo e recursos valiosos.

Esses desafios destacam a necessidade de estratégias de segurança cibernética adaptáveis e proativas que considerem o elemento humano como um elo crítico na cadeia de defesa cibernética. A colaboração entre entidades governamentais, setor privado e especialistas em segurança é fundamental para desenvolver soluções inovadoras que abordem tanto a sofisticação técnica das ameaças quanto suas dimensões humanas e organizacionais.

Embora o prognóstico em relação às ameaças seja preocupante, também é possível observar avanços estratégicos coordenados entre diversos agentes e setores. A crescente conscientização sobre a importância da segurança cibernética está, de fato, impulsionando mudanças significativas em políticas e regulamentações ao redor do mundo, inclusive no Brasil. Um exemplo disso é a atualização da Estratégia Digital do Brasil (E-Digital) para o ciclo 2022-2026, que enfatiza a confiança no ambiente digital, focando na proteção de direitos e privacidade, assim como na segurança digital. A estratégia inclui ações como a promoção de cooperação e compartilhamento de informações entre instituições públicas e privadas para aumentar a resiliência em segurança cibernética e a criação de uma política nacional de segurança cibernética para articular um sistema nacional envolvendo os setores público e privado (GOV BR, 2021c).

Além disso, a adoção da Lei Geral de Proteção de Dados (LGPD) no Brasil é um passo significativo na direção de fortalecer a segurança cibernética e a privacidade dos dados, alinhando-se com as recomendações da OCDE sobre as Diretrizes que Regem a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Esta lei cria uma estrutura regulatória para harmonizar e expandir o direito à proteção de dados pessoais, destacando a necessidade de uma abordagem mais ampla que inclua iniciativas sociais e econômicas para atingir os objetivos de segurança cibernética (OECD ILIBRARY, s.d.).

No que diz respeito à colaboração e compartilhamento de informações, ações estratégicas definidas pela E-Digital, como a promoção de mecanismos de cooperação entre instituições públicas e privadas, são essenciais para prevenir, tratar e responder a incidentes cibernéticos, elevando assim o nível de resiliência em segurança cibernética (GOV BR, 2021c).

Quanto à evolução das tecnologias de defesa, a constante atualização das políticas e estratégias de segurança cibernética, como observado na E-Digital e na LGPD, sugere um movimento em direção ao desenvolvimento de soluções de segurança alimentadas por IA e à implementação de práticas de seguran-

ça proativas. Essas medidas são fundamentais para enfrentar as ameaças em evolução e garantir uma postura de defesa robusta e contínua contra ataques cibernéticos (GOV BR, 2021c) (OECD ILIBRARY, s.d.)

## **GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO EM PERNAMBUCO**

A integração de novas tecnologias, como a computação em nuvem e a inteligência artificial, nas estratégias de segurança da informação, oferece oportunidades para melhorar a eficiência e a eficácia das medidas de segurança, mas também apresenta desafios que devem ser cuidadosamente gerenciados.

A gestão de riscos e segurança da informação em Pernambuco é uma abordagem abrangente e dinâmica, que envolve a adoção de políticas estaduais sólidas, o alinhamento com diretrizes nacionais e internacionais, e a implementação de padrões de segurança reconhecidos globalmente. À medida que o estado avança em suas iniciativas digitais, a contínua evolução dessas estratégias será crucial para garantir a segurança e a resiliência dos sistemas de informação governamentais.

### ***Adoção de Padrões Internacionais***

A adoção das normas ISO/IEC 27000 demonstram a adesão de uma entidade a práticas reconhecidas internacionalmente para a gestão de segurança da informação. Estas normas fornecem um arcabouço para o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI).

A família de normas ISO/IEC 27000 é um conjunto de padrões internacionais projetados para ajudar organizações a protegerem suas informações de forma sistemática e custo-efetiva, através da implementação de um SGSI. A ISO/IEC 27001 é a espinha dorsal deste conjunto, especificando os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI. Complementar a isso, a ISO/IEC 27002 fornece as melhores práticas de controles de segurança da informação que podem ser aplicadas com base nas necessidades de risco da organização. A ISO/IEC 27005 se dedica à gestão de riscos de segurança da informação, oferecendo orientações sobre como avaliar, tratar e monitorar riscos de forma eficaz. A ISO/IEC 27035 é centrada na gestão de incidentes de segurança da informação, delineando um processo estruturado para detectar, reportar e avaliar incidentes. Por fim, a ISO/IEC 27701 se estende para a privacidade, fornecendo orientações sobre a gestão de informações pessoais e ajudando as organizações a estarem em conformidade com as leis de proteção de dados como a LGPD. Juntas, essas normas formam um framework robusto para a segurança e privacidade da informação (ABNT NBR ISO/IEC 27001, 2022) (ABNT NBR ISO/IEC 27002, 2022) (ABNT NBR ISO/IEC 27005, 2023) (ABNT NBR ISO/IEC 27035, 2023) (ABNT NBR ISO/IEC 27701, 2019).

### ***Desafios e Estratégias Futuras***

Para Pernambuco, assim como para outras regiões que buscam manter e aprimorar suas políticas de segurança da informação e proteção de dados pessoais, adaptar-se às novas tecnologias e às ameaças emergentes é um desafio contínuo que requer uma abordagem multifacetada. Isso inclui:

1. **Avaliação Contínua de Riscos:** A segurança da informação começa com a identificação e avaliação dos riscos associados às informações e sistemas de TI. Isso envolve a análise regular das ameaças, vulnerabilidades e impactos potenciais para identificar onde as políticas e controles de segurança precisam ser fortalecidos.
2. **Atualização Periódica das Políticas:** À medida que novas tecnologias e ameaças surgem, as políticas de segurança e proteção de dados devem ser revisadas e atualizadas para refletir o ambiente

em constante mudança. Isso pode incluir a adoção de novos padrões de segurança, técnicas de criptografia, protocolos de autenticação e outras medidas de segurança.

3. Educação e Conscientização em Segurança Cibernética: O fator humano muitas vezes é o elo mais fraco na segurança da informação. Portanto, é crucial investir na educação e conscientização contínua de todos os funcionários do governo sobre as melhores práticas de segurança cibernética, incluindo higiene cibernética básica, reconhecimento de tentativas de phishing e engenharia social, e a importância de seguir as políticas de segurança.
4. Adoção de Tecnologias Avançadas de Segurança: À medida que as ameaças evoluem, também deve evoluir a tecnologia de segurança. Isso pode incluir a implementação de soluções de segurança avançadas, como inteligência artificial e aprendizado de máquina para detecção de ameaças, análise de comportamento para identificar atividades suspeitas e outras tecnologias emergentes que podem melhorar a capacidade de detectar e responder a incidentes de segurança.
5. Parcerias e Colaborações: A colaboração com outras entidades governamentais, setor privado e comunidade internacional pode proporcionar percepções valiosas sobre as melhores práticas de segurança e alertas precoces sobre novas ameaças. Participar de fóruns, grupos de trabalho e iniciativas de compartilhamento de informações pode enriquecer a estratégia de segurança de Pernambuco.
6. Testes e Simulações de Segurança: Realizar testes regulares de penetração, avaliações de vulnerabilidade e simulações de ataque (como exercícios de phishing) pode ajudar a identificar pontos fracos e avaliar a eficácia das medidas de segurança em vigor, permitindo ajustes proativos antes que os incidentes ocorram.

A importância do monitoramento contínuo da segurança da informação em organizações também é destacada pelo Instituto Nacional de Padrões e Tecnologia (NIST) em sua publicação "Continuous Monitoring of Information Security: An Essential Component of Risk Management" (Radack). Este documento enfatiza como o monitoramento contínuo pode fornecer uma consciência das ameaças e vulnerabilidades dos sistemas de informação, facilitando a avaliação dos ativos organizacionais e a eficácia dos controles de segurança. O NIST descreve o monitoramento contínuo da segurança da informação como um componente crucial da gestão de riscos, integrando-se às atividades de avaliação de riscos organizacionais e detalhando o processo organizacional de monitoramento contínuo da segurança da informação.

Olhando agora para os normativos estaduais e nacionais, a implementação de estratégias de gestão de riscos e o fortalecimento da segurança da informação no estado de Pernambuco é fundamentada em marcos estratégicos e robustos, que integram políticas estaduais e diretrizes nacionais para a proteção de ativos de informação e a garantia da continuidade das operações governamentais. Estes marcos são essenciais para enfrentar as ameaças cibernéticas em constante evolução e para assegurar a resiliência dos sistemas de informação do estado.

### ***Política Estadual de Segurança da Informação (PESI)***

A Política Estadual de Segurança da Informação (PESI) de Pernambuco, estabelecida pelo Decreto Nº 49.914 de 10 de dezembro de 2020, tem os seguintes pontos chave:

- Objetivo: Institui a PESI na administração pública estadual, aplicável a órgãos e entidades estaduais, seus servidores, funcionários, colaboradores e pessoas jurídicas de direito privado com relação contratual com o Estado de Pernambuco;

- **Princípios Basilares:** Incluem a confidencialidade, integridade, disponibilidade e autenticidade das informações. Os princípios também englobam a incorporação da segurança da informação na rotina dos órgãos estaduais, a capacitação dos agentes públicos em segurança da informação e a publicidade das normas e procedimentos, exceto em casos de necessidade de sigilo;
- **Objetivos da PESI:** São destacados objetivos como posicionar a segurança da informação como elemento fundamental nas ações públicas, dotar órgãos estaduais de instrumentos jurídicos e tecnológicos para assegurar a segurança da informação, promover o intercâmbio científico-tecnológico e garantir a continuidade das atividades governamentais dependentes de informação e sistemas de informação;
- **Diretrizes Gerais:** Incluem a proporcionalidade das medidas de segurança da informação, controle de acesso a sistemas e informações, registro de acessos e alterações de dados, acompanhamento permanente do cumprimento da PESI (através do monitoramento do tráfego e armazenamento da informação), gestão de riscos e qualidade em segurança da informação;
- **Composição da PESI:** A PESI é composta por normas temáticas complementares e políticas de segurança da informação locais adotadas individualmente pelos órgãos e entidades estaduais;
- **Responsabilidades do Comitê Técnico de Governança Digital (CTGD):** Deliberar o plano quadrienal estratégico para a área de segurança da informação, aprovar complementos e avaliações da PESI e monitorar seu cumprimento;
- **Papel da Agência Estadual de Tecnologia da Informação (ATI):** Atuar como órgão consultor de segurança da informação junto aos demais órgãos e entidades da administração pública estadual;
- **Responsabilidades dos Órgãos e Entidades Estaduais:** Promover a adequação de sua infraestrutura de TI à PESI.

### ***Política Estadual de Proteção de Dados Pessoais (PEPDP)***

A Política Estadual de Proteção de Dados Pessoais (PEPDP) do Poder Executivo Estadual de Pernambuco, conforme o Decreto Nº 49.265 de 6 de agosto de 2020, estabelece as seguintes diretrizes e disposições:

- **Objetivo e Âmbito:** A PEPDP visa desenvolver e adaptar ações governamentais à Lei Geral de Proteção de Dados Pessoais (LGPD), aplicando-se à Administração Pública Estadual direta, autárquica e fundacional;
- **Princípios:** A política observa princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas;
- **Diretrizes:** Incluem alinhamento às políticas de segurança da informação do Estado, atendimento simplificado e eletrônico das demandas do cidadão, equilíbrio com a promoção da transparência pública, proporcionalidade das medidas de proteção de dados e privacidade, desenvolvimento do nível de maturidade dos tratamentos dos dados, manutenção da segurança jurídica, economicidade das ações, alinhamento ao planejamento estratégico do Estado e aderência à Política de Tecnologia da Informação e Comunicação do Estado;
- **Definições:** Define termos como dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, agentes de tratamento e tratamento;

- Implementação: A PEPDP será implementada através do Plano Quadrienal Estratégico de Proteção de Dados Pessoais, que estabelecerá as prioridades estaduais quanto à adequação à LGPD;
- Governança: Competências são atribuídas a diversos comitês e órgãos estaduais, como o Comitê Executivo de Governança Digital e o Comitê Técnico de Governança Digital, para monitoramento e implementação da política;
- Atendimento ao Titular: Detalha procedimentos para atendimento ao titular dos dados, incluindo modalidades eletrônica e presencial;
- Tratamento de Dados Pessoais: Estabelece diretrizes para o tratamento de dados pessoais, restringindo-o à finalidade e executando-o de forma adequada e pelo prazo necessário;
- Compartilhamento de Dados Pessoais: Define condições para o compartilhamento de dados pessoais entre controladores públicos e entre controladores públicos e privados;
- Papel da Agência Estadual de Tecnologia da Informação (ATI): implementar e monitorar medidas de segurança para proteger dados pessoais, além de gerenciar a infraestrutura tecnológica necessária para garantir a segurança e eficiência das operações de TI do estado, adequando as arquiteturas e as operações compartilhadas de TIC hospedadas no datacenter e na rede corporativa às exigências da Lei Federal nº 13.709, de 2018 (LGPD).

#### ***Estratégia de Governo Digital (EGD) do Governo do Estado de Pernambuco:***

A contratação da nova solução de segurança e conectividade do Estado de Pernambuco está diretamente alinhada com os objetivos estratégicos estabelecidos na Estratégia de Governo Digital 2024-2027 (EGD), em particular com as metas de transformação digital, fortalecimento da segurança da informação e ampliação da conectividade no Estado. Esta contratação reflete o compromisso do Governo de Pernambuco em modernizar sua infraestrutura de TIC, garantindo serviços mais seguros e eficientes para os cidadãos, além de apoiar o desenvolvimento de um Governo mais ágil e responsivo.

O Objetivo Estratégico 7 da EGD, que visa fortalecer a infraestrutura de segurança da informação e promover a ampliação da conectividade no Estado, é uma das principais diretrizes que fundamentam esta contratação. O fortalecimento da segurança cibernética e a expansão de uma infraestrutura de rede robusta são essenciais para garantir que as escolas, hospitais, delegacias e outros serviços públicos tenham acesso confiável à internet de alta velocidade, atendendo às crescentes demandas por serviços digitais eficientes e seguros. A contratação proposta atende a essa necessidade, ao implementar soluções de proteção e monitoramento da rede, assegurando o pleno funcionamento das operações governamentais e a proteção dos dados sensíveis.

Além disso, esta contratação também se alinha ao Objetivo Estratégico 8, que busca inovar e otimizar as contratações públicas para reduzir custos e elevar a eficiência. A automação e a integração de serviços digitais estão no centro desse objetivo, e a adoção de uma infraestrutura de conectividade avançada e de ferramentas de segurança cibernética contribuirá para a redução de ineficiências operacionais, ao mesmo tempo em que proporciona um maior controle sobre os gastos públicos e garante a transparência na gestão dos serviços contratados.

Outro ponto de destaque é o Objetivo Estratégico 6, que prevê a impulsão da cultura de dados para a tomada de decisões estratégicas. A implementação de soluções tecnológicas que garantam o monitoramento e a segurança das informações é essencial para otimizar a coleta e o processamento de dados.

A contratação proposta está alinhada com essa visão, uma vez que a segurança da informação é um requisito fundamental para assegurar a integridade dos dados que embasam as políticas públicas, promovendo decisões mais eficazes e bem fundamentadas.

A contratação também está em conformidade com os princípios de sustentabilidade e responsabilidade descritos na EGD. A solução proposta tem o potencial de promover o uso eficiente dos recursos tecnológicos, garantindo a escalabilidade e a manutenção de um sistema sustentável a longo prazo. O foco em sustentabilidade não se limita ao uso eficiente de energia ou materiais, mas também envolve a criação de uma infraestrutura digital que seja adaptável, resiliente e capaz de suportar as futuras demandas tecnológicas do Estado. Este alinhamento reforça o compromisso do Governo de Pernambuco com a responsabilidade social e ambiental em suas contratações, contribuindo para o desenvolvimento sustentável do setor público.

Além do alinhamento com os objetivos estratégicos da EGD, é importante destacar que a integração dessa solução com outras iniciativas digitais já em andamento no Governo de Pernambuco é fundamental. A sinergia entre os diferentes projetos de transformação digital evita a duplicidade de esforços e promove o uso eficiente dos recursos tecnológicos e financeiros, potencializando o impacto positivo das soluções contratadas.

Finalmente, a contratação proposta está alinhada com os mecanismos de monitoramento e avaliação de desempenho estabelecidos pelo Governo de Pernambuco, assegurando que a implementação das soluções será acompanhada por métricas de sucesso e indicadores-chave de desempenho (KPIs). Estes KPIs serão críticos para avaliar o impacto das soluções de segurança e conectividade ao longo do tempo, garantindo a entrega dos resultados esperados e permitindo ajustes contínuos para otimizar a eficiência e a segurança da infraestrutura de TIC.

#### ***Marco Civil da Internet:***

O Marco Civil da Internet, sancionado no Brasil como Lei 12.965/2014, serve como um marco regulatório fundamental que delimita direitos, deveres e princípios para o uso da Internet no país. Apelidado de "Constituição da Internet", foi criado após amplo debate público, visando assegurar um equilíbrio entre a liberdade de expressão, a privacidade dos usuários, a neutralidade da rede e a segurança na internet. Entre seus principais pilares, destaca-se a garantia da neutralidade da rede, assegurando tratamento igualitário de todos os dados sem discriminação. A lei enfatiza a proteção da privacidade e dos dados pessoais, exigindo transparência no uso de informações pelos provedores de serviços de internet. Também protege a liberdade de expressão, delineia a responsabilidade dos provedores por conteúdo de terceiros apenas em determinadas condições e estabelece direitos dos usuários à informação clara e à não suspensão da conexão à internet exceto por inadimplência. Além disso, define regras para a guarda de registros por provedores, buscando equilibrar segurança e privacidade. O Marco Civil é um instrumento vital para a governança da Internet no Brasil, promovendo um ambiente digital que respeita os direitos fundamentais e a liberdade de expressão dos usuários.

#### **Fundamentação:**

- Art. 18º, § 1º, inciso II, da Lei nº 14.133, de 01 de abril de 2021;
- Art. 2º-G, da Lei nº 12.985, de 02 de janeiro de 2006;

- Art. 8º, inciso II, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Decreto nº 55.861, de 28 de novembro de 2023;
- Art. 8º, Portaria Conjunta SAD/PGE nº 97, de 14 de dezembro de 2023;
- Estratégia de Governança Digital - EGD conforme dispõe o Art. 2º-G da Lei 12.985, de 02/01/2006;
- Política Estadual de Segurança da Informação de Pernambuco (PESI), estabelecida pelo Decreto estadual nº 49.914, de 10 de dezembro de 2020;
- Assistência Técnica para o Projeto de Data Center e Rede de Banda Larga de Pernambuco - Relatório da Câmara de Comércio dos Estados Unidos (USTDA) para o Governo de Pernambuco;
- MCKINSEY & COMPANY. (2020). Follow the leaders: How governments can combat intensifying cybersecurity risks. Fonte: <https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks>;
- MCKINSEY & COMPANY. (2021a). Cybersecurity in a digital era. Fonte: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity-in-a-digital-era>;
- MCKINSEY & COMPANY. (2021b). Four ways to get more from government infrastructure projects. Fonte: <https://www.mckinsey.com/>;
- WORLD BANK BLOGS. (2021). World Bank Blogs. Fonte: <https://blogs.worldbank.org/>;
- MCKINSEY & COMPANY. (2021c). A smarter way to think about public-private partnerships. Fonte: <https://www.mckinsey.com/>;
- BLACKRIDGE RESEARCH & CONSULTING. (2022). Public Private Partnership (PPP): Meaning, Definition & Complete Guide. Fonte: <https://www.blackridgeresearch.com/>;
- CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. (s.d.). Cybersecurity Governance. Fonte: <https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance>;
- TECHTARGET. (2023). Top 12 IT security frameworks and standards explained. Fonte: <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one>;
- SECUREFRAME. (2023). ISO 27000 Series: What the Standards Are + Their Purpose. Fonte: <https://secureframe.com/blog/iso-27000>;
- ITGOVERNANCE. (2020). What is the ISO 27000 series of standards? Fonte: <https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards>;
- PLANALTO. (2014). LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Fonte: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm);
- POLITIZE. (2021). O que é o Marco Civil da Internet? Fonte: <https://www.politize.com.br/marco-civil-da-internet/>;
- IGARAPÉ INSTITUTE. (s.d.). O Brasil e o Marco Civil da Internet. Fonte: <https://igarape.org.br/marcocivil/pt/>;

- GOV.BR. (2019). Plano Estrutural de Redes de Telecomunicações - PERT. Fonte: <https://www.gov.br/anatel/pt-br/dados/infraestrutura/pert/>;
- GOV.BR. (2023). Plano Estrutural de Redes de Telecomunicações ganha versão atualizada. Fonte: <https://www.gov.br/anatel/pt-br/assuntos/noticias/plano-estrutural-de-redes-de-telecomunicacoes-ganha-versao-atualizada/>;
- ESCOLA SUPERIOR DE REDES. (2023). 9 principais ameaças para a segurança da informação corporativa! Fonte: <https://esr.rnp.br/seguranca/ameacas-seguranca-da-informacao/>;
- ENGINEERING BRASIL. (2022). 6 ameaças à segurança da informação e como proteger sua empresa. Fonte: <https://blog.engdb.com.br/ameacas-a-seguranca-da-informacao/>;
- ODATA. (2023). As principais ameaças cibernéticas para 2023 e os próximos anos. Fonte: <https://odatacolocation.com/blog/principais-ameacas-ciberneticas-2023/>;
- DEFENSE LIFE CYCLE. (2023). Ameaças e tendências de Segurança de Informação para 2023. Fonte: <https://defenselifecycle.com/noticias/ameacas-e-tendencias-2023/>;
- Hutchins, E. M., Cloppert, J. M., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.;
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and Philosophy.;
- MANAGE ENGINE. (2023). Ataques cibernéticos: o que esperar no futuro. Fonte: <https://blogs.manageengine.com/portugues/2023/05/04/ataques-ciberneticos-o-que-esperar-no-futuro.html>;
- Junior, W. M., & da Silva, C. L. (2023). Segurança Cibernética e seus Paradigmas na Era Digital. Revista Científica Multidisciplinar O Saber. Fonte: <https://www.revistacientificaosaber.com.br/artigos/seguran%C3%A7a-cibern%C3%A9tica-e-seus-paradigmas-na-era-digital>;
- GARTNER. (2022). Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23. Fonte: <https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio>;
- GOV BR. (2021c). Segurança Cibernética. Fonte: <https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica>;
- GOV.BR. (2021a). Estratégia Nacional de Segurança Cibernética. Fonte: <https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica>;
- GOV.BR. (2021b). Segurança Cibernética. Fonte: <https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica>;
- GOV.BR. (2022). Segurança de Infraestruturas Críticas. Fonte: <https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic>;

- GO CACHE. (2023). A importância da educação em segurança cibernética para funcionários. Fonte: <https://www.gocache.com.br/dicas/a-importancia-da-educacao-em-seguranca-cibernetica-para-funcionarios/>;
- WE LIVE SECURITY. (2019). A segurança cibernética deve ser um tema abordado na educação formal? Fonte: <https://www.welivesecurity.com/br/2019/11/19/a-seguranca-cibernetica-deve-ser-um-tema-abordado-na-educacao-formal/>;
- EVEO. (s.d.). Governança de segurança da informação: o que é, como funciona e sua importância. Fonte: <https://blog.eveo.com.br/governanca-seguranca-informacao/>;
- BLOG GESTÃO DE SEGURANÇA PRIVADA. (2023). Segurança Holística no Contexto da Segurança Empresarial: Defesa abrangente contra várias ameaças. Fonte: <https://gestaodesegurancaprivada.com.br/seguranca-holistica-contexto-seguranca-empresarial/>;
- INTERNATIONAL IT. (2023). Inteligência Artificial na Cibersegurança de OT: Desafios e Oportunidades. Fonte: <https://www.internationalit.com/post/intelig%C3%Aancia-artificial-na-ciberseguran%C3%A7a-de-ot-desafios-e-oportunidades>;
- KEEPER SECURITY. (2023). Como os cibercriminosos estão usando a IA para ataques cibernéticos. Fonte: <https://www.keepersecurity.com/blog/pt-br/2023/06/21/how-cybercriminals-are-using-ai-for-cyberattacks/>;
- CISO ADVISOR. (2023). Uso de IA generativa em ataques deve crescer em 2024, diz estudo. Fonte: <https://www.cisoadvisor.com.br/uso-de-ia-generativa-em-ataques-deve-crescer-em-2024-diz-estudo/>;
- OECD ILIBRARY. (s.d.). Capítulo 7. Políticas para a transformação digital: Recomendações para uma abordagem integral do governo (whole-of-government). Fonte: <https://www.oecd-ilibrary.org/sites/9a112bbe-pt/index.html?itemId=/content/component/9a112bbe-pt>;
- ABNT NBR ISO/IEC 27001. (2022). ISO/IEC 27001. International Organization for Standardization & International Electrotechnical Commission.;
- ABNT NBR ISO/IEC 27002. (2022). ISO/IEC 27002. International Organization for Standardization & International Electrotechnical Commission.;
- ABNT NBR ISO/IEC 27005. (2023). ISO/IEC 27005. International Organization for Standardization & International Electrotechnical Commission.;
- ABNT NBR ISO/IEC 27035. (2023). ISO/IEC 27035. International Organization for Standardization & International Electrotechnical Commission.;
- ABNT NBR ISO/IEC 27701. (2019). ISO/IEC 27701. International Organization for Standardization & International Electrotechnical Commission.;
- ABNT/CB-21. (Setembro de 2013). ABNT NBR ISO/IEC 27002.

## 5. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

O projeto consiste na contratação de serviços de conectividade multitecnologias (banda larga, satélite de baixa órbita (LEO) e média órbita (MEO) e 5G FWA (Fixed Wireless Access)), fundamentada na busca por uma conexão estável e de alta velocidade para suportar as atividades críticas do Estado, garantindo assim a eficiência e produtividade dos agentes públicos e colaboradores. Além da conectividade, a demanda também inclui a contratação de serviços de voz (contact center, comunicação unificada e pontos de voz) e de segurança da informação, onde para esses serviços devem abranger a implementação de hardwares, tecnologias, processos e a disponibilização de pessoal capacitado para garantir a proteção dos dados e sistemas do poder executivo e outros poderes do estado de Pernambuco contra ameaças cibernéticas. É essencial que os serviços de segurança oferecidos atendam aos padrões e normas de segurança da informação vigentes, assegurando a integridade, confidencialidade e disponibilidade das informações críticas do poder executivo e outros poderes do estado de Pernambuco. O escopo da demanda abrange a especificação detalhada dos pacotes de conectividade requeridos, incluindo suas respectivas velocidades e características técnicas, bem como dos serviços de voz que deverão ser mantidos, contemplando a evolução tecnológica dos dispositivos. Além disso, inclui a definição dos serviços de contact center, comunicação unificada, e a descrição dos serviços de segurança da informação necessários, detalhando os hardwares e tecnologias envolvidas, os processos de segurança a serem implementados, e a qualificação exigida do pessoal envolvido.

Todas as especificações técnicas demandadas serão detalhadas no Termo de Referência.

## 5.1. PREMISSAS

Podemos destacar as seguintes premissas para a contratação do serviço de Conectividade e Segurança compondo um item de Serviço da NOVA REDE CORPORATIVA DO GOVERNO DE PERNAMBUCO:

### 1. Demanda de Conectividade e Segurança:

- O serviço é essencial para atender às necessidades de conectividade e segurança do Governo do Estado de Pernambuco e outros Poderes sediados no Estado.

### 2. Otimização da Prestação de Serviços Digitais:

- A implementação da NOVA REDE CORPORATIVA DO GOVERNO DE PERNAMBUCO visa otimizar a prestação de serviços digitais, garantindo uma comunicação segura e eficiente entre as diversas entidades governamentais.

### 3. Governança Administrativa:

- Há um reconhecimento da necessidade de realizar a contratação para aprimorar o modelo de gestão de segurança da informação, conforme estabelecido pelo Decreto Nº 42.907 de 13 de abril de 2016.

### 4. Gestão Eficiente:

- A contratação visa garantir uma gestão eficiente da infraestrutura de conectividade e segurança, re-presentando a solução mais vantajosa para alcançar esse objetivo.

### 5. Continuidade dos Serviços:

- A implementação é vital para evitar interrupções nos serviços em andamento, prevenindo possíveis prejuízos e garantindo a continuidade das operações governamentais.

#### **6. Importância da Segurança Cibernética nas Atividades Estaduais:**

- Os recursos de segurança cibernética desempenham um papel crucial nas atividades tanto "meio" quanto "finalísticas" das secretarias e órgãos estaduais, garantindo a qualidade na prestação de serviços públicos e contribuindo para a modernização da gestão pública.

#### **7. Aprimoramento dos Resultados:**

- Busca-se aprimorar os resultados obtidos em edições anteriores, expandindo a oferta de serviços de conectividade, segurança e demais serviços, mantendo a qualidade e promovendo uma gestão eficiente.

#### **8. Atualização Tecnológica:**

- A análise de contratos recentes revelou a necessidade de atualização, considerando a evolução do mercado e das demandas do Governo, especialmente para serviços de conectividade e segurança, com ênfase na implementação de tecnologias de ponta como SD-WAN e segurança de endpoint avançada.

#### **9. Essencialidade do Serviço durante a Pandemia:**

- Durante a pandemia da COVID-19, a importância crucial de um serviço de conectividade e segurança robusto foi evidenciada, pois facilitou o trabalho remoto seguro e permitiu a comunicação eficiente mesmo em condições de isolamento.

#### **10. Resiliência e Recuperação de Desastres Naturais:**

- A contratação deve garantir que a infraestrutura de conectividade, segurança e demais serviços que incluam mecanismos robustos de resiliência e recuperação de desastres, assegurando a continuidade dos serviços em caso de incidentes críticos.

#### **11. Conformidade com Regulamentações:**

- A solução deve garantir conformidade com todas as regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras normas de segurança da informação.

#### **12. Proteção Proativa contra Ameaças:**

- Implementação de soluções de segurança que garantam proteção proativa contra ameaças cibernéticas emergentes, como a utilização de inteligência artificial e machine learning para detectar e mitigar ataques em tempo real.

#### **13. Monitoramento e Resposta a Incidentes:**

- A contratação deve incluir serviços de monitoramento contínuo e resposta a incidentes, garantindo que ameaças sejam identificadas e mitigadas rapidamente, minimizando impactos negativos.

#### **14. Treinamento e Conscientização em práticas de segurança:**

- Garantir treinamento online de conscientização em práticas de segurança para os agentes públicos, assegurando que os órgãos estejam preparados para lidar com as mais recentes ameaças.

#### **15. Integração com Infraestruturas Existentes:**

- A solução deve ser capaz de integrar-se perfeitamente com a infraestrutura de TI da contratante pré-existentes ao contrato, incluindo sistemas legados e novos desenvolvimentos, garantindo uma implementação eficiente;

#### **16. Telefonia Fixa:**

- Garantir que os números de telefones atuais sejam migrados (portabilidade) para o novo contrato, conforme demanda da contratante, e prestados por meio de serviços com tecnologias atuais e emergentes;

**17. Infraestrutura para rede sem fio:**

- Garantir o fornecimento, gestão e manutenção do serviço com tecnologias atuais e emergentes conforme necessidade da contratante;

**18. Infraestrutura de tecnologia de comunicação para serviços de Contact Center:**

- Garantir serviços de Contact Center com fornecimento de infraestrutura de tecnologia de comunicação utilizando os diversos meios tecnológicos disponíveis (telefone/chat/e-mail/redes sociais/etc);

**19. Serviço de SOC:**

- Garantir um serviço de Security Operation Center (SOC) de forma centralizada para monitorar, detectar, analisar e responder a incidentes de segurança cibernética em tempo real. Ele deve realizar a defesa das instituições estaduais contra ameaças cibernéticas e ser composto por uma combinação de processos, tecnologias e pessoal especializado.

**20. Serviço de NOC:**

- Garantir um serviço de Network Operation Center (NOC), ou Centro de Operações de Rede, de forma centralizada onde profissionais de TI devem monitorar, gerenciar e manter a rede corporativa. Ele deve desempenhar um papel crucial na garantia da operação contínua e eficiente da infraestrutura de rede do Governo do Estado.

**21. Serviço de Helpdesk:**

- Garantir um serviço de Helpdesk, com uma estrutura abrangente para a implementação de um serviço de helpdesk eficiente e eficaz para gestão de chamados de descontinuidade de serviços e ativos de segurança na rede corporativa do Governo do Estado. A adoção dessas práticas pode ajudar a garantir a rápida resolução de problemas e a manutenção da continuidade dos serviços essenciais.

**22. Permitir Serviços de Auditoria independente:**

- Permitir serviço de auditoria independente com o objetivo de oferecer uma visão imparcial, especializada e abrangente da qualidade, da segurança e da eficiência da rede corporativa do Governo do Estado, contribuindo para um ambiente mais seguro e robusto.

**23. Permitir Testes de Vulnerabilidade independente:**

- Permitir testes de vulnerabilidade independentes na rede corporativa do Governo do Estado com objetivo de fortalecer a segurança cibernética, identificar e corrigir vulnerabilidades e garantir a conformidade com regulamentações e padrões de segurança.

Essas premissas fornecem uma base sólida para a contratação dos serviços técnicos especializados para a implementação da NOVA REDE CORPORATIVA DO GOVERNO DE PERNAMBUCO.

## 5.2. NECESSIDADES DE NEGÓCIO

Ao considerar a Estratégia de Governo Digital (EGD) do Estado de Pernambuco, diversas Necessidades de Negócio (NNs) podem ser identificadas. Estas NNs devem estar alinhadas com os objetivos e diretrizes da EGD, e podem incluir, mas não se limitam a:

- **Melhoria na Prestação de Serviços Públicos Digitais:** Aumentar a eficiência e a eficácia dos serviços públicos oferecidos digitalmente, garantindo maior acessibilidade e conveniência para os cidadãos.
- **Expansão do Acesso à Internet:** Ampliar a cobertura de acesso à Internet em áreas rurais ou remotas do estado, promovendo a inclusão digital e garantindo que mais cidadãos possam acessar serviços digitais do governo.
- **Aumento da Resiliência da Conectividade:** Garantir a alta disponibilidade da rede de conectividade através do uso de redundâncias por tecnologias de acesso distintos (banda larga (fibra óptica), Satélites de Baixa Órbita (LEO), Satélites de Órbita Média (MEO) e 5G FWA (Fixed Wireless Access)).
- **Integração de Sistemas e Dados Governamentais:** Desenvolver e implementar soluções que permitam a integração de diferentes sistemas e bancos de dados governamentais para melhorar a troca de informações, a tomada de decisões baseada em dados e a prestação de serviços.
- **Segurança e Privacidade de Dados:** Reforçar as medidas de segurança para proteger os dados governamentais e dos cidadãos, em conformidade com as leis de proteção de dados, como a LGPD.
- **Modernização da Infraestrutura de TI:** Atualizar e expandir a infraestrutura tecnológica existente para suportar novas aplicações e serviços digitais, garantindo a capacidade e a resiliência do sistema.
- **Capacitação e Desenvolvimento de Competências Digitais:** Desenvolver habilidades e competências digitais entre os funcionários públicos para melhor operacionalizar e gerenciar soluções de governo digital.
- **Promoção de Governança e Transparência Digital:** Implementar soluções que promovam a transparência e a governança no setor público, incluindo plataformas de dados abertos e mecanismos de controle social.
- **Inovação e Uso de Tecnologias Emergentes:** Explorar e integrar tecnologias emergentes, como inteligência artificial e análise de dados, para melhorar a eficiência dos processos governamentais e a qualidade dos serviços públicos.
- **Desenvolvimento de Canais Unificados de Serviços:** Criar canais digitais unificados para que os cidadãos possam acessar facilmente diversos serviços governamentais.
- **Acessibilidade e Inclusão Digital:** Garantir que os serviços digitais do governo sejam acessíveis a todos os cidadãos, incluindo pessoas com deficiência, idosos e aqueles em áreas menos desenvolvidas.

Com base no Decreto Nº 49.914 de 10 de dezembro de 2020, que institui a Política Estadual de Segurança da Informação (PESI) em Pernambuco, algumas Necessidades de Negócio (NNs) específicas podem ser identificadas para inclusão no Estudo Técnico Preliminar (ETP) da nova rede de telemática. Estas NNs incluem:

- **Implementação de Medidas de Segurança da Informação:** Garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, conforme os princípios basilares da PESI (Art. 2º).
- **Promoção da Segurança da Informação nas Ações Públicas:** Posicionar a segurança da informação como elemento fundamental nas ações públicas e no planejamento estratégico da administração pública estadual (Art. 4º, I).
- **Capacitação e Aculturação dos Agentes Públicos:** Capacitar os agentes públicos em aspectos de segurança da informação, visando sua incorporação à rotina dos órgãos e entidades da administração pública estadual (Art. 2º, II).
- **Conformidade com Normas e Regulamentos:** Garantir que as atividades de gestão de segurança da informação estejam em conformidade com a padronização e normatização no âmbito da administração pública estadual (Art. 4º, III).

- **Desenvolvimento de Instrumentos Jurídicos e Normativos:** Dotar os órgãos e entidades da administração pública estadual de instrumentos jurídicos, normativos e organizacionais para assegurar a segurança da informação (Art. 4º, II).
- **Gestão de Riscos e Qualidade em Segurança da Informação:** Implementar processos de gestão de riscos e gestão da qualidade da segurança da informação, conforme as diretrizes gerais da PESI (Art. 5º, IV e VI).
- **Intercâmbio Científico-Tecnológico em Segurança da Informação:** Promover o intercâmbio entre órgãos e entidades estaduais e instituições públicas e privadas sobre atividades de segurança da informação (Art. 4º, IV).
- **Referencial de Segurança para Aquisições e Contratações de TI:** Estabelecer um referencial de segurança de informação para nortear as aquisições e a contratação de serviços de TI (Art. 4º, V).
- **Interoperabilidade dos Sistemas de Segurança da Informação:** Assegurar a interoperabilidade entre os sistemas de segurança da informação (Art. 4º, VI).
- **Continuidade das Atividades Governamentais Dependentes de Informação:** Garantir a continuidade das atividades do governo que dependem de informação e sistemas de informação (Art. 4º, IX).

A Política Estadual de Proteção de Dados Pessoais de Pernambuco (PEPDP), como descrita no Decreto Nº 49.914, apresenta várias necessidades de negócio (NNs) relevantes. Estas NNs estão estruturadas em torno de diretrizes, normas e ações para adaptar a ação governamental à Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito da Administração Pública Estadual direta, autárquica e fundacional. As NNs identificadas incluem:

- **Alinhamento às Políticas de Segurança da Informação:** Assegurar que o tratamento de dados esteja alinhado com as políticas de segurança da informação do Estado de Pernambuco, promovendo a proteção e integridade dos dados pessoais.
- **Promoção da Transparência e Acesso Eletrônico:** Estimular a transparência pública e facilitar o acesso eletrônico dos cidadãos às informações, garantindo a proteção de seus dados pessoais.
- **Desenvolvimento de Maturidade no Tratamento de Dados:** Focar no desenvolvimento do nível de maturidade dos tratamentos de dados, garantindo a eficiência e a conformidade com as normas de proteção de dados.
- **Segurança Jurídica e Economicidade:** Manter a segurança jurídica dos instrumentos firmados e buscar a economicidade nas ações relacionadas à proteção de dados.
- **Planejamento Estratégico e Adesão à Política de TIC:** Alinhar a política de proteção de dados ao planejamento estratégico do Estado e à Política de Tecnologia da Informação e Comunicação.
- **Gerenciamento de Riscos e Controles Internos:** Implementar um processo eficaz de gerenciamento de riscos e estabelecer controles internos robustos para a proteção de dados pessoais.
- **Auditoria Interna e Avaliação Baseada em Riscos:** Realizar auditorias internas para proteger o valor organizacional do Estado, fornecendo avaliação, assessoria e conhecimento baseados em riscos.
- **Desenvolvimento de Soluções de TIC e Consultoria Jurídica:** Orientar a aplicação de soluções de TIC relacionadas à proteção de dados pessoais e disponibilizar consultoria jurídica para dirimir questões relacionadas à LGPD.
- **Informar Incidentes de Privacidade:** Estabelecer um plano de respostas a incidentes de privacidade de dados pessoais e informar tais incidentes à Autoridade Nacional de Proteção de Dados Pessoais.

- **Atendimento Eletrônico ao Titular do Dado:** Prestar atendimento eletrônico aos titulares dos dados pessoais, garantindo a identificação idônea e um gerenciamento eficiente das demandas.

Estas NNs refletem o compromisso do Estado de Pernambuco com a segurança da informação, a proteção de dados pessoais e a conformidade com a legislação vigente, visando melhorar a governança, a transparência e a eficiência dos serviços públicos no âmbito da proteção de dados.

No desenvolvimento de projetos de TI, como o PE-Conectado II em Pernambuco, as necessidades de negócio podem incluir:

- **Melhoria de Serviços Públicos:** Implementar soluções tecnológicas para aprimorar a eficiência e a qualidade dos serviços públicos oferecidos à população.
- **Segurança da Informação:** Garantir a segurança, confidencialidade, integridade e disponibilidade das informações processadas e armazenadas pelos sistemas governamentais.
- **Conformidade com Regulamentações:** Assegurar que todos os aspectos do projeto estejam em conformidade com as leis e regulamentações pertinentes, como a Lei Federal 14.133/2021, a Política Estadual de Segurança da Informação (PESI), e outras normativas aplicáveis.
- **Acessibilidade e Inclusão Digital:** Facilitar o acesso dos cidadãos aos serviços digitais, promovendo a inclusão digital e a equidade no acesso à informação.
- **Eficiência Operacional:** Otimizar processos e reduzir custos operacionais, utilizando tecnologia para automatizar tarefas e melhorar a gestão de recursos.
- **Adaptação e Escalabilidade:** Desenvolver sistemas que sejam capazes de se adaptar a mudanças futuras e escalar conforme a demanda aumenta.

Em 2022, A Câmara de Comércio dos Estados Unidos da América (USTDA), através da Associação de Empresas Públicas de TI do Brasil (ABEP), desenvolveu um estudo para Pernambuco denominado "Assistência Técnica para o Projeto de Data Center e Rede de Banda Larga de Pernambuco". Este documento é um relatório técnico detalhado que aborda vários aspectos de tecnologia da informação e comunicação. Ele se concentra na coleta de dados e estudos de caso sobre tendências tecnológicas, prioridades estratégicas de agências governamentais de TI, e a implementação de data centers e redes de banda larga híbridas. O relatório inclui análises de casos específicos em diferentes regiões e países, como o Arizona e a Califórnia nos Estados Unidos, bem como exemplos brasileiros como o PRODEST no Espírito Santo e a Caixa Econômica Federal. Além disso, discute os modelos de implementação e operação de data centers e redes de banda larga, incluindo modelos públicos, híbridos e parcerias público-privadas, focando em como estes modelos atendem às demandas de atividades de governo eletrônico. Deste documento, podem ser extraídas as seguintes necessidades de negócio:

1. **Modernização e Consolidação de Data Centers:** Enfocando na eficiência, qualidade de serviço, e segurança, este aspecto aborda a necessidade de atualizar a infraestrutura de TI para suportar serviços digitais governamentais.
2. **Expansão e Melhoria de Redes de Banda Larga:** Visa a inclusão digital e melhoria da administração pública, concentrando-se no desenvolvimento de redes de banda larga acessíveis e eficientes.
3. **Implementação de Soluções em Nuvem:** Focado na transição para nuvens híbridas, refletindo a necessidade de infraestrutura flexível e econômica para serviços de TI.
4. **Cibersegurança e Gestão de Riscos:** Destaca a importância da segurança cibernética no contexto de uma infraestrutura de TI cada vez mais digitalizada e conectada.

5. **Atendimento às Demandas de Serviços de Governo Eletrônico:** Como educação a distância, telemedicina e administração interna, ressaltando a necessidade de infraestrutura de TI que suporte uma ampla gama de serviços digitais governamentais.

Dos documentos desenvolvidos ao longos dos últimos anos pelo CETIC.br, podemos destacar as seguintes NNs:

1. **Digitalização de Serviços Públicos:** Há uma ênfase na melhoria e na adaptação dos processos de digitalização de serviços, incluindo a inclusão da visão dos cidadãos no processo de digitalização e a experimentação com abordagens de design de serviços focados nas pessoas. Isto é essencial para tornar o governo mais responsivo e os serviços de melhor qualidade 1 - TIC Provedores, página 269.

2. **Inovação em Governança e Tecnologia da Informação:** A gestão e governança em saúde digital baseada em boas práticas podem contribuir para a melhoria da qualidade dos serviços oferecidos, redução de custos operacionais, otimização do tempo de atendimento, ampliação do acesso à saúde e melhor atendimento para o paciente. Isto também inclui a gestão adequada de dados e informações para garantir a segurança e a privacidade dos pacientes 1 - TIC Provedores, página 919.

3. **Implementação de Estratégias Inclusivas de Digitalização:** Reconhece a necessidade de implementar estratégias baseadas em modelos híbridos e inclusivos, já que iniciativas de "tamanho único" e digitais por padrão tendem a excluir populações marginalizadas 1 - TIC Provedores, página 260.

4. **Desenvolvimento de Habilidades Digitais:** A ampliação das habilidades digitais é fundamental para garantir que os usuários da Internet obtenham benefícios a partir do uso da rede, promovendo a conscientização e a segurança digital dos usuários 1 - TIC Provedores, página 415.

5. **Transparência e Proteção de Dados Pessoais:** Enfatiza a importância de considerar transparência e privacidade desde o início da concepção de novos sistemas e serviços digitais 1 - TIC Provedores, página 282.

6. **Capacitação e Desenvolvimento de Competências Individuais e Organizacionais:** Buscar construir e disseminar competências individuais e organizacionais que aumentem a capacidade do governo de aprender e se adaptar às mudanças nas necessidades da sociedade 1 - TIC Provedores, página 270.

7. **Adequação Legal e Boas Práticas de Privacidade e Proteção de Dados:** A importância de um aprendizado contínuo em relação à privacidade e proteção de dados, remontando às exigências do Marco Civil da Internet e adequação à LGPD, especialmente para empresas provedoras que lidam intensamente com coleta, guarda e tratamento de dados pessoais 1 - TIC Provedores, página 470.

8. **Segurança Digital e Mitigação de Riscos:** É crucial que os provedores mantenham atualizadas suas ações de mitigação dos riscos de segurança digital, considerando ataques digitais que podem levar ao vazamento de dados sensíveis 1 - TIC Provedores, página 470.

9. **Capacitação em Informática em Saúde:** Refere-se à necessidade de uma matriz de competências em informática em saúde, abrangendo conhecimentos em sistemas de informação, gestão de dados e informações, e segurança da informação em saúde 1 - TIC Provedores, página 949.

10. **Governança de Dados na Saúde Digital:** As boas práticas e o arcabouço jurídico voltados à proteção de dados devem estar presentes na governança da saúde digital, com medidas investigadas pela pesquisa, como a existência de políticas de segurança da informação 1 - TIC Provedores, páginas 19-20.

11. **Conscientização Interna sobre a LGPD:** Aumento da conscientização interna sobre a LGPD em estabelecimentos de saúde, incluindo a nomeação de encarregados de segurança de dados e implementação de planos de resposta a incidentes de segurança de dados 1 - TIC Provedores, página 921.

12. **Promoção da Alfabetização e Segurança Digital dos Usuários:** Esforços devem ser feitos para capacitar usuários, promovendo conscientização e segurança digital, com a finalidade de aumentar a confiabilidade no uso de aplicações digitais 1 - TIC Provedores, página 1837.

13. **Proteção de Dados Sensíveis:** Proteger rigorosamente dados sensíveis é crucial para a efetivação da igualdade e liberdade das pessoas, estimulando processos de adequação que incluem a criação de normas internas condizentes com a legislação 1 - TIC Provedores, página 365.

A partir da Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto Nº 11.856, várias necessidades de negócio (NNs) podem ser identificadas para entidades e organizações que operam no Brasil. Estas NNs incluem:

- **Desenvolvimento de Tecnologias de Segurança Cibernética:** Investir no desenvolvimento de produtos, serviços e tecnologias nacionais destinados à segurança cibernética, adequados às necessidades e regulamentos locais.
- **Fortalecimento da Infraestrutura de Segurança de Dados:** Garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados no processamento e armazenamento de informações.
- **Educação e Capacitação em Segurança Cibernética:** Desenvolver programas de educação e capacitação técnico-profissional em segurança cibernética, visando a conscientização e a preparação de profissionais e cidadãos.
- **Gestão de Riscos e Resiliência Cibernética:** Implementar medidas de proteção cibernética e gestão de riscos para prevenir, mitigar e neutralizar vulnerabilidades e ataques cibernéticos, aumentando a resiliência organizacional.
- **Combate a Crimes Cibernéticos:** Contribuir para o combate aos crimes cibernéticos e ações maliciosas no ciberespaço, desenvolvendo estratégias e ferramentas eficientes para a detecção e resposta a tais ameaças.
- **Fomento à Pesquisa e Inovação em Segurança Cibernética:** Estimular atividades de pesquisa científica, desenvolvimento tecnológico e inovação relacionadas à segurança cibernética, visando a criação de soluções avançadas e eficazes.
- **Cooperação e Intercâmbio de Informações de Segurança:** Promover a atuação coordenada e o intercâmbio de informações de segurança cibernética entre diferentes setores, incluindo a colaboração internacional.
- **Desenvolvimento de Mecanismos de Regulação e Controle:** Criar e implementar mecanismos de regulação, fiscalização e controle para aprimorar a segurança e a resiliência cibernéticas no âmbito nacional.

Estas necessidades de negócio refletem a importância de uma abordagem integrada e proativa em relação à segurança cibernética, abrangendo desde a infraestrutura tecnológica até a conscientização e capacitação em todos os níveis organizacionais.

Baseando-se nas informações extraídas do documento da Estratégia Nacional de Segurança Cibernética, as necessidades de negócio que podem ser identificadas são as seguintes:

- **Estabelecimento e Consolidação de Parcerias Estratégicas:** A necessidade de formar e solidificar parcerias estratégicas entre o governo, empresas privadas, a academia e a sociedade em geral, visando a segurança cibernética, destaca-se como uma necessidade de negócio crucial. Essas parcerias são fundamentais para abordar as responsabilidades compartilhadas na proteção das infraestruturas críticas e na promoção de um ambiente digital seguro;

- **Coordenação entre Diversos Atores do Ambiente Cibernético:** Identifica-se a necessidade de melhor coordenação e cooperação entre os vários atores envolvidos direta ou indiretamente com a segurança cibernética. Isso inclui a criação de canais de comunicação eficientes que permitam a inclusão de várias perspectivas e especialidades na elaboração, implementação e promoção de políticas públicas de segurança cibernética;
- **Criação de Mecanismos de Compartilhamento de Informações sobre Riscos Cibernéticos:** A necessidade de desenvolver e implementar sistemas para o compartilhamento de informações sobre ameaças e vulnerabilidades cibernéticas é essencial. Esses mecanismos ajudariam na identificação, gestão e mitigação de riscos, permitindo que as organizações previnam, avaliem e gerenciem riscos de forma mais eficaz.
- **Desenvolvimento de Planos de Ação Conjuntos e Mecanismos de Coordenação Efetivos:** Destaca-se a importância de construir planos de ação em colaboração e estabelecer mecanismos de coordenação que sejam eficazes para enfrentar os desafios da segurança cibernética de maneira unificada.

Essas necessidades refletem um entendimento abrangente da segurança cibernética não apenas como um desafio técnico, mas também como uma questão que requer uma abordagem colaborativa e integrada, envolvendo múltiplos setores e atores.

Com base no contexto e informações fornecidas no Edital de Chamamento Público Nº 0001/2023 – SAD/SECTI/SEPE, as Necessidades de Negócio (NNs) que poderiam ser extraídas são:

- **Melhoria da Infraestrutura de Conectividade:** A necessidade de expandir e modernizar a infraestrutura de rede para conectar os 185 municípios e o arquipélago de Fernando de Noronha do Estado de Pernambuco, superando as limitações da rede PE CONECTADO atual.
- **Suporte ao Governo Digital:** Implementar uma infraestrutura de TIC que possa sustentar a transformação digital dos serviços públicos, garantindo a eficiência operacional e a capacidade de atender às demandas futuras.
- **Acessibilidade e Inclusão Digital:** Assegurar que a rede de conectividade seja acessível a todas as localidades, independentemente da localização geográfica ou condição socioeconômica, promovendo inclusão digital e reduzindo desigualdades sociais.
- **Atendimento a Requisitos Regulatórios e Legais:** Cumprir os requisitos administrativos e regulatórios existentes, garantindo transparência e acesso à informação, e atendendo a legislações e normativas que regem a prestação de serviços públicos.
- **Melhoria da Resposta a Emergências:** Utilizar a infraestrutura de rede para facilitar uma resposta rápida e coordenada a crises ou emergências, como pandemias ou desastres naturais.
- **Capacidade e Alta Disponibilidade:** Construir uma rede com capacidade suficiente e alta disponibilidade para suportar todos os serviços corporativos críticos do governo, como folha de pagamento e emissão de licenciamentos, e garantir a continuidade dos serviços públicos.
- **Atualização Tecnológica:** Adaptar a infraestrutura de TIC às rápidas mudanças e inovações tecnológicas do setor, garantindo que a rede seja capaz de suportar tecnologias emergentes e uso específico para a gestão pública.
- **Segurança da Informação:** Implementar uma nuvem de segurança hospedada integralmente no Brasil, com serviços adequados para proteger a integridade e a confidencialidade dos dados e informações gerenciados pela rede do governo.
- **Eficiência e Redução de Custos:** Otimizar os processos e reduzir a burocracia e os custos operacionais por meio da digitalização de documentos e serviços, proporcionando uma gestão de registros mais eficiente.

- **Sustentabilidade da Infraestrutura:** Estabelecer mecanismos para o reinvestimento contínuo na infraestrutura de rede, assegurando sua sustentabilidade e atualização tecnológica constante.

O Marco Civil da Internet, formalmente conhecido como Lei Nº 12.965, estabelecido em abril de 2014 no Brasil, estabelece princípios, garantias, direitos e deveres para o uso da Internet no país. A partir desse marco regulatório, diversas necessidades de negócio podem emergir para organizações que operam na Internet, especialmente aquelas que têm grande interação com dados de usuários ou que fornecem serviços online. Algumas dessas necessidades podem incluir:

- **Privacidade e Proteção de Dados:** O Marco Civil exige o respeito à privacidade do usuário e a proteção de seus dados pessoais. Isso implica em necessidades de negócios relacionadas à implementação de políticas e tecnologias de segurança da informação, governança de dados, e compliance relacionado à proteção de dados pessoais;
- **Neutralidade da Rede:** A lei garante a neutralidade da rede, proibindo os provedores de Internet de discriminar ou degradar o tráfego de dados. Empresas que fornecem serviços na Internet podem precisar revisar suas práticas operacionais e técnicas para assegurar a aderência a este princípio, o que pode incluir investimentos em infraestrutura de rede e tecnologias de gerenciamento de tráfego;
- **Responsabilidade dos Provedores de Serviços de Internet:** O Marco Civil define claramente as responsabilidades legais dos provedores de conexão e aplicações na Internet, especialmente em relação ao conteúdo gerado pelos usuários. Isso cria necessidades de negócio relacionadas ao monitoramento, moderação e remoção de conteúdos ilícitos, além da implementação de mecanismos de notificação e retirada de conteúdos;
- **Liberdade de Expressão:** A lei protege a liberdade de expressão online, o que pode levar as empresas a revisar suas políticas de conteúdo e moderação para garantir que não estejam infringindo os direitos dos usuários;
- **Armazenamento de Registros:** O Marco Civil obriga os provedores de conexão a armazenar determinados registros de acesso por um período mínimo, o que implica na necessidade de sistemas de armazenamento seguro e políticas de retenção de dados que estejam em conformidade com a legislação;
- **Transparência e Informação ao Usuário:** A necessidade de informar claramente aos usuários sobre coleta, uso, armazenamento e tratamento de seus dados, bem como sobre as políticas de uso dos serviços, exige que as empresas desenvolvam e mantenham processos claros de comunicação e transparência;
- **Resposta a Incidentes e Violações de Segurança:** A necessidade de implementar procedimentos eficazes para resposta a incidentes de segurança, incluindo a notificação de usuários e autoridades em caso de violações significativas de dados.

Essas necessidades de negócio exigem que as empresas que operam online no Brasil, ou que processam dados de cidadãos brasileiros, invistam em tecnologia, treinamento, políticas internas e procedimentos legais para garantir a conformidade com o Marco Civil da Internet, além de se adaptar às expectativas e exigências dos usuários e autoridades regulatórias.

Ao adotar a ISO/IEC 27001:2022 como norteador da implantação de um sistema de gestão de segurança da informação (SGSI), podem ser geradas diversas necessidades de negócio para uma organização, refletindo a importância de estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). As principais são:

1. **Conformidade e Governança:** A necessidade de estabelecer um framework de governança que assegure a conformidade com leis, regulamentos e contratos relacionados à segurança da informação, incluindo proteção de dados pessoais, direitos de propriedade intelectual, e requisitos setoriais específicos.

2. **Gestão de Riscos:** Implementar uma abordagem sistemática e contínua para a identificação, avaliação e tratamento de riscos de segurança da informação, alinhada com os objetivos estratégicos da organização.
3. **Proteção de Ativos de Informação:** Identificar e classificar ativos de informação críticos e sensíveis, e desenvolver mecanismos adequados para sua proteção contra ameaças e vulnerabilidades, garantindo a confidencialidade, integridade e disponibilidade desses ativos.
4. **Capacitação e Conscientização:** Desenvolver programas de treinamento e conscientização em segurança da informação para funcionários, contratados e outras partes interessadas, visando a promover uma cultura de segurança da informação.
5. **Resposta a Incidentes e Continuidade de Negócios:** Estabelecer e manter planos de resposta a incidentes de segurança da informação e de continuidade de negócios para garantir a resiliência organizacional frente a incidentes e desastres.
6. **Melhoria Contínua:** Implementar um processo de melhoria contínua que permita à organização acompanhar a evolução das ameaças de segurança da informação, bem como a eficácia dos controles implementados.
7. **Relacionamento com Terceiros:** Gerenciar os riscos associados ao compartilhamento de informações e ao acesso a sistemas por terceiros, incluindo fornecedores, clientes e parceiros, exigindo a implementação de controles adequados e a realização de avaliações de segurança.
8. **Inovação e Transformação Digital:** Avaliar e adaptar as práticas de segurança da informação às novas tecnologias e modelos de negócio, como cloud computing, Internet das Coisas (IoT) e inteligência artificial, para suportar a inovação e a transformação digital de forma segura.
9. **Transparência e Confiança:** Demonstrar a clientes, parceiros e reguladores o comprometimento da organização com a segurança da informação, aumentando a confiança e potencialmente criando vantagens competitivas.

Estas necessidades refletem a importância de integrar a segurança da informação às práticas de negócio da organização, garantindo que a gestão de segurança da informação seja um componente central da estratégia organizacional, operações diárias e iniciativas de inovação.

Identificador da NN	Descrição	Origem
NN 01	Garantir links de boa qualidade e alta capacidade de tráfego suficientes para suprir as necessidades das instituições do Governo de Pernambuco.	APE
NN 02	Garantir segurança cibernética quando utilizando os links contratados.	APE
NN 03	Garantir alta disponibilidade e resiliência a falhas na comunicação.	APE
NN 04	Garantir recursos de segurança para proteção dos ativos que componham	APE

	as aplicações disponibilizadas nos Data Centers do Governo de Pernambuco.	
NN 05	Garantir a possibilidade de contingenciamento de links no equipamento de segurança nos endereços solicitados (última milha).	APE
NN 06	Garantir recursos de segurança para proteção dos ativos que componham as aplicações disponibilizadas pelos órgãos que utilizem IPs do AS do estado.	APE
NN 07	Garantir a integração com o serviço de telefonia fixa e portabilidade dos ramais do serviço atual para o novo.	APE
NN 08	Garantir que todos os usuários da rede em todas as localidades sejam autenticados para disponibilização do acesso à internet por soluções providas pelo governo do estado de Pernambuco ou Governo Federal ou por redes sociais.	APE
NN 09	Garantir o cumprimento dos Níveis Mínimos de Serviços (NMS) definidos pelo contratante.	APE
NN 10	Garantir links com características específicas conforme necessidade do contratante.	APE
NN 11	Garantir o monitoramento e gestão de links, ativos e segurança cibernética de forma centralizada.	APE
NN 12	Garantir um ponto único de entrada para abertura de incidentes e solicitações pelas localidades aderentes.	APE
NN 13	Garantir aderência às especificações contidas no termo de referência dos itens contratados.	APE
NN 14	Garantir o acompanhamento mensal da gestão da qualidade com a contratada.	ATI

NN 15	Garantir a disponibilização de acesso à rede sem fio com as tecnologias emergentes, com segurança cibernética e alta disponibilidade.	APE
NN 16	Garantir a permissão da atuação de um verificador independente para execução de auditoria dos serviços contratados.	APE
NN 17	Garantir a abertura e acompanhamento das ordens de serviço emitidas pelas instituições para o provimento dos serviços de telemática através de um sistema de Gestão.	APE
NN 18	Garantir o monitoramento de ativos de rede que componham a infraestrutura do serviço de conectividade da rede corporativa indicados pela contratante e que não pertençam a contratada.	APE
NN 19	Garantir a otimização dos custos operacionais com a infraestrutura de rede e serviços de segurança, assegurando que os recursos financeiros sejam alocados de forma eficiente e sustentável, com previsibilidade de gastos ao longo do tempo.	APE
NN 20	Garantir a continuidade dos contratos corporativos de voz (Pontos de Voz Fixo -PVF, Contact Center- CC e Comunicação Unificada - UC).	APE
NN 21	Os princípios de segurança da informação devem nortear o desenho dos serviços de TI desta licitação e licitações consequentes.	APE
NN 22	As empresas prestadoras dos serviços devem trabalhar buscando sinergias sempre que possível para agilizar as respostas a incidentes de segurança da informação.	APE

### 5.3. NECESSIDADES TECNOLÓGICAS

A seguir, apresentamos uma tabela detalhada das Necessidades Tecnológicas (NTs) essenciais para o projeto da Nova Rede Corporativa. Esta tabela abrange padrões, capacidades, metodologias, processos e competências das equipes, com especial atenção à segurança da informação. As especificações aqui listadas são fundamentais para garantir que a solução proposta atinja os resultados de negócio almejados, incluindo sua infraestrutura, capacidade organizacional, práticas estabelecidas e planejamento estratégico.

Esta lista, composta por bens e serviços essenciais, inclui desde equipamentos e serviços de instalação ou configuração até produtos finais, capacitações e demandas de áreas interdependentes. Cada item foi cuidadosamente definido para assegurar que as Necessidades Tecnológicas estejam plenamente alinhadas com os objetivos estratégicos da Nova Rede Corporativa, viabilizando a realização das Necessidades de Negócio.

A tabela a seguir oferece uma visão organizada dessas necessidades, facilitando a visualização das demandas tecnológicas que sustentam o projeto da Nova Rede Corporativa.

Identificador da NT	Descrição	Origem
NT 01	Processo de gestão de endpoint envolvendo a implantação, configuração, manutenção e monitoramento de softwares que protegem os endpoints contra ameaças, garantindo também a conformidade com as políticas de segurança da organização.	APE
NT 02	Solução de monitoramento de ativos projetada para gerenciar ativos como sistemas, servidores e firewalls, com o objetivo de garantir a eficiência operacional desses ativos e, em caso de eventos ou incidentes, permitir que a equipe identifique e responda rapidamente, restaurando os ativos à normalidade.	APE
NT 03	Solução de gestão de ativos que mantenha um registro completo de todos os ativos de TI com suas informações detalhadas, facilitando auditorias, auxiliando a conformidade de políticas e regulamentos e facilitando a identificação de possibilidade de otimização, e acompanhamento do ciclo de vida, possibilitando a eficiência das operações, manutenções e atualiza-	APE

	ção de software e segurança.	
NT 04	Solução de gerenciamento de serviços de TI que gerencie e otimize os serviços de tecnologia, melhorando a eficiência, a qualidade e a entrega de serviços, ajudando na gestão de incidentes, problemas e mudanças, com o registro de tickets e a possibilidade de troca de filas de atendimento, bem como o acompanhamento dos níveis de serviço para registro e monitoramento de estouro de tempo ou atendimento dentro do prazo pré-estabelecido.	APE
NT 05	Processo de gerenciamento de usuários que garanta que apenas usuários autorizados tenham acesso aos recursos e informações, auxiliando na proteção contra ameaças internas e externas. Envolvendo vários aspectos que visam garantir a integridade, confidencialidade e disponibilidade dos dados.	APE
NT 06	Solução de gerenciamento de identidade de acesso com a capacidade de determinar o nível de acesso baseado em função e permissão. Sistema que irá realizar a gestão de funções e privilégios de acesso de usuário aos ativos e sistemas para atender as políticas e regulamentos implantados.	APE
NT 07	Solução de segurança de identidade que controle, monitore e audite o acesso a contas e recursos privilegiados em sistemas de TI. Protegendo credenciais de administradores e outros usuários com acesso privilegiado, reduzindo o risco de abuso ou uso indevido dessas contas.	APE
NT 08	Múltiplo fator de autenticação solicitando ao usuário de uma plataforma, um aplicativo ou um sistema que confirme sua identidade em dois ou mais momentos, antes de liberar o	APE

	acesso dele ao sistema.	
NT 09	Solução de segurança de confiança zero que verifique a identidade e a segurança de cada usuário e dispositivo antes de conceder acesso a recursos de rede, independentemente de sua localização.	APE
NT 10	Processo de campanha de segurança da informação para promover a conscientização e a adoção de práticas seguras em uma organização.	APE
NT 11	Solução de filtro de mensagens indesejadas que reduza ou elimine o recebimento de mensagens não solicitadas, geralmente de natureza comercial ou promocional, enviadas em massa por e-mail.	APE
NT 12	Processo de monitoramento de alertas de segurança, que sejam emitidos por ferramentas de correlação e monitoramento, onde o time responsável realize a tratativa e resposta.	APE
NT 13	Solução de monitoramento e análise de eventos de segurança, software que centralize a coleta, armazenamento, e correlação de LOGs para tratar um evento ou incidente de segurança, provendo uma resposta mais rápida e assertiva. Podendo ser coletados eventos gerados por diversas aplicações de segurança, como firewalls, IPS, IDS, Antivírus, ou qualquer outro equipamento que se tenha na rede.	APE
NT 14	Profissionais responsáveis por monitoramento proativo dos links, ativos e das operações de segurança, bem como atividades relacionadas a configurações de segurança, relatoria e atendimento de incidentes e requisições reativos. Time que atue 24x7.	APE
NT 15	Processo de gestão de incidentes de	APE

	segurança da informação com um conjunto de etapas estruturadas com o propósito de lidar com eventos que comprometam a confidencialidade, integridade ou disponibilidade dos dados da organização (Incidente de segurança).	
NT 16	Plano de resposta a incidentes que auxilie na tratativa com incidentes de segurança da informação, ataques cibernéticos, entre outras situações que possam comprometer um ou mais pilares da segurança da informação.	APE
NT 17	Equipe composta por um time multidisciplinar, composto por diversos profissionais especialistas em vários segmentos de TI e segurança. Time que atue de segunda a sexta das 8h às 18h e tenha regime de plantão para casos de incidentes ou necessidades de acionamento por parte do time de analistas de primeiro nível.	APE
NT 18	Solução de filtro de aplicativos web que proteja aplicações web contra ataques cibernéticos, como injeção de SQL, cross-site scripting (XSS) e outros tipos de ataques comuns a aplicações web. Que monitore, filtre e bloqueie o tráfego HTTP e HTTPS entre um aplicativo web e a internet para detectar e bloquear ataques maliciosos.	APE
NT 19	Solução unificada de segurança de rede com diversas soluções integradas compondo um único equipamento de borda para proteção de redes locais.	APE
NT 20	Solução de detecção e resposta para dispositivos finais fornecendo a capacidade de monitorar terminais quanto a comportamento suspeito e registrar cada atividade e evento fornecendo contexto crítico para detectar	APE

	ameaças avançadas e executando a atividade de resposta automatizada, como isolar um endpoint infectado da rede quase em tempo real.	
NT 21	Solução de detecção e resposta estendida que integre e correlacione dados de diversas fontes, como endpoints, servidores, e-mails, redes e nuvem, fornecendo uma visão mais abrangente e eficaz da postura de segurança da organização.	APE
NT 22	Solução para gerenciamento de acessos à rede que possa ser usada para restringir o acesso à rede, garantindo que apenas dispositivos autorizados e conformes com as políticas de segurança da organização possam se conectar e acessar recursos.	APE
NT 23	Solução de detecção de ameaças de rede que detecte e responda a ameaças na rede, monitorando o tráfego de rede em busca de comportamentos suspeitos ou indicativos de ataques. Que utilize análise de tráfego em tempo real e técnicas de detecção de ameaças para identificar e responder a atividades maliciosas.	APE
NT 24	Solução de automação de resposta a incidentes de segurança que realize gerenciamento de incidentes de segurança, integrando ferramentas de segurança para automatizar tarefas repetitivas e orquestrar a resposta a incidentes, aumentando assim a eficiência e eficácia dos times de segurança.	APE
NT 25	Processo de gestão de continuidade de serviços de TI que tenha como objetivo assegurar a manutenção e rápida restauração dos serviços de TI após interrupções ou desastres, minimizando o impacto dessas eventualidades nas operações da organização.	APE

NT 26	Processo de rotina de backup que tenha como objetivo realizar cópias de dados e arquivos importantes e armazená-los num local seguro.	APE
NT 27	Equipe formada por especialistas em segurança da informação, com atuação voltada para testes de simulação de ataques com o objetivo de identificar e corrigir vulnerabilidades antes que estas sejam exploradas.	APE
NT 28	Processo de gestão de vulnerabilidades que tenha como objetivo identificar, avaliar, corrigir e mitigar vulnerabilidades em sistemas e ativos, que podem ser decorrentes de configurações inadequadas, sistemas desatualizados ou outros pontos fracos exploráveis por ameaças, resultando em incidentes de segurança da informação.	APE
NT 29	Solução para varrer a rede em busca de vulnerabilidades construídas com o objetivo de identificar e analisar potenciais vulnerabilidades nos sistemas, redes e dispositivos.	APE
NT 30	Processo de testes de intrusão que realizem uma avaliação de segurança da organização, fazendo simulações de exploração de vulnerabilidades e ataques para localizar os principais pontos de falhas de segurança e corrigi-las o mais rápido possível, diminuindo assim as chances de sofrer um ataque real.	APE
NT 31	Soluções que proporcionem um ambiente de testes onde a rede seja simulada no máximo nível possível, de forma que todas as brechas sejam observadas e testadas, portanto, é crucial que no ambiente tenha-se os mesmos sistemas e serviços da rede real, por exemplo, firewall, servidores, versão de sistema operacional etc.	APE

NT 32	<p>Processo de gestão de riscos de segurança que determine a aplicação equilibrada de controles de segurança na organização, de acordo com o seu perfil de riscos de segurança.</p> <p>Possibilitando a diminuição da probabilidade de exposição ou perda resultante de uma vulnerabilidade sendo explorada por uma ameaça.</p>	APE
NT 33	<p>Solução de matriz de probabilidade e impacto que realize a gestão de riscos de uma organização, composta por duas informações, que se trata justamente da probabilidade de um risco ocorrer, representada por porcentagem, escala ou qualquer outra forma preferível pela organização, e caso ele ocorra, qual será o impacto e as consequências para a organização, geralmente representado por escala (baixa, média, alta).</p>	APE
NT 34	<p>Processos, políticas e soluções com embasamento na norma ISO/IEC 27005 para que forneça diretrizes e princípios para a gestão de riscos de segurança da informação. Que especifique os processos e as atividades para a gestão de riscos de segurança da informação, com o objetivo de ajudar as organizações a identificar, avaliar e tratar os riscos associados à segurança da informação.</p>	APE
NT 35	<p>Processos, políticas e soluções com embasamento na norma ISO/IEC 27002 para que oriente a gestão da segurança da informação, oferecendo diretrizes e princípios. Com o propósito de auxiliar as organizações na implementação de controles de segurança da informação e na criação de um Sistema de Gestão da Segurança da Informação.</p>	APE
NT 36	<p>Processo de gestão de conformidade que tenha como objetivo garantir que a organização esteja seguindo os pa-</p>	APE

	drões regulatórios, leis, normas, políticas, frameworks adotados, ou qualquer outra diretriz relacionada a segurança da informação que a empresa esteja comprometida.	
NT 37	Processo de gestão da qualidade da segurança da informação que integre o processo de gestão da qualidade com as boas práticas de segurança da informação na organização, estabelecendo um conjunto de atividades e práticas destinadas a assegurar a proteção eficaz dos ativos e informações contra ameaças, bem como o gerenciamento eficiente desses recursos.	APE
NT 38	Equipe responsável por monitoramento proativo do centro de operações de segurança satélite, bem como atividades relacionadas a configurações de segurança, relatoria e atendimento de incidentes e requisições reativos. Time que atue com todos os processos, tecnologias e pessoas (mesmos conhecimentos) do centro de operações de segurança da ATI (equipe coordenadora).	APE
NT 39	Profissional que atuará liderando e gerenciando as operações de segurança do centro de operações de segurança para garantir que as atividades sejam realizadas de maneira eficiente e eficaz.	APE
NT 40	Profissional responsável por atender os clientes de forma especializada, entendendo suas necessidades, analisando requisitos de conectividade e segurança, propondo soluções adequadas, oferecendo suporte técnico, coordenando equipes técnicas, e monitorando e realizando manutenção das soluções implementadas.	APE
NT 41	Equipe responsável por receber e registrar os tickets de incidentes e	APE

	solicitações dos clientes, além de fornecer suporte inicial e encaminhar os tickets para a equipe especializada, quando necessário.	
NT 42	Profissional responsável por gerenciar o escalonamento dos tickets para o suporte da provedora de links, garantindo que os problemas sejam resolvidos dentro dos prazos acordados.	APE
NT 43	Profissionais responsáveis por garantir a aderência às especificações contidas no termo de referência dos itens contratados, a qualidade do projeto e a satisfação do contratante.	ATI
NT 44	Equipe responsável por fornecer suporte técnico especializado para resolver problemas relacionados à conectividade e garantir o funcionamento adequado dos links de comunicação.	APE
NT 45	Solução de rede sem fio com segurança responsável por fornecer conectividade sem fio segura, com foco na proteção dos dados e na prevenção de ameaças.	APE
NT 46	Gerenciamento de ativos de rede que componham a infraestrutura do serviço de conectividade da rede corporativa indicados pela contratante e que não pertençam a contratada.	APE
NT 47	Portfólio com diversas opções de links conforme especificado no termo de referência.	APE
NT 48	Solução compondo dupla abordagem para garantir alta disponibilidade e desempenho da comunicação.	APE
NT 49	Solução de links de multitecnologias para garantir alta disponibilidade e desempenho da comunicação.	APE
NT 50	Adequação, manutenção e sustentação do sistema de gestão das ordens	APE

	de serviço de propriedade do estado.	
NT 51	Garantir e possibilitar acesso aos ambientes e sistemas da contratada e dos contratantes para realização de auditoria dos serviços contratados.	APE
NT 52	Prover um serviço de telefonia fixa corporativa integrado a rede pública de telefonia (PVFs).	APE
NT 53	Prover um serviço de Contact Center (CC) corporativo para o Estado, contemplando integrações com redes sociais e aplicativos de mensageria populares.	APE
NT 54	Prover um serviço de Comunicação Unificada (UC) corporativo para o Estado.	APE
NT 55	Prover um serviço de voz corporativo em concordância com as recomendações dos especialistas em segurança da informação do serviço central de segurança (SOC).	APE

#### 5.4. REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

As soluções de conectividade e segurança requeridas devem atender a uma ampla gama de requisitos funcionais e não funcionais para garantir a eficácia e a segurança das comunicações e dados. Os requisitos funcionais abrangem desde a capacidade de estabelecer e manter conexões seguras até a capacidade de gerenciar e monitorar o tráfego de rede de forma eficiente. Já os requisitos não funcionais incluem a conformidade com padrões de segurança reconhecidos, a escalabilidade para lidar com aumentos na demanda de tráfego e a capacidade de recuperação rápida em caso de falhas. A solução deve garantir a integridade, confidencialidade e disponibilidade dos dados, atendendo às necessidades de conectividade e segurança do poder executivo e outros poderes do estado de Pernambuco de forma abrangente e eficaz. Abaixo o detalhamento dos requisitos de cada solução mapeada:

##### Processo de gestão de dispositivos finais

Funcionais: Inventário, proteção, atualizações, controle de acesso, criptografia, monitoramento e detecção, relatórios.

Não funcionais: Desempenho, segurança, disponibilidade, escalabilidade, facilidade de uso.

##### Solução de monitoramento de ativos

Funcionais: monitoramento de desempenho, gestão de configuração, monitoramento de disponibilidade, gestão de inventário, alertas e notificações, filtros.

Não funcionais: acesso remoto, controle de acessos, acessos simultâneos.

### **Solução de gerenciamento de ativos**

Funcionais: inventário de ativos de hardware, inventário de ativos de software, inventário de ativos em nuvem, inventário de ativos móveis, descoberta de ativos, painel central, gestão de política de ativos, integrações.

Não funcionais: gerenciamento de riscos, correlação inteligente de eventos, análise rápida de causa raiz, gerenciamento proativo de mudanças, cobertura abrangente de dispositivos e plataformas, visualizações e interfaces personalizadas e baseadas em funções, isolamento de falhas e análise de causa raiz, relatórios, suporte abrangente de infraestrutura, extensibilidade de monitoramento flexível, modelagem de rede robusta, monitoramento e cobertura de rede de gerenciamento.

### **Solução de gerenciamento de serviços de TI**

Funcionais: Gerenciamento de mudanças, gestão de ativos, relatórios, fluxo de trabalho do processo, console de administração, gerenciamento de acesso, sistema de tickets.

Não funcionais: Alertas, automação, registro de desempenho.

### **Processo de gerenciamento de usuários**

Funcionais: Criação de contas de usuário, autenticação e autorização, gerenciamento de perfis de usuário, reset de senha, desativação de contas.

Não funcionais: Segurança, desempenho, escalabilidade, disponibilidade, confiabilidade.

### **Solução de gerenciamento de identidade de acesso**

Funcionais: MFA, RBAC, Ciclo de vida, Conformidade, SSO, Gestão de identidade.

Não funcionais: Segurança, desempenho, escalabilidade, disponibilidade, confiabilidade.

### **Solução de segurança de identidade**

Funcionais: Gerenciamento centralizado de credenciais privilegiadas, controle de acesso baseado em políticas, monitoramento e registro de atividades privilegiadas, capacidade de análise de comportamento para detectar atividades suspeitas, integração com sistemas de gerenciamento de identidade e acesso.

Não funcionais: Desempenho, escalabilidade, segurança, disponibilidade, facilidade de uso.

### **Solução de múltiplo fator de autenticação**

Funcionais: Suporte a múltiplos fatores, integração com sistemas existentes, facilidade de uso, gestão de políticas, relatórios e auditoria.

Não funcionais: Segurança, desempenho, escalabilidade, disponibilidade, confiabilidade.

### **Solução de segurança de confiança zero**

Funcionais: Autenticação multifatorial, autorização baseada em políticas, criptografia, visibilidade e controle sobre o acesso à rede e atividades dos usuários, integração com outros sistemas de segurança e gerenciamento de identidade.

Não funcionais: Desempenho, escalabilidade, segurança, disponibilidade, facilidade de uso.

### **Processo de campanhas de conscientização**

Funcionais: Conteúdo educativo, acessibilidade, feedback e avaliação, personalização.

Não funcionais: Engajamento, impacto, sensibilização, aderência às normas e regulamentações.

### **Solução de filtro de mensagens indesejadas**

Funcionais: Listas negras, análise de conteúdo, verificação de reputação, bloqueio de IP, Listas brancas, desafios de verificação.

Não funcionais: Desempenho, precisão, escalabilidade, disponibilidade.

### **Processo de monitoramento de alertas**

Funcionais: Recepção de alertas, correlação de alertas, análise de alertas, gestão de incidentes, notificação de

alertas.

Não funcionais: Desempenho, escalabilidade, disponibilidade, segurança, integração.

#### **Solução de monitoramento e análise de eventos de segurança**

Funcionais: coleta de logs a partir de qualquer fonte, normalização dos logs, categorização, indexação, correlação de logs, detecção, alertas, análise, análise de comportamento, mapeamento de alertas no mitre att&ck, integração com SOAR/EDR/XDR.

Não funcionais: Conformidade com a LGPD, Dashboards personalizáveis, relatórios personalizáveis, fontes de threat intelligence, UEBA, escalável, monitoramento em tempo real, capacidade de processamento de grande volume de dados, acessos individuais a ferramenta para os analistas, sem limite de acessos simultâneos.

#### **Analistas de nível 1**

Funcionais: Formação em redes de computadores ou segurança da informação, experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

#### **Processo de gestão de incidentes**

Funcionais: Preparação, detecção, análise, resposta, recuperação, lições aprendidas.

Não funcionais: Baseado na ISO/IEC, baseado no NIST, baseado no ITIL.

#### **Processo de resposta a incidentes**

Funcionais: detecção de incidentes, análise de incidentes, classificação de incidentes, notificação de incidentes, contenção de incidentes, investigação de incidentes, resposta imediata.

Não funcionais: baseado em padrões de segurança como NIST e ISO/IEC 27001, documentação e registros, avaliação pós-incidente, melhoria contínua, integração com outras áreas.

#### **Grupo de especialistas**

##### **Especialista em segurança de dispositivos finais**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos, Experiência em análise e investigação de incidentes e eventos em endpoints, Experiência em implantação e suporte de EDR/XDR.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

##### **Especialista em segurança de rede sem fio**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores, Certificação CWSP (Certified Wireless Security Professional) ou similar.

##### **Especialista em firewall de borda**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores, Certificação CISSP (Certified Information Systems Security Professional).

##### **Especialista em firewall dos clientes**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos, Experiência em análise e investigação de incidentes e eventos em firewalls, Experiência em implantação, configuração e suporte de firewalls.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

##### **Especialista em segurança de perímetro de rede local**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs,

monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos, Experiência em análise, investigação e resposta a eventos de segurança.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Especialista em solução de monitoramento e análise de eventos de segurança**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Fornecimento de treinamentos técnicos, Experiência em análise, investigação e resposta a eventos de segurança, Experiência em análise e investigação de incidentes e eventos em SIEM, Experiência em implantação, configuração e suporte de soluções de SIEM.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Especialista em conformidade**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Experiência em participação de auditorias de segurança da informação.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores, Certificação voltada para LGPD.

**Especialista forense**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Certificação CHFI (Computer Hacking Forensic Investigator) ou similar.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Especialista em falhas e desempenho**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Experiência no monitoramento de redes.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Especialista em solução de gerenciamento de serviços de TI**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Certificação ITIL Foundation v4 ou superior.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Especialista em processos**

Funcionais: Formação em redes de computadores ou segurança da informação, Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, Certificação ITIL Foundation v4 ou superior, Certificação CBPA (Certified Business Process Associate) ou superior.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

**Solução de filtro de aplicativos web**

Funcionais: Filtragem de tráfego HTTP e HTTPS, detecção e bloqueio de ataques comuns a aplicações web, personalização de políticas de segurança, relatórios e alertas sobre atividades de segurança, integração com outras soluções de segurança.

Não funcionais: Desempenho, escalabilidade, segurança, disponibilidade, facilidade de configuração e gerenciamento.

**Solução unificada de segurança de rede**

Funcionais: Firewall, antivírus/antimalware, IPS, Web filter, VPN, Application control, SD-WAN.

Não funcionais: Desempenho, escalabilidade, disponibilidade, segurança, facilidade de gerenciamento, compatibilidade.

**Solução de rede sem fio com segurança**

Funcionais: Conectividade segura, gestão de usuários, auditoria de segurança, compatibilidade.

Não funcionais: Desempenho, disponibilidade.

### **Solução de detecção e resposta para dispositivos finais**

Funcionais: Gestão de ativos, isolamento do sistema, inteligência de endpoint, detecção de malware, remediação automática, relatório de incidentes, análise comportamental.

Não funcionais: Desempenho, escalabilidade, disponibilidade, segurança, facilidade de integração, facilidade de uso.

### **Solução de detecção e resposta estendida**

Funcionais: Integração de dados de várias fontes de segurança, correlação de eventos para detecção avançada de ameaças, resposta automatizada a incidentes de segurança, análise de dados para fornecer insights acionáveis, suporte a padrões de segurança e interoperabilidade com outras soluções.

Não funcionais: Desempenho, escalabilidade, segurança, disponibilidade, facilidade de uso.

### **Solução para gerenciamento de acessos à rede**

Funcionais: Autenticação de dispositivos, autorização baseada em políticas, avaliação de conformidade de dispositivos, isolamento de dispositivos não conformes, integração com outros sistemas de segurança.

Não funcionais: Desempenho, escalabilidade, segurança, disponibilidade, facilidade de uso.

### **Solução de detecção e resposta a ameaças de rede**

Funcionais: Monitoramento contínuo do tráfego de rede, análise de tráfego em tempo real, detecção de ameaças baseada em comportamento, geração de alertas e relatórios, integração com outras soluções de segurança.

Não funcionais: Desempenho, escalabilidade, precisão na detecção de ameaças, segurança, facilidade de uso.

### **Solução de automação de resposta a incidentes de segurança**

Funcionais: Emissão de alertas, Acompanhamento de linha de base de desempenho, Visualização de dados, Inteligência de ameaças, Orquestração de Segurança, Correção Automatizada, Mapeamento de fluxo de trabalho, Automação de fluxo de trabalho.

Não funcionais: Alta disponibilidade/recuperação de desastres, Monitoramento de registros.

### **Solução de detecção e resposta estendidas gerenciadas**

Funcionais: Automação de resposta, Threat Intelligence, Detecção baseada em regras, Detecção em tempo real, Machine learning, Integração com qualquer equipamento ou solução de segurança (qualquer fabricante).

Não funcionais: Desempenho, escalabilidade, disponibilidade, segurança, facilidade de gerenciamento.

### **Processo de gestão de continuidade de serviços de TI**

Funcionais: análise de riscos, avaliação de impacto nos negócios, desenvolvimento de estratégia de continuidade, desenvolvimento e implementação de planos de continuidade, testes, conscientização, melhoria contínua.

Não funcionais: Compliance, eficiência, resiliência, agilidade, segurança.

### **Processo de rotina de backup**

Funcionais: agendamento de backup, seleção de dados, backup incremental, backup completo, armazenamento seguro, restauração de dados, notificações.

Não funcionais: desempenho, escalabilidade, disponibilidade, integridade dos dados, segurança, facilidade de gerenciamento.

### **Especialistas em testes de segurança ofensiva**

Funcionais: formação em segurança da informação ou sistemas da informação, certificações CEH, OSCP ou equivalentes, experiência em testes de invasão e exploração de vulnerabilidades, condução de treinamentos.

Não funcionais: experiência em testes de invasão e exploração de vulnerabilidades, habilidades de comunicação, capacidade de trabalhar sob pressão, pensamento crítico.

### Processo de gestão de vulnerabilidades

Funcionais: Identificação de vulnerabilidades, avaliação de vulnerabilidades, priorização de vulnerabilidades, correção de vulnerabilidades, monitoramento de vulnerabilidades, relatórios.

Não funcionais: eficiência, escalabilidade, integração, segurança, conformidade, disponibilidade.

### Solução de varredura de vulnerabilidades

Funcionais: verificações automatizadas, teste de conformidade, varredura de perímetro, monitoramento de configuração, análise de código estático, teste de caixa preta.

Não funcionais: desempenho, escalabilidade, segurança, facilidade de uso, relatórios, compatibilidade.

### Processos de testes de intrusão

Funcionais: Identificação de Vulnerabilidades, Exploração de Vulnerabilidades, Relatórios, Recomendação de Ações Corretivas, Repetibilidade.

Não funcionais: Segurança, descrição, escopo, compliance, documentação, tempo de execução.

### Solução para ambiente de testes

Funcionais: Criação de Ambientes de Testes, Configuração Personalizada, Simulação de Ataques, Análise de Vulnerabilidades, Relatórios.

Não funcionais: Desempenho, Segurança, Escalabilidade, Facilidade de uso, compatibilidade, documentação.

### Processo de gestão de Riscos

Funcionais: Identificação de Ativos, Identificação de Ameaças e Vulnerabilidades, Análise de Riscos, Avaliação de Riscos, Tratamento de Riscos, Monitoramento e Revisão.

Não funcionais: Escalabilidade, Integridade, Confidencialidade, Disponibilidade, Conformidade.

### Processo de gestão de Conformidade

Funcionais: mapeamento de requisitos de conformidade, avaliação de conformidade, monitoramento de conformidade, relatórios de conformidade, auditoria de conformidade, gestão de ações corretivas.

Não funcionais: Escalabilidade, integridade, confidencialidade, disponibilidade, conformidade com regulamentos.

### Processo de gestão da qualidade da segurança da informação

Funcionais: definição de políticas de segurança, implementação de controles de segurança, monitoramento de conformidade, avaliação de conformidade, melhoria contínua.

Não funcionais: Escalabilidade, integridade, confidencialidade, disponibilidade, conformidade com normas e regulamentos.

### Analistas do centro de operações de segurança satélite

Funcionais: Formação em redes de computadores ou segurança da informação, experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes.

Não funcionais: Certificações ISFS, CompTIA Security+ ou superiores.

### Liderança

Funcionais: Formação em Redes de Computadores ou Segurança da Informação, certificações em segurança da informação, experiência em segurança da informação e liderança.

Não funcionais: habilidades de liderança, gerenciamento de crises, visão estratégica, gestão de pessoas, comunicação.

### Especialista de atenção

Funcionais: Atendimento personalizado, análise de requisitos, suporte técnico, coordenação, monitoramento.

Não funcionais: Disponibilidade, confidencialidade, qualidade, atualização profissional.

### Service Desk

Funcionais: Registro de tickets, classificação e priorização, resolução inicial, escalonamento adequado.

Não funcionais: Disponibilidade, comunicação clara e eficiente, trabalho em equipe, resolução rápida e eficiente.

#### **Analista de suporte residente**

Funcionais: Escalonamento de tickets, acompanhamento de tickets, comunicação entre equipes.

Não funcionais: Disponibilidade, comunicação eficiente, escalonamento eficiente.

#### **Qualidade**

Funcionais: Gestão de processos, controle de qualidade, melhoria contínua, gestão de riscos.

Não funcionais: Disponibilidade, comunicação eficaz, orientação para resultados.

#### **Suporte da operadora**

Funcionais: Atendimento rápido, resolução de problemas, comunicação clara.

Não funcionais: Disponibilidade, eficiência, qualidade no atendimento.

#### **Verificador independente**

Funcionais: Escopo de auditoria, identificação de padrões e regulamentações relevantes, metodologia de auditoria, documentação e relatórios, recomendações e planos de ação, confidencialidade e integridade.

Não funcionais: Confiabilidade, desempenho, segurança, escalabilidade, usabilidade, conformidade, transparência, independência e imparcialidade.

#### **Telefonia fixa**

Funcionais: Realização de chamadas, recepção de chamadas, chamada em espera, desvio de chamadas, transbordo de chamadas, conferência de chamadas, relatórios detalhados de chamadas, monitoramento de QoS específico do serviço de telefonia fixa,, compatibilidade com aparelhos IP, preferencialmente sem fio (WIFI e DECT).

Não funcionais: Alta disponibilidade, baixa latência em chamadas, qualidade de voz clara e sem interrupções, capacidade de suportar um grande número de chamadas simultâneas, escalabilidade, facilidade de manutenção, facilidade de uso, cumprimento das regulamentações locais e internacionais, e conformidade com normas de segurança e privacidade.

#### **Links multitecnologia e/ou específicos**

Funcionais: Capacidade e velocidade, disponibilidade, confiabilidade, baixa latência, desempenho, segurança, redundância, failover, suporte, monitoramento, escalabilidade.

Não funcionais: Confiabilidade, desempenho, segurança, escalabilidade, manutenibilidade, usabilidade, conformidade, custo-efetividade.

#### **Proteção de DNS**

Funcionais: Filtragem de conteúdo, proteção contra malware e phishing, mitigação de ataques DDoS, segurança e integridade com DNSSEC, monitoramento e geração de relatórios, definição de políticas de acesso.

Não funcionais: Garantia de disponibilidade e integridade do serviço de DNS, eficiência na autenticação de respostas DNS, desempenho da solução em situações de ataque.

#### **Guarda de LOGs e relatoria**

Funcionais: Coleta de LOGs de múltiplas fontes, armazenamento seguro de LOGs, retenção de LOGs para conformidade, análise e correlação de LOGs, geração de relatórios e visualizações.

Não funcionais: Segurança no armazenamento dos LOGs para evitar adulteração, conformidade com regulamentações legais, retenção de LOGs por períodos especificados.

### Operação de rede

Funcionais: Operação 24/7 de rede de dados e voz, tratamento de tickets e monitoramento de indicadores, backup e recuperação de configurações, ativação e implantação de novos serviços, fornecimento de ferramentas de gerenciamento e suporte técnico.

Não funcionais: Operação contínua, padrões de qualidade para reparos e serviços, resposta rápida a incidentes para minimizar tempo entre falhas.

### Coordenação

Funcionais: Apresentação de relatórios periódicos, apoio à integração de equipes especializadas, planejamento e gestão das equipes e fluxos de trabalho, validação de indicadores de desempenho, supervisão de instalação e manutenção das plataformas, monitoramento de backups.

Não funcionais: Execução em horário comercial com possibilidade de horas extras, qualidade no planejamento e gestão das equipes, padrões de qualidade e acompanhamento constante dos serviços.

### Gerenciamento do projeto

Funcionais: Gestão do portfólio e subprojetos, alocação de recursos e controle de custos, comunicação entre partes interessadas, identificação e mitigação de riscos, preparação de relatórios de status e cronogramas.

Não funcionais: Conformidade com cronogramas e controle financeiro, qualidade das entregas conforme os padrões estabelecidos, eficiência na comunicação e mitigação de riscos.

### Análise forense

Funcionais: Identificação e preservação de evidências digitais, coleta e análise forense de dados, reconstituição de incidentes, geração de relatórios técnicos e recomendações de mitigação, documentação legal.

Não funcionais: Aderência a padrões legais e aceitação judicial das evidências, confiabilidade e precisão dos relatórios forenses, utilização de ferramentas reconhecidas no mercado.

### Evolução da maturidade em segurança da informação

Funcionais: Implementação de políticas de segurança, segmentação de redes e controle de acesso, detecção de ameaças e resposta a incidentes, avaliação de conformidade e riscos cibernéticos, melhoria contínua dos processos de segurança.

Não funcionais: Conformidade com normas e frameworks, incremento gradual da maturidade em segurança, otimização contínua das práticas de segurança cibernética.

## 6. LEVANTAMENTO DE MERCADO

### SOLUÇÕES ATUAIS ENCONTRADAS NO MERCADO

A proposta para o Centro de Operações de Segurança (SOC) do governo de Pernambuco foi desenvolvida após análises detalhadas e estudos técnicos abrangentes, que incluíram processos, recursos humanos, tecnologias e conhecimentos relacionados à segurança da informação. Abaixo estão listados, de forma detalhada, todas as integrações pensadas.

#### Gestão de Endpoint

A gestão de endpoint (dispositivo final, por exemplo: notebook) é um processo crucial nas organizações para auxílio na garantia de segurança, conformidade e eficiência de todos os dispositivos finais (computadores, notebooks,

e até mesmo servidores). O processo é contínuo, portanto, o ideal é que seja automatizado o tanto quanto for possível, e seu monitoramento não pode parar, deve haver um acompanhamento constante, visando proteger os ativos das últimas ameaças lançadas pois o endpoint é o elo mais frágil das camadas de proteção da rede, pois lida diretamente com o usuário, que por vezes não possui tanto conhecimento ou orientação das melhores práticas de segurança, ficando vulnerável a ameaças constantemente.

A seguir os principais pontos abordados no processo:

- Inventário: registro e acompanhamento dos dispositivos que compõem a rede, com informações essenciais como o modelo, sistema operacional, IP, entre outras informações que possam ser consideradas essenciais para a organização;
- Proteção: instalar, configurar e monitorar soluções de proteção como EDR, e garantir a conformidade do equipamento com as políticas de segurança da organização;
- Atualizações: garantir que as atualizações de sistema e de segurança sejam atualizadas conforme os últimos lançamentos, se possível, o ideal é que o processo seja automatizado;
- Controle de acesso : aplicar políticas de controle de acesso visando garantir que apenas usuários autorizados tenham acesso aos ativos e dados necessários;
- Criptografia: aplicar criptografia de disco, para em casos de sinistros, os dados armazenados estejam seguros;
- Monitoramento e detecção: enviar dados do endpoint para um sistema de monitoramento e detecção centralizado, para detecção de possíveis eventos e anomalias nos dispositivos;
- Relatórios: emitir relatórios periódicos com informações dos dispositivos e a saúde deles, visando atender a políticas de segurança e conformidade.

#### Ferramentas de monitoramento de ativos

Uma ferramenta de monitoramento de ativos é um sistema projetado para monitorar e gerenciar os ativos de tecnologia da informação. Esses ativos podem ser sistemas, servidores, firewalls, entre outros. O principal objetivo é assegurar que os ativos operem de maneira eficiente, e em caso de eventos ou incidentes, o time consiga identificar e responder rapidamente, voltando os ativos a normalidade.

Abaixo algumas das principais funções desse tipo de ferramenta:

- Monitoramento de disponibilidade: Os ativos são cadastrados na ferramenta e através de um protocolo de gerenciamento, fica 24x7 monitorando a disponibilidade dos ativos, e em caso de inoperância, dispara um alerta para o time. O monitoramento tem que ser constante, onde a ferramenta fica em intervalos pré-definidos enviando disparos para os ativos, a fim de acompanhar o retorno da disponibilidade. Geralmente a comunicação é realizada via SNMP.
- Monitoramento de desempenho: Semelhante o monitoramento de disponibilidade, o de desempenho também realiza o monitoramento constantemente, porém, em vez de acompanhar o status down/up, são definidos thresholds para cada parâmetro (ex.: perda de pacote, latência etc.) e ao ultrapassar o pré-estabelecido, é gerado o alerta para o time de monitoramento.
- Gestão de configuração: É importante que nesse sistema seja guardado uma série de informações do ativo, como localização, nome, IP etc. Porém, também é importante que haja o levantamento e armazenamento do backup de configuração daquele ativo, e este seja conferido periodicamente, de forma que caso o hardware precise ser trocado, haja a possibilidade de reposição sem maiores problemas, pois com o backup da configuração, a troca se torna muito mais ágil e assertiva. Também é importante que haja o registro de alterações da configuração.
- Gestão de inventário: Outro aspecto primordial para a gestão dos ativos da rede, é a possibilidade de agrupamento dos ativos por setor/filial/órgão, de forma que caso necessário, possa ser feito um levantamento dos ativos pertencentes a cada localidade de forma rápida e precisa.

- Alertas e notificações: Uma gestão de ativos não seria eficiente ou eficaz sem que haja a possibilidade de monitoramento constante, através de alertas em caso do threshold estabelecido seja violado. Logo, a ferramenta deve ser capaz de gerar alertas e enviar notificações conforme necessário, ao time responsável pelo monitoramento.
- Acesso remoto: A solução deve permitir que os ativos gerenciados sejam acessados remotamente, para o caso de testes (desempenho, disponibilidade ou checagem de configurações). O acesso deverá comportar a possibilidade de pelo menos duas formas diferentes, por exemplo ssh, telnet, https etc.
- Controle de acessos: A ferramenta deve comportar usuários locais suficientes para todo o time de analistas, cada qual com usuários individuais, e a troca de senha deve ser requisitada periodicamente (atendendo a política de segurança definida), também deve ser possível criar usuários com visualizações e permissões específicas para sua função.
- Acessos simultâneos: Deve ser possível abrir a interface da solução em diversos dispositivos diferentes, de forma simultânea, sem limite de telas para a operação.
- Filtros: Permitir realizar filtragem para localização de ativos e alertas.

Qual a importância do monitoramento de ativos para a segurança da informação?

Para atender aos pilares da segurança da informação, que consistem em confidencialidade, integridade e disponibilidade, faz-se necessário monitorar os ativos, garantindo que eles estejam sempre disponíveis e trabalhando conforme o esperado, evitando assim, que a perda de desempenho ou disponibilidade ou até mesmo que pessoas não autorizadas acessem esses ativos por usuários locais indevidamente configurados, ou afins, de forma que afetem o ciclo da informação para as partes interessadas.

Outro ponto é que com a gestão dos ativos, é possível acompanhar quantos ativos existem, seus donos, as configurações, quando tempo ficou indisponível, ou em casos de incidentes de segurança, é possível ainda correlacionar informações de tráfego com disponibilidade, quanto mais rico de dados o time estiver munido, mais rápida e assertiva será a resposta a incidentes. Com o histórico de configurações e thresholds também é possível identificar o ponto chave que ocasionou determinado evento ou incidente.

### **Ferramenta de gerenciamento de ativos**

A gestão de ativos de TI (também conhecida como ITAM) é o processo usado para garantir que os recursos de uma empresa sejam contabilizados, implementados, mantidos, atualizados e descartados quando necessário. Em resumo, é garantir que os itens valiosos, tangíveis e intangíveis da empresa sejam rastreados e usados. (Atlassian, s.d.)

Geralmente as ferramentas de ITAM mantêm um registro completo de todos os ativos de TI com suas informações detalhadas, como número de série, localização, status, licenciamento, garantindo a conformidade e evitando expiração de licença. Também facilita auditorias de ativos, para conformidade de políticas e regulamentos, ou até mesmo facilitando a identificação para otimização do uso dos ativos, acompanhando seu ciclo de vida, possibilitando a eficiência das operações, manutenções, atualizações de software e de segurança.

Uma ferramenta de ITAM é valiosa pois ajuda a evitar o desperdício de recursos, reduzir riscos de segurança, garantir conformidade e facilitar a tomada de decisões relacionadas aos ativos de TI.

Para análise de requisitos de uma ferramenta de ITAM foi realizado uma pesquisa em alguns sites das principais ferramentas recomendadas, e dessa relação foram selecionadas as ferramentas mais citadas.

(SITE 1, s.d.)	(SITE 2, s.d.)	(SITE 3, s.d.)
PRTG	ManageEngine Service Desk Plus	Freshservice
ManageEngine AssetExplorer	SysAid	Lansweeper
Spiceworks Inventory	AssetExplorer	Snipe-IT
Atera	InvGateName	InvGate Assets
Snipe-IT	SolarWinds	
SysAid	Jira Service Management	
AssetPanda	SpiceWorks	
Lansweeper	Asset Panda	
Ivanti IT Asset Management Suite		
SolarWinds Server & Application Monitor		

As ferramentas escolhidas foram a Lansweeper, Snipe-IT e InvGate Assets, ambas foram citadas cada uma duas vezes. De acordo com o comparativo entre as ferramentas selecionadas, segue abaixo a relação de funcionalidades em comum entre elas, que podem ser considerados como os critérios mínimos recomendados a serem exigidos:

- Inventário de ativos de hardware
- Inventário de ativos de software
- Painel Central

Tendo em vista que as ferramentas citadas acima possuem uma carência de funcionalidades, foi realizado um segundo levantamento que originou um comparativo entre quatro fabricantes de ITAM (Incidente IQ, NinjaOne, ScalePad e Scrut Automation) que possuem uma abrangência maior de funcionalidades, e foi levantado os seguintes requisitos mínimos recomendados a serem exigidos:

- Inventário de ativos de hardware
- Inventário de ativos de software
- Inventário de ativos em nuvem
- Inventário de ativos móveis
- Descoberta de ativos
- Painel Central
- Gestão de política de ativos
- Gerenciamento de riscos
- Integrações

Hoje é utilizado no projeto o CA Spectrum como inventário da infraestrutura do projeto. Segue abaixo as características dessa ferramenta:

- Correlação inteligente de eventos
- Análise rápida da causa raiz
- Gerenciamento proativo de mudanças

- Cobertura abrangente de dispositivos e plataformas
- Visualizações e interfaces personalizadas e baseadas em funções
- Isolamento de falhas e análise de causa raiz
- Gerenciamento proativo de mudanças
- Relatórios sofisticados fornecem insights poderosos
- Suporte abrangente de infraestrutura
- Extensibilidade de monitoramento flexível
- Modelagem de rede robusta, monitoramento e cobertura de rede de gerenciamento

### Ferramenta de gerenciamento de serviços de TI

O gerenciamento de serviços de TI, conhecido pela sigla ITSM, é a maneira como as equipes de TI gerenciam a entrega completa dos serviços de TI aos clientes. Ele inclui todos os processos e atividades de projeto, criação, entrega e suporte de serviços de TI. (Atlassian, s.d.)

Uma ferramenta de ITSM visa gerenciar e otimizar os serviços de tecnologia na organização, melhorando a eficiência, a qualidade e a entrega de serviços, com o objetivo de atender as necessidades dos usuários finais. Esse tipo de ferramenta se torna essencial para organizações complexas, com um grande volume de solicitações e a necessidade de atendimento a padrões regulatórios e de conformidade.

Uma ferramenta de ITSM ajuda na gestão de incidentes, problemas e mudanças, com o registro de tickets com informações pertinentes ao cenário, e a possibilidade de troca de filas de atendimento entre os envolvidos, bem como o acompanhamento dos níveis de serviço para registro e monitoramento de estouro de tempo ou atendimento dentro do prazo pré-estabelecido. Também auxilia na gestão de ativos e configuração, mantendo uma base de dados que documenta suas informações, relacionamentos e dependências. Além disso emite relatórios com métricas que podem auxiliar na avaliação geral da organização, nas auditorias, e na melhoria contínua do negócio.

Para análise de requisitos de uma ferramenta de ITSM foi realizado uma pesquisa em alguns sites das principais ferramentas recomendadas, e dessa relação foram selecionadas as ferramentas mais citadas.

(SITE 1, 2024)	(SITE 2, s.d.)	(SITE 3, s.d.)	(SITE 4, s.d.)
Service Desk Plus	Naverisk	Cherwell Service Management	Atlassian Jira Service Desk
Asset Panda	HaloITSM	SolarWinds Web Help Desk	SolarWinds Web Help Desk
BMC helix ITSM	InvGate Service Desk	TOPdesk	ServiceNow
Cherwell	Tiflux	Zendesk	ManageEngine ServiceDesk Plus
Gerenciamento de serviços do Jira	HaloPSA	ServiceNow	Ivanti Service Manager
HaloITSM	SolaWinds Service Desk		Spiceworks
SolarWinds ITSM	ManageEngine Endpoint Central		Freshworks Freshservice
Spiceworks	Atera		Cherwell Service Management
SysAid	Vision Helpdesk		Samange Service Desk
Zendesk	GitLab		BMC Remedyforce
InvGateName	SysAid		TOPdesk
			Zendesk

As ferramentas escolhidas para o comparativo foram SolarWinds Web Help Desk (citada nos 4 sites), Cherwell Service Management e Zendesk (ambas foram citadas em 3 sites). Além delas foi usado como base a ferramenta usada

atualmente da Broadcom. De acordo com o comparativo entre as ferramentas selecionadas, segue abaixo a relação de funcionalidades em comum entre elas, que podem ser considerados como os critérios mínimos recomendados a serem exigidos:

- Gerenciamento de mudanças
- Gestão de ativos
- Relatórios
- Fluxo de trabalho do processo
- Console de administração
- Gerenciamento de acesso
- Sistema de tickets
- Alertas
- Automação
- Registro de desempenho

#### **Gerenciamento de usuários**

O processo de gerenciamento de usuários tem como objetivo garantir que apenas usuários autorizados tenham acesso aos recursos e informações, auxiliando na proteção contra ameaças internas e externas. O processo envolve vários aspectos que visam garantir a integridade, confidencialidade e disponibilidade dos dados.

Inicia-se pela criação das contas, cada usuário deve possuir seu acesso individual, e este deve estar de acordo com o perfil definido, com as atribuições específicas da função de cada um, podemos chamar esse método de RBAC, que consiste basicamente em controle de acesso baseado em funções. Geralmente se usa um Active Directory para base de contas de usuários, mas a organização pode utilizar a tecnologia que preferir, desde que atenda aos requisitos de conformidade com as políticas e boas práticas adotadas pela organização.

Com as contas criadas deve-se definir também o método de autenticação, como o tamanho e parâmetros mínimos para as senhas, se vai usar autenticação de duplo ou múltiplos fatores, os critérios devem estar de acordo com a política de segurança da organização.

Deve-se possuir um monitoramento ativo sobre as contas de usuários, realizando auditorias periódicas na base para checagem dos usuários inativos e das permissões concedidas, e qualquer alteração ou revogação de função deve ser refletida nas contas de usuários. Além desse monitoramento das contas, deve haver também o monitoramento de LOGs de usuários, para que seja acompanhado o comportamento dos usuários na rede, de forma que caso aconteça alguma atividade suspeita, seja rapidamente e facilmente identificada pelo time de segurança para atuação imediata, antes do completo comprometimento da conta ou da rede.

Outro aspecto de extrema importância é a conscientização dos usuários, eles devem ser devidamente informados sobre o método utilizado, as políticas de segurança e privacidade devem ser claras e acessíveis a todos, e eles devem ser orientados sobre as melhores práticas de uso da conta e armazenamento de credenciais.

Os usuários são o elo mais fraco das camadas de proteção da informação, portanto, a devida conscientização e os métodos de proteção contra ameaças internas e externas devem ser considerados, para que se tenha um gerenciamento eficiente, contribuindo para um ambiente mais seguro, fortalecendo a postura de segurança da organização.

#### **Ferramentas de gerenciamento de identidade de acesso**

IAM se trata de Gerenciamento de identidade e acesso, que consiste em determinação de nível de acesso baseado em função e permissão. Logo, uma ferramenta de IAM é um sistema que irá realizar a gestão de funções e privilégios de acesso de usuário aos ativos e sistemas para atender as políticas e regulamentos implantados.

A implementação eficaz de ferramentas de IAM é fundamental para garantir a segurança da informação, o cumprimento de regulamentações e a gestão eficiente dos recursos de TI. Essas ferramentas são utilizadas para proteger dados sensíveis e garantir que o acesso seja concedido de maneira apropriada.

As funcionalidades previstas de uma solução de IAM em conjunto com a atuação do time de analistas tem em vista atender a padrões e boas práticas de segurança, como:

- MFA: Múltiplos fatores de autenticação consiste basicamente em você realizar a autenticação com dois ou mais métodos, que são categorizados em: o Algo que se sabe – Ex.: Uma senha o Algo que se tem – Ex.: Um token o Algo que se é – Ex.: Biometria
- RBAC: Controle de acesso baseado em função é um método que faz a gestão de usuários em cima de suas respectivas funções, limitando as permissões de acesso aos sistemas de TI que não correspondem com suas atividades.
- Ciclo de vida: A gestão do ciclo de vida dos usuários consiste em realizar o acompanhamento da criação, manutenibilidade e exclusão, bem como concessão ou revogação de acesso dos usuários conforme a necessidade.
- Conformidade: Auditoria em cima de atividades de usuários para atendimento em conformidade das políticas, normas e leis cabíveis.
- SSO: Essa função consiste em permitir que o usuário acesse diversos aplicativos, sistemas e rede com uma única autenticação.
- Gestão de identidade: Gerenciamento das informações da identidade do usuário, como o nome, e-mail, função, e demais atributos relacionados ao usuário e que sejam pertinentes a organização.

## PAM

O PAM (Privileged Access Management) é uma abordagem de segurança que visa controlar, monitorar e auditar o acesso a contas e recursos privilegiados em sistemas de TI. Ele é usado para proteger credenciais de administradores e outros usuários com acesso privilegiado, reduzindo o risco de abuso ou uso indevido dessas contas.

Benefícios:

- Protege contra acessos não autorizados a contas privilegiadas
- Permite o controle granular de quem pode acessar recursos privilegiados e quando
- Ajuda a reduzir o risco de roubo de credenciais e uso indevido de privilégios
- Facilita a auditoria e conformidade com requisitos regulatórios
- Melhora a visibilidade e o controle sobre o acesso privilegiado

Características:

- Capacidade de gerenciar e proteger credenciais privilegiadas
- Capacidade de monitorar e auditar o acesso a recursos privilegiados
- Capacidade de impor políticas de acesso privilegiado
- Capacidade de integrar-se com sistemas existentes, como diretórios LDAP e bancos de dados

## Múltiplo Fator de Autenticação

O que é autenticação de múltiplos fatores?

Trata-se de uma tecnologia que solicita ao usuário de uma plataforma, um aplicativo ou um sistema confirmar sua identidade em dois ou mais momentos, antes de liberar o acesso dele ao sistema. Esse processo é bastante comum quando tentamos acessar os dados de instituições financeiras pela internet. Neste caso, após inserir login e senha na plataforma, o cliente só pode dar sequência à operação se inserir em um campo determinado o código que lhe foi informado por meio de um hardware token, por exemplo. Entre os meios para a múltipla verificação estão o software token e o push, entre outros. (NovaRed, s.d.)

Múltiplos fatores de autenticação consistem basicamente em você realizar a autenticação com dois ou mais métodos, que são categorizados em:

- Algo que se sabe: Uma senha
- Algo que se tem: Um token
- Algo que se é: Biometria

Por que aderir à autenticação de múltiplos fatores? Existem muitos bons motivos para aderir à autenticação de múltiplos fatores. Porém, o mais básico e recorrente está relacionado ao fato de que grande parte dos usuários de internet possui uma senha padrão para acessar diferentes plataformas pessoais e profissionais. Os criminosos sabem disso. Por essa razão, quando estão focados em atacar determinada companhia, fazem o rastreamento de profissionais-chave, hackeiam as senhas pessoais dessas pessoas e fazem tentativas de acesso com combinações de caracteres iguais ou semelhantes no ambiente corporativo. Em muitos casos, a ação é concluída com sucesso, evidenciando a fragilidade da autenticação tradicional apenas por meio de usuário e senha. (NovaRed, 2024)

É recomendável que a autenticação multifatorial seja utilizada principalmente pelo time da operação dos equipamentos/dispositivos, exigindo sempre que for necessário o acesso aos firewalls ou demais dispositivos da rede para suporte ou ajustes. Por exemplo, sempre que o analista precisar acessar o firewall da localidade, deve ser exigido além do usuário e senha um token de autenticação, aumentando a garantia de segurança na autenticação privilegiada.

## ZTNA

O ZTNA (Zero Trust Network Access) é um modelo de segurança que se baseia no princípio de "confiança zero", ou seja, não confia automaticamente em usuários ou dispositivos dentro ou fora da rede corporativa. Em vez disso, ele verifica a identidade e a segurança de cada usuário e dispositivo antes de conceder acesso a recursos de rede, independentemente de sua localização.

Benefícios:

- Aumenta a segurança ao reduzir a superfície de ataque
- Protege contra ameaças internas e externas
- Melhora a visibilidade e o controle sobre quem e o que acessa a rede
- Facilita a implementação de políticas de acesso granulares
- Permite o acesso seguro a recursos de rede a partir de qualquer localização

Características:

- Capacidade de autenticar e autorizar usuários e dispositivos de forma segura
- Capacidade de aplicar políticas de segurança granulares com base na identidade e contexto do usuário e dispositivo

- Capacidade de fornecer acesso seguro a recursos de rede, independentemente da localização do usuário

### **Campanhas de conscientização**

Uma campanha de segurança da informação é um esforço contínuo e abrangente para promover a conscientização e a adoção de práticas seguras em uma organização. Ao contrário de uma ação específica de conscientização, uma campanha envolve um processo de aprendizado gradual ao longo do tempo. Isso se deve ao fato de que ninguém absorve todo o conhecimento em um único evento.

Além disso, a campanha de segurança da informação é mais eficaz porque reconhece a curva de aprendizado e cria uma cultura de segurança através da convivência e da rotina. Portanto, é um processo constante de aprendizagem, tornando-se uma parte integrada da empresa e maximizando a conscientização e a proteção dos dados. (Kavlac, Psycurity: Awareness as a Protection, 2023)

Para obter bons resultados com a campanha, deve-se seguir etapas que se complementam, garantindo a efetividade da ação. Abaixo o descritivo:

- **Avaliação inicial:** Recomenda-se que antes de iniciar as campanhas seja feito uma avaliação geral da organização, do cenário, dos colaboradores, dos principais riscos aos quais a informação está exposta, para a partir daí ser montado o plano de ação.
- **Testes de abertura:** Com a avaliação inicial pronta e as principais vulnerabilidades identificadas, recomenda-se que seja feito um teste inicial, que pode ser de phishing por e-mail, por exemplo, para identificar qual o nível de maturidade em segurança os colaboradores estão, e para que possa ser feito um comparativo com o teste após a campanha, de forma a medir a efetividade da ação.
- **Preparação do conteúdo:** Hora de montar o plano de ação, nessa etapa deve ser construído um conteúdo de evolução gradual de conhecimentos em segurança da informação, que devem ser repassados por e-mail, vídeos, apresentações, cartazes, ou da melhor forma definida entre a gestão e o time de segurança. Os assuntos devem abordar os principais conceitos da segurança da informação, ameaças mais comuns e as melhores práticas recomendadas.
- **Divulgação do material e treinamentos:** Com o plano de ação e cronograma montados, os treinamentos devem ser ministrados e o material de conscientização divulgado pelos canais especificados.
- **Teste de efetividade:** Após os treinamentos, devem ser realizados testes para medir a efetividade, feedbacks do público e avaliações de segurança podem ser coletados para garantir que as mensagens estão sendo compreendidas e que as práticas de segurança estão melhorando;
- **Melhoria contínua:** Recomenda-se manter a comunicação e os testes de forma contínua;

Alguns pontos chave se mostram importantes na efetividade da ação, como:

- As políticas, comunicações e treinamentos devem ser claros, compreensíveis e acessíveis a todo o público.
- Reconhecimentos podem ser dados ao público que mais se destacarem nos testes e boas práticas de segurança, isso pode motivar os demais a participarem ativamente da conscientização.
- As mensagens podem ser personalizadas de acordo com o público ou segmento de atuação, de forma que sejam mais bem compreendidas e fixadas.

### **AntiSpam**

Antispam é uma tecnologia ou conjunto de técnicas usadas para reduzir ou eliminar o recebimento de mensagens não solicitadas, geralmente de natureza comercial ou promocional, enviadas em massa por e-mail. O objetivo do

antispam é filtrar ou bloquear essas mensagens indesejadas, mantendo a caixa de entrada livre de spam e protegendo os usuários contra fraudes, phishing e outros tipos de abusos.

O antispam possui várias características que ajudam a identificar e filtrar mensagens indesejadas. Para consolidar as principais features mais comuns, foi realizado um levantamento em três sites diferentes, e analisado as marcas mais citadas.

As ferramentas escolhidas para o comparativo foram Comodo Group, Check Point e SPAMfighter (ambas foram citadas em 2 dos 3 sites).

(SITE 1, 2024)	(SITE 2, 2024)	(SITE 3, 2024)
Symantec	Guardz	Proofpoint Email Security and Protection
Comodo Group	Mailwasher	Avanan Cloud Email Security
Trend Micro	ESET Protect Mail Plus	SaneBox
TitanHQ	Hornetsecurity Email Spam Filter and Malware Protection Service	Symantec Mail Security for Microsoft Exchange
Mimecast	SpamTitan	Everest
Check Point	SpamSieve	Check Point Anti-Spam & Email Security
Cisco System	Trustifi Inbound Shield	Proofpoint Email Fraud Defense
Barracuda Networks	Comodo Group (Comodo Dome Antispam)	AVG Internet Security Business Edition
SolarWinds MSP	MX Guarddog	Security Gateway
Greenview Data	SPAMfighter	Avast Business Antivirus Pro Plus
Exclaimer	ORF Fusion	
SPAMfighter	Zerospam	
ALTOSPAM		
GFI Mail Essentials		
AppRiver		

Algumas das principais características incluem:

- Listas negras: São listas de remetentes conhecidos por enviar spam. O antispam pode bloquear mensagens provenientes desses remetentes.
- Análise de conteúdo: O antispam examina o conteúdo das mensagens em busca de palavras-chave, padrões ou características típicas de spam.
- Verificação de reputação: Avalia a reputação do remetente, do servidor de envio e do conteúdo da mensagem para determinar se é provável que seja spam.
- Bloqueio de IP: Bloqueia mensagens provenientes de endereços IP conhecidos por enviar spam.
- Whitelists: Lista de remetentes conhecidos e confiáveis, cujas mensagens devem ser sempre aceitas.
- Desafios de verificação: Alguns sistemas de antispam solicitam aos remetentes desconhecidos que confirmem sua identidade antes de permitir a entrega da mensagem.

### Monitoramento de alertas

Podemos dividir os alertas em duas categorias, alertas de segurança que geralmente são gerados pelo SIEM, e alertas de disponibilidade e desempenho gerados pelas ferramentas de monitoramento dos ativos. Para o monitoramento de alertas de segurança faz-se necessário a utilização do SIEM. Ele irá fazer o gerenciamento, e correlação dos LOGs recebidos e ao corresponder com os parâmetros pré-definidos nas regras de detecção emite alertas para o monitoramento, que devem então ser tratados pelos operadores.

Com o auxílio do SIEM na operação do SOC, o trabalho fica mais rápido e assertivo, visto que ele já faz o trabalho de correlação e emissão dos alertas para que haja então a tratativa necessária por parte dos analistas. Geralmente as regras são baseadas no mitre att&ck e nas boas práticas de segurança, e por padrão, já existem centenas de regras nativas previamente definidas no SIEM, e estas são constantemente atualizadas para comportar as últimas ameaças lançadas.

Há também a possibilidade de cruzamento com bases de threat intelligence, onde a ferramenta irá se alimentar dos informes dos principais vendedores e pesquisadores que divulgam os IPs mais ofensivos e que foram envolvidos recentemente em atividades maliciosas, e faz a correlação com o tráfego interno a fim de localizar possíveis atividades suspeitas na rede, caso seja localizado algum IP reportado na rede, automaticamente um alerta é emitido para que a equipe de analistas realize a investigação.

Durante o período de adaptação é natural que sejam emitidos muitos falsos positivos, até que toda a rede seja compreendida e que sejam criadas as exceções de acordo com o cenário em questão, todavia, é importante que o monitoramento e análise desses alertas seja contínuo, não deixando brecha para possíveis incidentes de segurança por falta de análise de algum alerta.

A operação de segurança não precisa necessariamente se limitar ao monitoramento reativo dos alertas, deve-se utilizar a estratégia de threat hunting, visando proativamente buscar as ameaças da rede e comportamentos anômalos.

Para o monitoramento de alertas emitidos pelo SIEM, faz-se necessário atuar nas seguintes etapas:

- Configuração das regras: após a implantação do SIEM, é necessário averiguar o cenário em questão e habilitar apenas as regras que correspondam as características da rede. Por padrão, os fabricantes produzem centenas de regras de detecção baseadas em boas práticas de segurança e a matriz do mitre att&ck, também há a especificidade de fabricantes e tipos de ativos (por exemplo: Microsoft, apache etc.). Feito a ativação das regras, elas irão ser processadas e correlacionadas aos LOGs recebidos dos ativos da rede, em caso de correspondência com os parâmetros estimados, um alerta é gerado e enviado para o dashboard de monitoramento.
- Envio dos LOGs : para melhor aproveitamento da ferramenta o ideal é que sejam enviados os LOGs apenas dos principais ativos da rede (por exemplo: firewall de borda, servidores críticos etc.). O envio pode ser feito geralmente através de um agente ou um coletor. Os LOGs são então enviados, armazenados, normalizados, correlacionados e os alertas são emitidos.
- Monitoramento: o time de analistas deve monitorar o ambiente 24x7, acompanhando os alertas emitidos, e priorizando a tratativa destes, de acordo com a escala de criticidade dos ativos. Os falsos positivos são fechados e o foco deve ser os que podem apresentar ofensividade ao ambiente.
- Registro: após triagem dos alertas, um registro deve então ser feito, contendo as primeiras informações coletadas para análise.
- Investigação: durante a investigação deve-se coletar o máximo de informações possíveis sobre os ativos envolvidos, o tráfego em questão, o IP ou URL externa relacionado, seu nível de criticidade e ofensividade, e se houve de fato uma atividade maliciosa ou se foi devidamente mitigado.
- Resposta: com a investigação realizada e tendo posse das evidências comprobatórias de atividade maliciosa, deve-se imediatamente realizar a resposta aquela atividade. Efetuar os bloqueios necessários, os ajustes precisos, ou qualquer outra ação solucionadora mapeada para o cenário em questão. Caso se faça necessário, o pool de especialistas pode ser acionado para tratar de algum incidente crítico de segurança.
- Lições aprendidas: após o evento ou incidente ter sido solucionado é crucial que todas as informações em detalhes sejam registradas e documentadas, e que seja feito uma análise de melhoria para mitigar possíveis atividades maliciosas futuras nos ativos. O mitre att&ck da as diretrizes essenciais para cada tipo de ofensi-

vidade, é sempre recomendado que seja seguida essa matriz para um melhor aproveitamento dos recursos e maior proteção da organização.

A eficácia do monitoramento de alertas no SOC depende da combinação de tecnologia avançada, processos bem definidos e uma equipe qualificada de analistas de segurança. O aprimoramento contínuo é fundamental para manter a capacidade de resposta do SOC frente às ameaças em constante evolução.

## SIEM

O SIEM é uma solução de software para centralizar a coleta, armazenamento, e correlação de LOGs para tratar um evento ou incidente de segurança, provendo uma resposta mais rápida e assertiva. Podem ser coletados eventos gerados por diversas aplicações de segurança, como firewalls, IPS, IDS, Antivírus, ou qualquer outro equipamento que se tenha na rede.

Após coletados, esses dados são normalizados, armazenados e exibidos em tempo real, para que possa ser feita a tratativa deles, seja por um SOAR ou pela equipe de segurança responsável.

O SIEM possibilita uma rápida investigação e resposta aos incidentes, visto que esses dados serão correlacionados a partir de diversas bases de ingestão de eventos, mitigando os falsos positivos, e enxugando a visualização, deixando uma visão mais clara e objetiva da informação.

O SIEM transforma dados em uma informação útil, ajuda a identificar comportamentos anômalos, incidentes de segurança, quebra de padrões (melhorado se utilizado Jobs de machine learning), faz alertas de segurança que podem ser notificados na tela do sistema, ou através de disparos automáticos (por e-mail ou telegram, por exemplo), possibilita também a emissão de relatórios mais sofisticados sobre as condições de segurança da rede, com uma maior assertividade de informações, tendo os dados centralizados, e permitindo uma retenção e indexação a longo prazo destes, para uma possível análise posterior, caso faça-se necessário.

Funcionalidades:

- **Coleta:** Por se tratar de uma solução de análise de logs, um dos principais objetivos é coletar o máximo de registros que puder para garantir uma visão completa e precisa sobre os eventos e sobre possíveis riscos. Essa coleta é realizada em firewalls, servidores etc.
- **Normalização:** Processo onde são aplicados um conjunto de regras que visa, principalmente, a organização para redução da redundância de dados, aumento da integridade e desempenho.
- **Categorização e indexação:** Além de coletar, o SIEM também categoriza e indexa os dados em sua base, organizando os registros de eventos em categorias específicas, de acordo com características comuns. Dentro desse conceito de categorização, há a prática de enriquecer os logs, acrescentando metadados essenciais para uma compreensão mais aprofundada dos eventos.
- **Correlação:** Se trata de uma análise fundamentada em regras simples e predefinidas. Estas regras são configuradas com base no conhecimento da empresa sobre situações e eventos específicos, ou já vem de forma nativa pelo fabricante da solução baseado em boas práticas. Em resumo, o processo envolve a análise dos eventos em busca de padrões que satisfaçam as regras previamente definidas.
- **Deteção e alertas:** A identificação ocorre através do monitoramento das atividades de possíveis invasores, juntamente com a análise de sua correlação com outros eventos. O processo de identificação é automatizado e reforçado por módulos de inteligência artificial, com a capacidade de reconhecer padrões nos registros de atividades, possibilitando a antecipação de potenciais ameaças. O sistema emite alertas e notificações, fornecendo informações aos profissionais responsáveis sobre a situação e as medidas a serem tomadas. Todo esse processo é visualizado em painéis de controle.

- **Análise:** A análise procura compreender os registros, buscando identificar possíveis padrões, em forma de monitoramento contínuo dos eventos em tempo real, buscando correspondências com o que o sistema já reconheceu como padrão atípico e suspeito.
- **Análise de comportamento:** Se trata da avaliação do comportamento do usuário. O sistema, alimentado por machine learning, examina os efeitos dos riscos, atribuindo uma pontuação em cada situação para realizar essa análise de impacto.

**Características necessárias:**

- Coleta de LOGs a partir de qualquer fonte
- Normalização dos LOGs
- Conformidade com a LGPD
- Correlação de LOGs
- Mapeamento de alertas no Mitre Att&ck
- Dashboards personalizáveis
- Relatórios personalizáveis
- Integração com SOAR, EDR/XDR
- Fontes de threat intelligence
- UEBA
- Escalável
- Monitoramento em tempo real
- Capacidade de processamento de grande volume de dados
- Acessos individuais a ferramenta para os analistas
- Sem limite de acessos simultâneos

**Analistas de nível 1**

Equipe responsável por monitoramento proativo do SOC, bem como atividades relacionadas a configurações de segurança, relatoria e atendimento de incidentes e requisições reativos. O time deverá atuar 24x7.

O analista de primeiro nível é responsável por:

- Monitoramento contínuo dos alertas de segurança
- Caça e identificação de anomalias que possam indicar atividades maliciosas
- Identificação, registro e investigação de alertas de segurança, bem como sua classificação e priorização com base no impacto potencial
- Realiza a análise dos incidentes de segurança para determinar a natureza e extensão das ameaças
- Coleta as informações mais relevantes e escalona os incidentes críticos para o pool de especialistas
- Executa os procedimentos de resposta a incidentes pré-definidos, e aplica correções para mitigar o impacto
- Geração de relatórios pós-incidentes para análises e melhoria contínua
- Participa de treinamentos continuamente para desenvolver habilidades necessárias para enfrentar novos desafios

- Contribui na atualização das regras de detecção de eventos de segurança
- Realiza o atendimento de solicitações feitas pelo cliente
- Realiza o atendimento de incidentes reativos (reportados pelo cliente)
- Emite relatórios periódicos
- Emite relatórios personalizados ou solicitados pelo cliente

Deverá ser exigido o seguinte nível de conhecimento mínimo dos analistas:

- Formação em redes de computadores ou segurança da informação
- Certificações ISFS, CompTIA Security+ ou superiores
- Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes

### Gestão de Incidentes

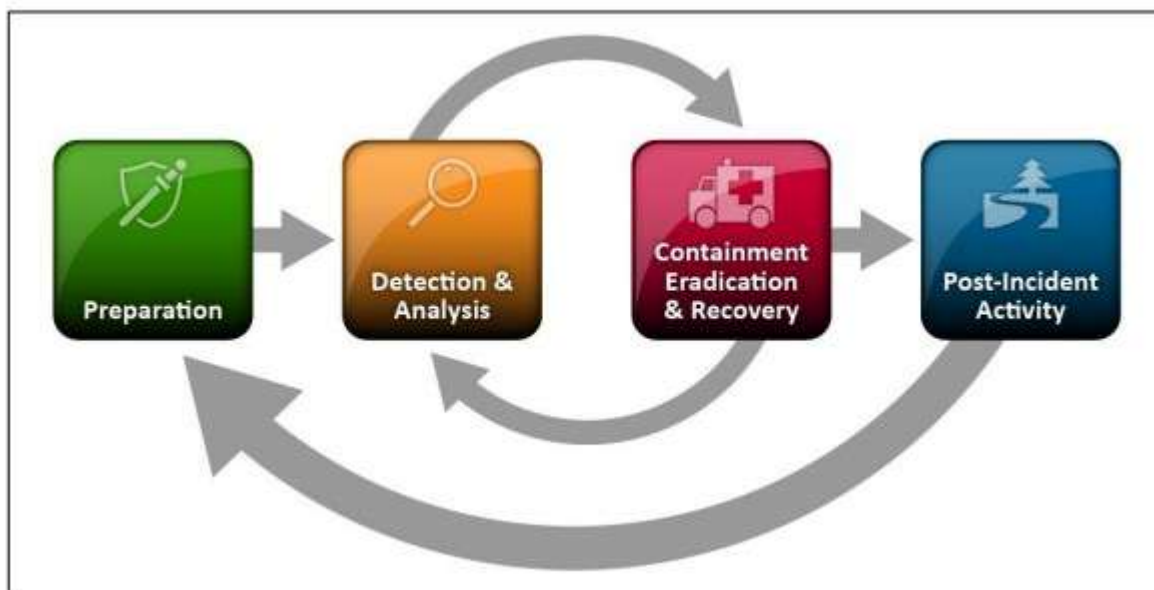
O processo de gestão de incidentes de segurança da informação é um conjunto de etapas estruturadas com o propósito de lidar com eventos que comprometam a confidencialidade, integridade ou disponibilidade dos dados da organização (Incidente de segurança). O objetivo da gestão de incidentes é detectar, responder, mitigar e aprender com os incidentes para minimizar o impacto e prevenir recorrências.

A gestão de incidentes da segurança da informação geralmente é composta pelas seguintes etapas:

- Preparação: desenvolvimento de políticas e procedimentos de segurança, determinar uma equipe de resposta a incidentes designando responsabilidades específicas, implementar ferramentas e tecnologias de prevenção, monitoramento e detecção;
- Detecção: monitoramento dos eventos de segurança, alertas e sistemas de detecção para identificar potenciais incidentes, comunicação eficiente de incidentes;
- Análise: investigação, priorização e análise do incidente para entender a gravidade, avaliação do impacto nos sistemas e dados da organização, determinação da origem e causa raiz do incidente;
- Resposta: aplicação do plano de resposta a incidentes, isolamento de sistemas comprometidos, implementação de contramedidas para contenção da ameaça, notificação as partes interessadas;
- Recuperação: restauração dos sistemas e dados afetados, verificação da eficácia das contramedidas implementadas;
- Lições aprendidas: análise e documentação das lições aprendidas.

Há alguns frameworks que tratam o tópico, fornecendo diretrizes para auxiliar a organização na gestão dos incidentes de segurança, abaixo alguns mais vistos no mercado:

- ISO/IEC 27002:2022: O controle 24 diz que: A organização deve planejar-se e preparar-se para o gerenciamento de incidentes de Segurança da Informação, por meio da definição, do estabelecimento e da comunicação dos processos, funções e responsabilidades relativos a eles. Com o propósito de garantir rapidez, eficácia, consistência e respostas ordenadas aos incidentes de Segurança da Informação, incluindo comunicação nos eventos.
- NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) - Esta publicação procura ajudar as organizações a mitigarem os riscos de incidentes de segurança informática, fornecendo orientações práticas sobre como responder a incidentes de forma eficaz e eficiente. Inclui diretrizes no estabelecimento de um programa eficaz de resposta a incidentes, mas o foco principal do documento é detectar, analisar, priorizar e tratar incidentes. As organizações são incentivadas a adaptar as diretrizes e soluções recomendadas para atender aos seus requisitos específicos de segurança e missão. (NIST, s.d.)



Ciclo de vida da resposta a incidentes (NIST, s.d.)

- ITIL (Information Technology Infrastructure Library) – O gerenciamento de incidente ITIL nada mais é do que um conjunto de boas práticas que visam antever e controlar problemas de serviços de TI, com base em contratos de nível serviço (SLAs) combinados. Uma gestão de incidentes efetiva é importante porque ela busca assegurar que essas falhas sejam solucionadas rapidamente, assim como também tende a diminuir a sua frequência. Por meio dela, é possível realizar um diagnóstico completo sobre o incidente e descobrir como ele começou. Essa prática é fundamental porque uma empresa deve tentar reduzir ao máximo o número de incidentes, visto que a constância desses problemas gera insatisfação em um público muito importante: seus clientes. Além disso, é onde são mantidos os Acordos de Níveis de Serviços firmados com as áreas de negócios. E isso pode ser feito por meio de um reparo rápido ou do fornecimento de uma solução alternativa ao cliente. (Zendesk, 2023)

### Resposta a incidentes

O plano de resposta a incidentes faz parte de um processo estruturado (gerenciamento de incidentes de segurança da informação) e visa lidar com incidentes de segurança da informação, ataques cibernéticos, entre outras situações que possam comprometer um ou mais pilares da segurança da informação.

De acordo com o Computer Security Incident Handling Guide do NIST no tópico 2.3.2, o plano de resposta a incidentes deve incluir os seguintes elementos:

- Missão
- Estratégias e objetivos
- Aprovação da alta administração
- Abordagem organizacional para resposta a incidentes
- Como a equipe de resposta a incidentes se comunicará com o resto da organização e com outras organizações
- Métricas para medir a capacidade de resposta a incidentes e sua eficácia
- Roteiro para amadurecer a capacidade de resposta a incidentes

- Como o programa se enquadra na organização geral

A organização deve implementar o plano e revisá-lo pelo menos anualmente para garantir que a organização esteja seguindo o roteiro para amadurecer a capacidade e cumprir seus objetivos de resposta a incidentes.

Os especialistas jurídicos devem revisar os planos, políticas e procedimentos de resposta a incidentes para garantir deles conformidade com lei e Federal orientação, incluindo o certo para privacidade. Em Adição, a orientação do consultor jurídico geral ou do departamento jurídico deve ser procurada se houver motivo acreditar que um incidente pode ter legal ramificações, incluindo evidência cobrança, acusação de um suspeito, ou uma ação judicial, ou se houver necessidade de um memorando de entendimento (MOU) ou outros acordos vinculativos que envolvam limitações de responsabilidade para o compartilhamento de informações. (Technology)

Ainda segundo o NIST o ciclo de vida de um incidente é dividido da seguinte forma:



Fonte: NIST80061.

Dito isso, abaixo o descritivo das etapas necessárias para o processo:

- **Preparação:** convém que sejam desenvolvidas e implantadas políticas de segurança e políticas complementares a esta. Também convém que seja estabelecido uma equipe de resposta a incidentes e suas devidas responsabilidades. Os ativos críticos também precisam ser identificados bem como os dados sensíveis para a organização. Faz-se necessário ainda a implantação de ferramentas de monitoramento de segurança. Os planos de comunicação tanto internos quanto externos também precisam ser definidos e é recomendável que sejam planejados treinamentos e testes regulares para todo o time.
- **Detecção e análise:** durante a operação diária do SOC o time deve monitorar continuamente e em tempo real o ambiente, com uma atenção mais criteriosa para os ativos críticos da organização. Ao identificar possíveis eventos de segurança, esses devem ser registrados e analisados a fim de identificar possíveis incidentes, e em caso positivo para incidente de segurança, este deve ser classificado e priorizado de acordo com o tipo e gravidade.
- **Contenção:** ao identificar um incidente de segurança o primeiro passo é isolar os sistemas e ativos envolvidos para que não seja propagada a infecção. Caso seja possível, recomenda-se que os serviços comprometidos sejam desconectados ou desativados até que a solução definitiva seja aplicada, e caso a solução definitiva seja de alta complexidade, recomenda-se que sejam implementadas contramedidas temporárias para redução do impacto.

- **Erradicação:** após a identificação e a contenção deve-se trabalhar na erradicação definitiva da causa do incidente. Logo, a causa deve ser identificada e removida completamente, e as vulnerabilidades que levaram ao incidente devem ser corrigidas.
- **Recuperação:** após a completa erradicação da origem do incidente e da vulnerabilidade identificada, deve-se restaurar todos os ativos e sistemas ao modo normal, verificando a integridade dos dados e dos serviços.
- **Lições aprendidas:** após o incidente uma análise completa deve ser feita para entendimento da origem do incidente, seu impacto, e necessidades de atualização de políticas, processos e controles de segurança, e este conhecimento adquirido deve ser disseminado dentro da equipe e com os demais stakeholders. Todas as ações e informações sobre o ocorrido deve ser documentado e arquivado para fins de relatório, auditoria e base de conhecimento.
- **Comunicação:** os stakeholders devem ser notificados sobre o ocorrido, e se for necessário, para atender a itens de conformidade, as autoridades ou o departamento jurídico também. Convém que a comunicação seja transparente para manutenibilidade da confiança.

Convém que o plano de respostas a incidentes seja revisado e atualizado regularmente, pois é um processo contínuo e para garantir que esteja alinhado com as ameaças emergentes e as mudanças da organização, deve estar diretamente envolvido no ciclo PDCA.

#### **Grupo de especialistas**

Equipe composta por um time multidisciplinar, composto por diversos profissionais especialistas em vários segmentos de TI e segurança. Time atuará de segunda a sexta das 8h às 18h e deverá haver regime de plantão para casos de incidentes ou necessidades de acionamento por parte do time de analistas de primeiro nível.

O blue team é responsável por:

- Fazer análise e resposta a incidentes críticos
- Documentação das táticas, técnicas e procedimentos (TTPs) dos atacantes
- Identifica e desenvolve novos indicadores de comprometimento (IOCs) com base em análises de incidentes e inteligência de ameaças
- Configura e otimiza ferramentas de segurança e sistemas de detecção
- Desenvolve e aprimora scripts ou ferramentas de automação de tarefas
- Fornece treinamento técnico para analistas de primeiro nível
- Participa ativamente na definição de estratégias de segurança cibernética, desenvolvendo e implementando estratégias que estejam alinhadas aos objetivos e riscos específicos
- Lida com ameaças avançadas, como ataques persistentes avançados (APTs), desenvolve contramedidas para ameaças complexas e persistentes.
- Conduz pesquisas sobre novas ameaças ou vulnerabilidades e sua remediação
- Avalia novas medidas e tecnologias que possam contribuir positivamente para lidar com a segurança da informação
- Contribui para o desenvolvimento de políticas, procedimentos e diretrizes de segurança
- Planeja e executa simulações de testes de intrusão em ambiente controlado
- Participa de auditorias de segurança e garante a conformidade com regulamentos e padrões relevantes
- Realiza a implantação de equipamentos e soluções

- Realiza atendimento de incidentes e solicitações escalonados do primeiro nível

A equipe deverá ter especialistas em:

- Segurança de endpoint
- Segurança de rede sem fio
- Firewall de borda
- Firewall dos clientes
- Segurança de perímetro de rede local
- SIEM
- Conformidade
- Forense
- Falhas e desempenho
- ITSM
- Processos

Deverá ser exigido o seguinte nível de conhecimento mínimo dos analistas:

- Formação em redes de computadores ou segurança da informação
- Certificações ISFS, CompTIA Security+ ou superiores
- Experiência em análise de LOGs, monitoramento de segurança e resposta a incidentes, fornecimento de treinamentos técnicos

Deverá ser exigido o seguinte nível de conhecimento mínimo dos analistas especialistas:

- Segurança de Endpoint
  - Experiência em análise e investigação de incidentes e eventos em endpoints
  - Experiência em implantação e suporte de EDR/XDR
- Segurança de rede sem fio
  - Certificação CWSP (Certified wireless security professional) ou similar
- Firewall dos clientes
  - Experiência em análise e investigação de incidentes e eventos em firewalls
  - Experiência em implantação, configuração e suporte de firewalls
- Firewall de borda
  - Certificação CISSP (Certified Information Systems Security Professional)
- Segurança de perímetro de rede local
  - Experiência em análise, investigação e resposta a eventos de segurança
- SIEM
  - Experiência em análise e investigação de incidentes e eventos em SIEM
  - Experiência em implantação, configuração e suporte de soluções de SIEM

- Conformidade
  - Experiência em participação de auditorias de segurança da informação
  - Certificação voltada para LGPD
- Forense
  - Certificação CHFI (Computer Hacking Forensic Investigator) ou similar
- Falhas e desempenho
  - Experiência no monitoramento de redes
- ITSM
  - Certificação ITIL Foundation v4 ou superior
- Processos
  - Certificação ITIL Foundation v4 ou superior
  - Certificação CBPA (Certified Business Process Associate) ou superior

## WAF

O WAF (Web Application Firewall) é um tipo de firewall específico para proteger aplicações web contra ataques cibernéticos, como injeção de SQL, cross-site scripting (XSS) e outros tipos de ataques comuns a aplicações web. Ele monitora, filtra e bloqueia o tráfego HTTP e HTTPS entre um aplicativo web e a internet para detectar e bloquear ataques maliciosos.

Benefícios:

- Protege aplicações web contra uma variedade de ataques cibernéticos
- Ajuda a manter a conformidade com regulamentações de segurança, como PCI DSS
- Oferece visibilidade detalhada do tráfego e atividades da aplicação web
- Permite a implementação de políticas de segurança específicas para cada aplicação web
- Reduz o risco de comprometimento da aplicação web e perda de dados

Características:

- Capacidade de filtrar e inspecionar o tráfego HTTP e HTTPS
- Capacidade de detectar e bloquear ataques comuns a aplicações web
- Capacidade de personalizar políticas de segurança para cada aplicação web
- Capacidade de integrar-se com outras soluções de segurança da informação

## UTM

UTM (Unified Threat Management) é uma ferramenta com diversas soluções integradas que compõem um único equipamento de borda para proteção de redes locais. Podemos considerar o UTM como um Firewall de nova geração. Como principal benefício desse equipamento podemos citar o custo-benefício, pois ele une em uma única interface a administração e monitoramento de segurança da rede local, sendo assim, mais econômico do que implantar uma série de soluções de segurança separadas.

De acordo com o (Gartner , 2022) os líderes de mercado na solução são Fortinet, Palo Alto, Check Point, como topo do quadrante “Desafiantes” entra a Cisco. Foi feito uma comparação entre Fortinet, Palo Alto e Cisco e abaixo as funções mais comuns numa UTM (G2 Compare, 2024):

- UTM (Unified Threat Management) é uma ferramenta com diversas soluções integradas que compõem um único equipamento de borda para proteção de redes locais. Podemos considerar o UTM como um Firewall de nova geração. Como principal benefício desse equipamento podemos citar o custo-benefício, pois ele une em uma única interface a administração e monitoramento de segurança da rede local, sendo assim, mais econômico do que implantar uma série de soluções de segurança separadas.
- IPS: O IPS analisa o tráfego buscando padrões suspeitos. Ele bloqueia ou alerta sobre atividades maliciosas, ajudando a proteger a rede contra ameaças.
- Antivírus: A UTM pode incluir um mecanismo antivírus integrado para detectar e remover malware de arquivos, e-mails e outros tipos de tráfego de rede.
- Filtro de conteúdo: Essa funcionalidade permite controlar o acesso dos usuários a sites da web com base em categorias, como redes sociais, jogos ou pornografia, ajudando a melhorar a segurança e a produtividade.
- VPN: Uma UTM pode oferecer suporte a VPNs para permitir que os usuários remotos se conectem à rede de forma segura, protegendo os dados transmitidos pela Internet.

Para um pleno funcionamento do equipamento, a UTM deve ser capaz de lidar com o tráfego de rede da organização sem comprometer a velocidade ou a qualidade da conexão, é essencial que o dispositivo também receba atualizações regulares de segurança para proteger contra nova ameaças e vulnerabilidades. Além disso, deve ser compatível com os sistemas e dispositivos existentes na rede, de forma escalável para atender a possíveis necessidades de crescimento, e deve possuir uma interface de gerenciamento harmoniosa para simplificação da administração e configurações da rede. Além disso, é necessário que o equipamento esteja em conformidade com regulamentações específicas e fornecer recursos que ajudem a garantir conformidade com as normas vigentes as quais a organização deve responder.

Foi realizado o dimensionamento para atender a dois portes de localidade, de forma a garantir a adequada prestação do serviço durante todo o período contratual, sem prejuízo de desempenho, conforme apresentado no quadro abaixo:

Item	Especificação	Solução de segurança da rede corporativa	
		Solução unificada de segurança de rede - P	Solução unificada de segurança de rede - M
1	Throughput de Firewall (Gbps)	12	24
2	Conexões simultâneas (milhões)	1,2	2,4
3	Novas conexões por segundo (mil)	90	180
4	Throughput de IPSec (Gbps)	2,4	4,8
5	Proteção combinada contra ameaças (Gbps)	2	4
6	Qtd mínima de interfaces (1 Gbps)	4	8
7	Qtd mínima de interfaces (10 Gbps)	2	4
8	Quantidade de Instâncias Virtuais Licenciadas	2	2

1 - Throughput de Firewall (Gbps): Consideramos que o equipamento teria que ter a capacidade máxima de processamento de 50% da soma das capacidades de todas as portas do equipamento, temos:

- o 4 portas de 1Gbps + 2 portas de 10Gbps = 24Gbps x 50% = 12 Gbps e
- o 8 portas de 1Gbps + 4 portas de 10Gbps = 48Gbps x 50% = 24 Gbps.

o Logo a justificativa baseia-se na capacidade do equipamento de lidar com as capacidades máximas das portas do equipamento, considerando que a rede local estaria usando o máximo da capacidade física das portas.

2 - Conexões simultâneas (milhões): Mantida a mesma base de usuários, estimou-se que:

- o cada usuário de uso comum mantém cerca de 250 sessões simultâneas;
- o cada usuário corporativo, 750 sessões;
- o cada usuário de uso intenso, 1500 sessões.

o A multiplicação ponderada por 2000 segundos de duração média fornece a quantidade de sessões simultâneas exigida para o dimensionamento do UTM.

3 - Novas conexões por segundo (mil): Considerou-se uma média de 100 usuários por unidade, sendo 60 % de uso comum (60 usuários), 30 % de uso corporativo (30 usuários) e 10 % de uso intenso (10 usuários). O cálculo adota um tempo médio de 2 000 segundos por sessão, resultando em uma taxa de abertura de conexões compatível com os picos de utilização previstos.

4 - Throughput de IPSec (Gbps): Obtido a partir da capacidade de proteção combinada, acrescido de 20 % para compensar o overhead de criptografia e compressão, resultando em margem de segurança operacional adequada ao ambiente multi-VDOM.

5 - Proteção combinada contra ameaças (Gbps): Representa a capacidade total efetiva de processamento de pacotes com todos os módulos de segurança habilitados, em operação contínua, sob regime de tráfego LAN + WAN agregado.

6 - Qtd mínima de interfaces (1 Gbps): Quantidade prevista para atendimento das necessidades de rede interna dos órgãos.

7 - Qtd mínima de interfaces (10 Gbps): Visa atender a necessidade de ambientes com APs e switches de 10Gbps.

8 - Quantidade de Instâncias Virtuais Licenciadas: Quantidade necessária para atender a demanda já existente no estado hoje.

## Access Point

A solução de rede sem fio com segurança será responsável por fornecer conectividade sem fio segura, com foco na proteção dos dados e na prevenção de ameaças. Para suportar o serviço, o local deverá comportar toda a infraestrutura necessária para viabilizar o correto funcionamento do serviço. Aqui estão algumas características que poderiam ser esperadas:

- Criptografia
- Segmentação de rede
- Firewall integrado
- Autenticação dos usuários
- Controle de acesso
- Detecção e prevenção de intrusões
- Monitoramento de segurança

- Auditoria de segurança
- Atualizações de segurança
- Gestão centralizada

## EDR

O EDR (Endpoint Detection and Response) fornece a uma organização a capacidade de monitorar terminais quanto a comportamento suspeito e registrar cada atividade e evento. Em seguida, ele correlaciona informações para fornecer contexto crítico para detectar ameaças avançadas e, finalmente, executa a atividade de resposta automatizada, como isolar um endpoint infectado da rede quase em tempo real. (Brasiline, 2021)

Em outras palavras, o EDR é uma categoria de soluções de segurança desenvolvidas para identificar, investigar e responder a ameaças em dispositivos finais.

Quais os benefícios do EDR?

- Detecção avançada de ameaças: O EDR utiliza tecnologias avançadas, como análise comportamental e aprendizado de máquina, para identificar padrões suspeitos ou atividades maliciosas nos dispositivos finais.
- Investigação Forense: Permite que as equipes de segurança investiguem incidentes, examinem o histórico de eventos e compreendam a natureza e o escopo das ameaças. Isso facilita a resposta a incidentes e a implementação de medidas corretivas.
- Resposta rápida a incidentes: Ao identificar ameaças em tempo real, o EDR ajuda as organizações a responderem rapidamente a incidentes de segurança, minimizando o impacto e reduzindo o tempo de exposição a ameaças.
- Monitoramento em tempo real: Fornece visibilidade em tempo real sobre as atividades nos endpoints, permitindo que as organizações identifiquem comportamentos suspeitos ou anômalos que podem indicar uma possível ameaça.
- Prevenção e mitigação proativas: Além de detectar ameaças, muitas soluções EDR também oferecem recursos de prevenção, ajudando a bloquear atividades maliciosas antes que possam causar danos.
- Melhoria da segurança em camadas: O EDR complementa outras medidas de segurança, como antivírus e firewalls, proporcionando uma abordagem em camadas para proteger os ambientes contra ameaças cibernéticas.
- Conformidade e relatórios: Ajuda as organizações a cumprirem requisitos regulatórios, fornecendo registros detalhados de atividades nos endpoints e facilitando a geração de relatórios necessários para conformidade.

Quais as funcionalidades mínimas exigidas para um EDR?

Para análise de requisitos de um EDR foi feito um comparativo (G2 Compare, 2024a) entre quatro dos principais fabricantes do mercado de acordo com o Gartner 2022: Microsoft, CrowdStrike, SentinelOne, Sophos.

Abaixo as funcionalidades em comum de todos eles:

- Gestão de ativos
- Isolamento do sistema
- Inteligência de endpoint
- Detecção de malware
- Remediação automática

- Relatório de incidentes
- Análise comportamental

#### XDR

O XDR (Extended Detection and Response) é uma abordagem de segurança que vai além do tradicional EDR (Endpoint Detection and Response) ao integrar e correlacionar dados de diversas fontes, como endpoints, servidores, e-mails, redes e nuvem, para fornecer uma visão mais abrangente e eficaz da postura de segurança da organização.

##### Benefícios:

- Oferece uma visão unificada das ameaças em todo o ambiente de TI da organização
- Melhora a detecção de ameaças ao correlacionar dados de várias fontes
- Aumenta a eficácia da resposta a incidentes ao fornecer insights mais detalhados sobre ameaças
- Reduz o tempo de detecção e resposta a incidentes de segurança
- Ajuda a simplificar a segurança da informação ao integrar várias soluções em uma única plataforma

##### Características:

- Capacidade de integrar e correlacionar dados de várias fontes de segurança, como endpoints, servidores, e-mails, redes e nuvem
- Capacidade de fornecer uma visão unificada das ameaças em todo o ambiente de TI
- Capacidade de detectar e responder a ameaças de forma eficaz e automatizada
- Capacidade de fornecer insights acionáveis para melhorar a postura de segurança da organização

#### NAC

O NAC (Network Access Control) é uma abordagem de segurança usada para restringir o acesso à rede, garantindo que apenas dispositivos autorizados e conformes com as políticas de segurança da organização possam se conectar e acessar recursos. O NAC é implementado por meio de software, hardware ou uma combinação de ambos.

##### Benefícios:

- Reforça a segurança da rede ao controlar quem e o que pode se conectar
- Ajuda a garantir a conformidade com as políticas de segurança
- Reduz o risco de ataques de dispositivos não autorizados ou não conformes
- Facilita a detecção e resposta a ameaças na rede
- Melhora a visibilidade da rede, fornecendo informações detalhadas sobre dispositivos conectados

##### Características:

- Capacidade de autenticar e autorizar dispositivos
- Capacidade de avaliar e aplicar políticas de segurança da rede
- Capacidade de isolar dispositivos não conformes ou maliciosos
- Capacidade de integrar-se com outros sistemas de segurança da informação, como firewalls e sistemas de detecção de intrusão (IDS/IPS)

## NDR

O NDR (Network Detection and Response) é uma abordagem de segurança que visa detectar e responder a ameaças na rede, monitorando o tráfego de rede em busca de comportamentos suspeitos ou indicativos de ataques. O NDR utiliza análise de tráfego em tempo real e técnicas de detecção de ameaças para identificar e responder a atividades maliciosas.

Benefícios:

- Detecta ameaças que podem passar despercebidas por outras camadas de segurança
- Fornece visibilidade detalhada do tráfego de rede e atividades suspeitas
- Ajuda a reduzir o tempo de detecção e resposta a incidentes de segurança
- Melhora a capacidade de investigação e análise de incidentes
- Complementa outras soluções de segurança, como firewalls e sistemas de detecção de intrusão (IDS/IPS)

Características:

- Capacidade de monitorar e analisar o tráfego de rede em tempo real
- Capacidade de detectar padrões de tráfego maliciosos ou suspeitos
- Capacidade de gerar alertas e relatórios sobre atividades suspeitas
- Capacidade de integrar-se com outras soluções de segurança da informação

## SOAR

SOAR é uma solução integrada para gerenciamento de incidentes de segurança. A proposta é que seja uma solução que integre ferramentas de segurança para automatizar tarefas repetitivas e orquestrar a resposta a incidentes, aumentando assim a eficiência e eficácia dos times de segurança. Abaixo as características principais de um SOAR:

- Orquestração: Coordenação automatizada de processos e atividades relacionadas à segurança, pode ser integrado a diversas ferramentas para trabalhar de forma conjunta, facilita a criação de fluxos de trabalho automatizado para resposta a incidentes.
- Automação: Execução automatizada de tarefas de rotina e repetitivas, e tarefas de resposta a incidentes como isolamento de sistemas comprometidos, coleta de evidências, entre outras.
- Resposta: Procedimentos de respostas pré-configurados de forma automatizada, mitigando ameaças rapidamente, pode incluir aplicação de correções, quarentena de sistemas, notificações, relatórios, entre outros.
- Dashboards e relatórios: Interface para monitorar e gerenciar incidentes, e emissão de relatórios detalhados sobre desempenho, eficácia e padrões de ataques.
- Integração: Integração com diversas ferramentas e sistemas através de APIs.

Quais os benefícios do SOAR?

- Redução do tempo médio de detecção e resposta
- Planos de resposta a incidentes mais estruturados
- Centralização de visão de segurança
- Automatização de tarefas repetitivas

- Redução de falsos positivos
- Padronização de processos
- Relatórios de segurança mais detalhados de forma automática

Quais as funcionalidades mínimas exigidas para o SOAR?

Para análise de requisitos de um SOAR foi feito um comparativo (G2 Compare, 2024b) entre três fabricantes do mercado (IBM, Splunk e Swimlane) e listado as funcionalidades em comum abaixo:

- Emissão de alertas
- Acompanhamento de linha de base de desempenho
- Alta disponibilidade/recuperação de desastres
- Visualização de dados
- Inteligência de ameaças
- Orquestração de Segurança
- Monitoramento de registros
- Correção Automatizada
- Mapeamento de fluxo de trabalho
- Automação de fluxo de trabalho

#### **MXDR**

Deteção e resposta estendidas gerenciadas (MXDR) estende os serviços de MDR por toda a empresa para obter uma solução totalmente gerenciada que inclui análises e operações de segurança, caça avançada a ameaças, deteção e resposta rápida em ambientes de endpoint, rede e nuvem. (Brasiline, 2021)

Quais os benefícios do MXDR?

- Redução do tempo médio de deteção
- Redução do tempo médio de investigação
- Redução do tempo médio de resposta
- Maior visibilidade do escopo de segurança
- Deteção e resposta unificadas
- Gerenciamento de vulnerabilidades
- Redução de custos
- Recursos otimizados

Quais as funcionalidades mínimas exigidas para o MXDR?

Para análise de requisitos de um MXDR foi feito um comparativo entre quatro marcas do mercado (Deloitte, s.d.), (CheckPoint, s.d.), (CrowdStrike, s.d.), (TrendMicro, s.d.) e listado as funcionalidades em comum abaixo:

- Automação de resposta
- Threat Intelligence
- Deteção baseada em regras

- Detecção em tempo real
- Machine learning
- Integração com qualquer equipamento ou solução de segurança (qualquer fabricante)

Quais os benefícios do MXDR em comparação com o SIEM e SOAR?

O SIEM coleta, agrega, analisa e armazena grandes volumes de dados de log de toda a empresa. O SIEM começou sua jornada com uma abordagem muito ampla: coleta de dados de log e eventos disponíveis de quase todas as fontes da empresa para serem armazenados em vários casos de uso. Isso incluiu governança e conformidade, correspondência de padrões baseada em regras, detecção de ameaças heurísticas / comportamentais como UEBA e busca em fontes de telemetria por IOCs ou indicadores atômicos.

As ferramentas SIEM, no entanto, requerem muitos ajustes e esforços para serem implementadas. As equipes de segurança também podem ficar sobrecarregadas com o grande número de alertas que vêm de um SIEM, fazendo com que o SOC ignore os alertas críticos. Além disso, embora um SIEM capture dados de dezenas de fontes e sensores, ainda é uma ferramenta analítica passiva que emite alertas.

A plataforma XDR visa resolver os desafios da ferramenta SIEM para detecção e resposta eficazes a ataques direcionados e inclui análise de comportamento, inteligência de ameaças, perfis de comportamento e análises.

As plataformas de orquestração de segurança e resposta automatizada (SOAR) são usadas por equipes de operações de segurança maduras para construir e executar playbooks de várias etapas que automatizam ações em um ecossistema de soluções de segurança conectado por API. Em contraste, o XDR permitirá integrações de ecossistema por meio do Marketplace e fornecerá mecanismos para automatizar ações simples contra controles de segurança de terceiros.

SOAR é complexo, caro e requer um SOC altamente maduro para implementar e manter integrações de parceiros e manuais. O XDR foi criado para ser 'SOAR-lite': uma solução simples, intuitiva e sem código que fornece capacidade de ação da plataforma XDR para ferramentas de segurança conectadas.

Um serviço MXDR aumenta os recursos XDR do cliente com serviços MDR para monitoramento adicional, investigações, caça a ameaças e recursos de resposta. (Brasiline, 2021)

Todavia, com base na avaliação da complexidade da rede, das capacidades e maturidade da equipe, optou-se pela adoção de soluções SIEM e SOAR em vez de uma plataforma XDR/MXDR. O SIEM foi escolhido por sua robustez na coleta, correlação e armazenamento centralizado de logs de múltiplas fontes, possibilitando visibilidade ampla e suporte a auditorias, conformidade e investigações aprofundadas. Já o SOAR foi selecionado para automatizar respostas e orquestrar processos complexos de segurança, aproveitando a integração com sistemas legados e a personalização de playbooks de resposta. A escolha visa atender às necessidades específicas do ambiente, que já possui ferramentas integradas e equipe capacitada para operar e evoluir essas soluções.

### Gestão de Continuidade de Serviços de TI

O processo de gestão de continuidade de serviços de TI tem como objetivo assegurar a manutenção e rápida restauração dos serviços de TI após interrupções ou desastres, minimizando o impacto dessas eventualidades nas operações da organização.

O processo abrange diversas etapas essenciais, incluindo:

- Análise de Riscos: Identificação de ameaças e vulnerabilidades que possam afetar os serviços, avaliando o impacto potencial dessas ameaças;
- Avaliação de Impacto nos Negócios: Identificação e priorização dos serviços críticos para as operações, juntamente com a determinação do tempo máximo tolerável de inatividade para cada serviço;

- Desenvolvimento de Estratégia de Continuidade: Elaboração e implementação de planos estratégicos para garantir a continuidade dos serviços, incorporando soluções como backup, redundância e recuperação de desastres, conforme necessidades específicas da organização;
- Desenvolvimento e Implementação de Planos de Continuidade: Criação de planos detalhados para cada serviço crítico de TI, definindo procedimentos de recuperação, atribuindo responsabilidades e alocando os recursos necessários;
- Testes: Realização de testes regulares para garantir a eficácia dos planos de continuidade, identificando áreas de melhoria e ajustando os planos conforme necessário;
- Conscientização: Treinamentos regulares para garantir que toda a equipe compreenda seus papéis durante uma interrupção, enfatizando a importância da continuidade dos serviços para a organização;
- Melhoria Contínua: Atualização constante dos planos para refletir mudanças na infraestrutura e operações comerciais, além de revisões periódicas das estratégias e procedimentos para garantir relevância e eficácia ao longo do tempo.

A gestão de continuidade de serviços adota uma abordagem proativa, visando capacitar as organizações a lidarem efetivamente com interrupções, minimizando impactos nos serviços críticos e acelerando os processos de recuperação.

Abaixo alguns frameworks que fornecem diretrizes para construção do processo de gestão de continuidade de serviços de TI:

- ITIL: é um conjunto de práticas amplamente adotado para gerenciamento de serviços de TI. Ele fornece um conjunto de boas práticas para o gerenciamento de serviços de TI, incluindo a gestão de continuidade de serviços. (InterOp, 2022)
- COBIT: a estrutura do processo “DS4 - Assegurar a “Continuidade dos Serviços” encontra-se no domínio de entrega e suporte do COBIT 4.1. Este processo foca na disponibilidade dos serviços de TI, através de desenvolvimento, manutenção e testes do plano de continuidade de TI provendo a continuidade dos serviços de TI. (Castilho, Continuidade dos Serviços de TI, 2015)
- ISO 22301: é uma norma de sistema de gestão publicada pela Organização Internacional de Padronização que especifica requisitos para planejar, estabelecer, implementar, operar, monitorar, revisar, manter e melhorar continuamente um sistema de gestão documentado para proteger contra reduzir a probabilidade de ocorrência, preparar-se para responder e recuperar-se de incidentes perturbadores quando eles surgirem. Pretende-se que seja aplicável a todas as organizações, ou partes delas, independentemente do tipo, tamanho e natureza da organização. (Wikipedia, 2024)

### Rotina de backup

O que é backup?

A palavra em inglês Backup, significa em português “cópia de segurança” e segundo o Wikipédia é:

“A cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados”.

Sendo assim, seus arquivos são copiados para um outro local e podem ser acessados caso aconteça algum problema e os originais. Sejam perdidos devido a vírus, problemas físicos no computador ou no caso de alguém apagar de forma proposital ou alterar sem querer, por exemplo. (InformaTI, 2024)

Uma rotina de backup é um processo que tem como objetivo realizar cópias de dados e arquivos importantes e armazená-los num local seguro. Essas cópias são essenciais para a organização, pois ajudam a proteger os dados

contra perdas acidentais ou intencionais. O backup regular reduz o risco de perda irreparável de dados em caso de falha de hardware, exclusão acidental ou corrupção de arquivos.

Em casos de ataques de ransomware ou outros tipos de malware, ter cópias de backup pode ser crucial para restaurar os dados sem ceder às exigências de resgate. Em situações de desastres, como incêndios, inundações ou terremotos, as cópias de backup facilitam a recuperação rápida dos dados, minimizando o tempo de inatividade. O backup também pode ajudar a preservar a integridade dos dados ao longo do tempo, permitindo a recuperação de versões anteriores dos arquivos se necessário.

Na política de backup da organização deve estar registrado quais dados e arquivos precisam ser copiados, quantas cópias devem ser feitas, onde os arquivos devem ser copiados, qual a melhor opção de backup (local, nuvem, ambos), quando os arquivos devem ser copiados e com qual frequência, se vai ser backup completo, incremental ou diferencial, também deve ser determinado testes periódicos no backup, bem como um plano de recuperação de desastres e o processo deve ser monitorado regularmente, verificando se os dados estão sendo salvos e se as cópias estão atualizadas.

Caso o método de backup escolhido seja a nuvem, algumas informações essenciais devem ser observadas, como o método de autenticação utilizado, se há restrições de tipo ou tamanho de arquivo, qual o custo, políticas de privacidade, se está em conformidade com as normas e leis que abrangem a organização, qual o procedimento para restauração, o tempo e a capacidade máximos para download, qual o tempo máximo de retenção dos dados e arquivos, qual a reputação da nuvem escolhida, qual o tempo médio de disponibilidade do portal, se existe suporte disponível, e opinião dos usuários.

As cópias devem ser periódicas, seguindo a lógica de criação ou modificação dos arquivos, o ideal é que sejam realizadas 3 cópias, em 2 tipos de mídia e que pelo menos 1 delas seja offline. Os backups devem ser identificados com informações que ajudem a localizar o tipo do arquivo e a data de gravação. A recuperação pode ser feita parcial ou totalmente, de acordo com a necessidade.

Uma rotina de backup bem executada é uma parte fundamental de uma estratégia abrangente de segurança da informação, garantindo a disponibilidade e a integridade dos dados essenciais para uma organização.

### Red Team

Equipe formada por especialistas em segurança da informação, com atuação voltada para testes de simulação de ataques com o objetivo de identificar e corrigir vulnerabilidades antes que estas sejam exploradas.

O analista red team é responsável por:

- Simulação de ataques: O analista se passa por um atacante, fazendo uso de diversas táticas e técnicas (mapeadas no mitre att&ck) para explorar as vulnerabilidades da rede, sistemas e usuários.
- Testes controlados de resposta a incidentes: Consiste basicamente no analista simular um incidente de segurança para avaliação da eficiência e eficácia do plano de resposta a incidentes e da postura dos envolvidos.
- Análise de vulnerabilidade: Identificação e análise das vulnerabilidades e seus riscos associados nos sistemas e ativos, políticas e controles, visando corrigir ou mitigar os possíveis impactos ao negócio.
- Treinamentos: Fornece treinamentos em segurança para os colaboradores de forma a conscientizar os usuários sobre as ameaças, melhores práticas e respostas a incidentes.
- Relatórios: Emissão de relatórios de testes e da saúde da segurança da rede, das vulnerabilidades e as recomendações de correção e seus respectivos impactos caso não sejam corrigidas.

Deverá ser exigido o seguinte nível de conhecimento mínimo dos analistas:

- Formação em segurança da informação ou sistemas da informação

- Certificações CEH, OSCP ou equivalentes
- Experiência em testes de invasão e exploração de vulnerabilidades, e condução de treinamentos.

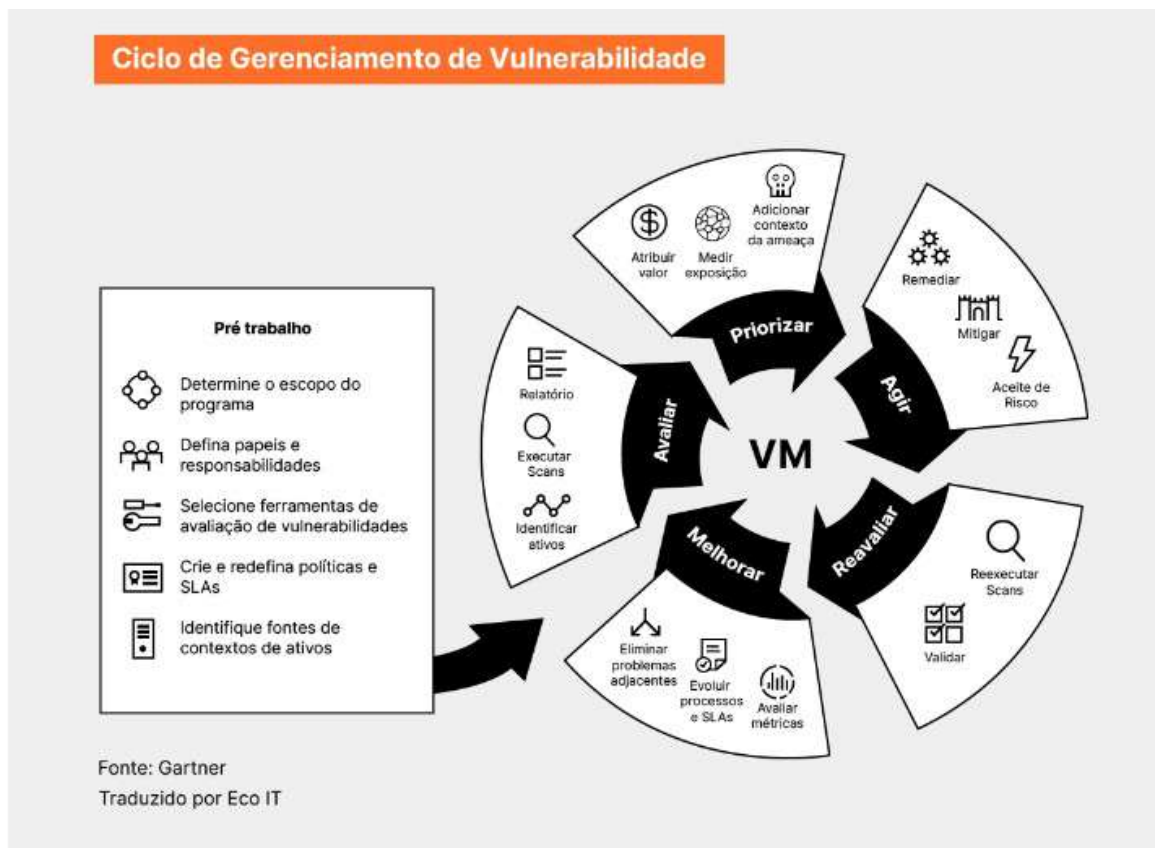
### Gestão de vulnerabilidades

O processo de gestão de vulnerabilidades tem como objetivo identificar, avaliar, corrigir e mitigar vulnerabilidades em sistemas e ativos, que podem ser decorrentes de configurações inadequadas, sistemas desatualizados ou outros pontos fracos exploráveis por ameaças, resultando em incidentes de segurança da informação.

O processo abrange diversas etapas, iniciando-se pela identificação de vulnerabilidades. As vulnerabilidades de segurança em Tecnologia da Informação são meticulosamente catalogadas e rastreadas por meio da lista de CVEs. Gerenciada pela MITRE Corporation e financiada pela Agência de Cibersegurança e de Infraestrutura (CISA), que faz parte do Departamento de Segurança Interna dos EUA, essa lista é um recurso vital para o setor. Pesquisadores, fornecedores e membros da comunidade de código aberto têm a capacidade de submeter suas falhas de segurança à lista de CVEs.

A identificação dessas vulnerabilidades envolve uma busca proativa por brechas em sistemas e redes, podendo ser conduzida manualmente por uma pessoa ou por meio de sistemas especializados. Com as vulnerabilidades devidamente identificadas, o próximo passo é a avaliação dos riscos diretamente associados a elas, atribuindo uma priorização. Nesse contexto, o Sistema de Pontuação de Vulnerabilidade Comum (CVSS) emerge como um padrão do setor, aplicando uma fórmula que considera diversos fatores, como a probabilidade de um possível ataque remoto, a complexidade do ataque e a necessidade de ação por parte do usuário. O CVSS atribui a cada CVE uma pontuação que varia de 0 (nenhum impacto) a 10 (maior impacto), baseando-se no cruzamento entre probabilidade e impacto dos riscos associados.

Com a devida priorização estabelecida, o próximo passo é a implementação das correções necessárias. Por fim, o processo culmina com o monitoramento contínuo, que envolve a verificação constante de novas vulnerabilidades. Nesse sentido, é crucial priorizar e aplicar as correções necessárias para manter a segurança do sistema. (Red Hat, 2023)



(EcoTrust, 2023)

A ISO/IEC 27002 (controle 12.6) diz o seguinte:

- Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.
- Um inventário completo e atualizado dos ativos de informação é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica. Informação específica para o apoio à gestão de vulnerabilidade técnica inclui o fornecedor de software, o número da versão, o status atual de desenvolvimento (por exemplo, quais softwares estão instalados e em quais sistemas), e a(s) pessoa(s) na organização responsável (is) pelos softwares.
- Convém que seja tomada ação apropriada, no devido tempo, como resposta às potenciais vulnerabilidades técnicas identificadas.
- É fundamental que a gestão de vulnerabilidades seja encarada como um processo contínuo, uma vez que desempenha um papel crucial na identificação e correção das brechas de segurança, reduzindo substancialmente os riscos de exploração por ameaças. Ao estabelecer um processo sólido, a equipe de segurança se capacita para uma constante atualização e adaptação às novas ameaças, resultando na redução efetiva da probabilidade de ataques e na prevenção de potenciais violações de segurança. Essa abordagem proativa não apenas fortalece a postura de segurança da organização, mas também promove a resiliência frente às ameaças em constante evolução.

### Scanner de vulnerabilidades

As ferramentas para scanear a rede em busca de vulnerabilidades são construídas com o objetivo de identificar e analisar potenciais vulnerabilidades nos sistemas, redes e dispositivos. É de extrema importância para a seguran-

ça, visto que ao identificar as vulnerabilidades, estas devem ser corrigidas antes de serem exploradas por alguma ameaça, diminuindo assim a probabilidade de ocorrer um incidente de segurança da informação.

O scan busca ativamente por possíveis fraquezas em sistemas, redes e dispositivos, incluindo falhas de configuração, ausência de atualização, e qualquer outro aspecto que torne o ativo vulnerável para exploração. Geralmente as varreduras são feitas de forma automática periodicamente, buscando por padrões de vulnerabilidade, geralmente configurado pelo time de TI e em especial em redes extensas e complexas, onde a identificação manual pode se tornar impraticável.

Ao fazer a varredura as vulnerabilidades encontradas são classificadas de acordo com a gravidade e o impacto, tornando claro quais itens precisam ser corrigidos com urgência. Essas ferramentas em geral emitem relatórios detalhados descrevendo as vulnerabilidades localizadas, o grau de severidade, como pode ser explorada e como corrigir antes que esta seja explorada por um atacante.

O time de TI deve realizar as correções o quanto antes com base na priorização, e o esforço deve ser contínuo, monitorando regularmente o ambiente e garantindo que as fraquezas sejam corrigidas de imediato.

Para análise de requisitos mínimos de uma ferramenta de scan de vulnerabilidades foi realizado uma pesquisa em alguns sites das principais ferramentas recomendadas, e dessa relação fora selecionadas as ferramentas mais citadas.

(SITE 1, s.d.)	(SITE 2, s.d.)	(SITE 3, s.d.)	(SITE 4, s.d.)
Nessus	Nessus Essentials	Nuclei	OpenVAS
QualysGuard	Nexpose Community Edition	Nikto	Tripwire IP360
OpenVAS	OpenVAS	Cariddi	Nessus Vulnerability Scanner
Acunetix	Qualys Community Edition	OpenVAS	Comodo HackerProof
Burp Suite	ManageEngine Vulnerability Manager	Wapiti	Nexpose Community
Rapid7 Nexpose			Vulnerability Manager Plus
EcoTRUST			Nikto
Qualys Vulnerability Management			Wireshark
McAfee Vulnerability Manager			Aircrack-ng
Rapid7 InsightVM			Retina network security scanner

As ferramentas escolhidas foram a OpenVAS (citada nos 4 sites), a Nessus (citada em 3 dos 4 sites) e a Nexpose (citada em 2 dos 4 sites). De acordo com o comparativo (G2, 2024) entre as ferramentas selecionadas, segue abaixo a relação de funcionalidades em comum entre elas, que podem ser considerados como os critérios mínimos recomendados a serem exigidos:

- Verificações automatizadas
- Teste de conformidade
- Varredura de perímetro
- Monitoramento de configuração
- Análise de código estático
- Teste de caixa preta

#### Testes de intrusão

Os testes de intrusão são necessários para avaliação de segurança da organização. O objetivo principal é realizar simulações de exploração de vulnerabilidades e ataques para localizar os principais pontos de falhas de segurança e corrigi-las o mais rápido possível, diminuindo assim as chances de sofrer um ataque.

Os testes devem ser realizados pelo Red Team em um ambiente de testes controlado preferencialmente, porém, pode ser realizado também no ambiente de produção, tomando todos os cuidados necessários para não haver interrupção ou danos no serviço, e deve seguir as políticas da organização e ter autorização prévia. O ideal é que siga uma linha de planejamento muito bem definida e documentada.

Abaixo as etapas recomendadas para execução plena dos testes:

- **Planejamento:** na fase de planejamento deve ser levantado os dispositivos e sistemas que serão testados, e quais testes serão realizados, e com o escopo previamente definido, este deve ser autorizado formalmente pelas autoridades da organização.
- **Fase inicial:** na fase inicial é feito o levantamento das informações dos alvos como IP, serviços associados, sistemas, entre outros, além das vulnerabilidades expostas desses alvos, feita a devida identificação, os alvos serão então explorados.
- **Exploração:** nessa fase são utilizados exploits e técnicas hacking, simulando ataques para identificar até onde as vulnerabilidades existem e podem ser exploradas.
- **Execução:** se na fase anterior o analista obtiver sucesso, ele deverá persistir no acesso e simular o que um atacante verdadeiro faria, explorando informações sensíveis e executando ações de caráter malicioso, sem causar danos permanentes ao serviço.
- **Relatórios:** após todos os testes serem realizados, o analista deve documentar todas as informações da ação, desde o planejamento, passando pela fase de reconhecimento, exploração e finalmente os testes que foram feitos e seus resultados. Recomendações de correção devem ser feitas em detalhes e todas as informações devem ser documentadas e repassadas para as autoridades responsáveis para dar início ao plano de correção.
- **Correção:** com as correções necessárias mapeadas e o plano desenhado, deve-se dar início as correções para eliminar totalmente a vulnerabilidade ou mitigar ao nível máximo possível.
- **Melhoria contínua:** após as devidas correções serem executadas, estas devem ser acompanhadas para garantir a efetividade da correção, e periodicamente os testes devem ser repetidos, para acompanhar as novas ameaças da cibersegurança.

Durante todo o processo deve ser garantida as responsabilidades do analista, o comprometimento em ethical hacking deve ser explícito, e o profissional deve ser adequadamente qualificado para garantia de que as avaliações sejam realizadas de maneira controlada sem causar danos aos serviços e ao negócio. Termos de confidencialidade podem ser assinados, e as políticas da organização devem ser seguidas para garantir a conformidade.

### **Ambiente de testes**

O ambiente de testes controlado é importante para a organização pois nele serão executados os testes de exploração de vulnerabilidades e testes de invasão, simulando diversos cenários de ataques de segurança da informação.

Para um ambiente de testes bem-sucedido é importante que a rede seja simulada no máximo nível possível, de forma que todas as brechas sejam observadas e testadas, portanto, é crucial que no ambiente tenha-se os mesmos sistemas e serviços da rede real, por exemplo, firewall, servidores, versão de sistema operacional etc.

Ferramentas poderão ser usadas para auxílio nos testes, como scanner de vulnerabilidades por exemplo, ou até mesmo uma máquina virtual com o sistema kali Linux, visto que possui diversas ferramentas para apoio nos testes.

Deve-se também manter-se atualizado nos últimos lançamentos da segurança, tanto no quesito malwares quanto ferramentas de testes e proteção, visando a melhoria contínua.

Com o ambiente controlado, os testes podem ser iniciados, a matriz do Mitre Att&ck pode ser usada como base para uso das táticas e técnicas dos atacantes, simulando diversos tipos de ataque para levantamento das fraquezas do ambiente, após o resultado, os relatórios devem ser gerados e enviados as partes interessadas para as devidas ações de correção.

Dito isso, o ambiente deve ser construído o mais próximo da rede real possível, e ferramentas de scanner de vulnerabilidades, e ataque devem ser usadas para a exploração. A ferramenta mais comum para construção de malwares é o Kali Linux, outras equivalentes podem ser utilizadas.

### Conectividade Redundante

Diante da criticidade das operações realizadas nos diversos sites governamentais do Estado de Pernambuco, é essencial a implantação de uma rede com alta disponibilidade e redundante, de modo a assegurar a continuidade dos serviços públicos. Para tanto, será explorada a utilização de diferentes tecnologias de conectividade:

- **Link Banda Larga:** Solução de conectividade que utilizando tecnologias como GPON, XG-PON e XGS-PON, a velocidade pode alcançar até **10 Gbps**. Oferece alta disponibilidade (99,5%), latência abaixo de 50 ms e jitter controlado (<30 ms), assegurando estabilidade para aplicações sensíveis. Com fibra óptica, garante escalabilidade e resiliência, especialmente quando combinada com soluções de failover, com grande foco em custo-benefício.
- **Link Ponto a Ponto (P2P):** Ideal para sites críticos. Oferece alta segurança com velocidades de 1 Gbps a 10 Gbps, latência de até 10 ms e disponibilidade de 99,9%, garantindo confiabilidade e privacidade.
- **Satélite LEO:** Adequado para áreas remotas, com baixa latência (20-40 ms), velocidade até 100 Mbps e redundância eficiente. Ótimo para sites com demanda de conectividade rápida e estável em locais inacessíveis.
- **Satélite MEO:** Cobertura robusta com velocidades semelhantes ao LEO, mas com maior latência (até 100 ms). Indicado para locais mais distantes ou que requerem alta resiliência em regiões sem infraestrutura terrestre.
- **5G Fixed Wireless Access (FWA):** Alta velocidade (até 1 Gbps) e latência extremamente baixa (inferior a 10 ms), ideal para sites de alta demanda e sensíveis a tempo de resposta. Além da alta velocidade, o 5G traz a vantagem de implantação rápida, sem a necessidade de infraestrutura física extensa, como cabos de fibra, sendo uma excelente opção para áreas urbanas e de difícil acesso.

A disponibilidade do 5G pode alcançar **99,7%**, e com redundância em redes 4G como backup, garantindo continuidade operacional. Sua capacidade de atender a múltiplos dispositivos simultaneamente, aliada à resiliência de redes sem fio, faz do 5G FWA uma solução estratégica para locais com alta densidade de usuários e grandes demandas de dados.

A escolha da tecnologia de conectividade para cada site deverá considerar a criticidade das operações locais, bem como as condições de viabilidade técnica e financeira para sua implementação. O uso de links complementares em áreas urbanas e remotas fortalece a infraestrutura, minimizando interrupções e assegurando a continuidade dos serviços governamentais.

A utilização de satélites LEO para áreas críticas remotas e 5G FWA para ambientes urbanos maximiza a eficiência e resiliência da rede, permitindo maior flexibilidade, resiliência e alta disponibilidade à rede governamental, atendendo a todas as demandas de serviço e continuidade de operações do Estado de Pernambuco.

### Gestão de Riscos

A gestão de riscos de segurança é um processo que determina a aplicação equilibrada de controles de segurança na organização, de acordo com o seu perfil de riscos de segurança. É necessária para mitigar a probabilidade de exposição ou perda resultante de uma vulnerabilidade sendo explorada por uma ameaça. Podemos utilizar a norma ISO/IEC 27002:2013 (ABNT/CB-21, 2013) como apoio para a estruturação do processo, visto que é uma norma que fornece diretrizes para a gestão de riscos.

A seguir o descritivo das fases da gestão de riscos:

- **Identificação:** O propósito é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. Convém que a identificação de riscos inclua os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.
  - **Identificação dos ativos:** Um ativo é algo que tem valor para a organização e que, portanto, requer proteção. Para a identificação dos ativos convém que se tenha em mente que um sistema de informação compreende mais do que hardware e software. Convém que seja executada com um detalhamento adequado que forneça informações suficientes para o processo de avaliação de riscos.
  - **Identificação das ameaças:** Uma ameaça tem o potencial de comprometer ativos. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as fontes de ameaças acidentais, quanto as intencionais, sejam identificadas. Uma ameaça pode surgir de dentro ou de fora da organização.
  - **Identificação dos controles existentes:** Convém que a identificação dos controles existentes seja realizada para evitar custos e trabalho desnecessários. Além disso, enquanto os controles existentes estão sendo identificados, convém que seja feita uma verificação para assegurar que eles estão funcionando corretamente. Convém que seja levada em consideração a possibilidade de um controle selecionado falhar durante sua operação, sendo assim, controles complementares são necessários para tratar efetivamente o risco identificado.
  - **Identificação das vulnerabilidades:** A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças.
  - **Identificação das consequências:** Uma consequência pode ser, por exemplo, a perda da eficácia, condições adversas de operação, a perda de oportunidades etc. Essa atividade identifica o prejuízo ou as consequências para a organização que podem decorrer de um cenário de incidente.
- **Análise:** A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Uma metodologia para a análise pode ser qualitativa ou quantitativa ou uma combinação de ambos, dependendo das circunstâncias.
  - **Análise qualitativa:** A análise qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo, pequeno, médio e grande) e a probabilidade dessas consequências ocorrerem.
  - **Análise quantitativa:** A análise quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na análise qualitativa) tanto para consequências quanto para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integridade dos valores numéricos e da validade dos modelos utilizados.

- **Avaliação:** Para avaliar os riscos, convém que as organizações comparem os riscos estimados com os critérios de avaliação de riscos definidos durante a definição do contexto. Convém que os critérios de avaliação de riscos utilizados na tomada de decisões sejam consistentes com o contexto definido, externo e interno, relativo à gestão de riscos de segurança da informação e levem em conta os objetivos da organização, o ponto de vista das partes interessadas etc.
- **Tratamento:** Há quatro opções disponíveis para o tratamento do risco: modificação do risco, retenção do risco, ação de evitar o risco e compartilhamento do risco. Convém que as opções do tratamento do risco sejam selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.
  - **Modificação do risco:** Convém que controles apropriados e devidamente justificados sejam selecionados para satisfazer os requisitos identificados através do processo de avaliação de riscos e do tratamento deles. Convém que essa escolha leve em conta os critérios para a aceitação do risco assim como requisitos legais, regulatórios e contratuais. Convém que essa seleção também leve em conta custos e prazos para a implementação de controles, além de aspectos técnicos, culturais e ambientais.
  - **Retenção do risco:** Se o nível de risco atende aos critérios para a aceitação do risco, não há necessidade de se implementar controles adicionais e pode haver a retenção do risco.
  - **Ação de evitar o risco:** Quando os riscos identificados são considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja através da eliminação de uma atividade planejada ou existente, seja através de mudanças nas condições em que a operação da atividade ocorre.
  - **Compartilhamento do risco:** O compartilhamento do risco envolve a decisão de se compartilhar certos riscos com entidades externas. O compartilhamento do risco pode criar riscos ou modificar riscos existentes e identificados. Portanto, um novo tratamento do risco pode ser necessário.
  - **Aceitação do risco:** Convém que os planos de tratamento do risco descrevam como os riscos serão tratados para que os critérios de aceitação do risco sejam atendidos. Em alguns casos, o nível de risco residual pode não satisfazer os critérios de aceitação do risco, pois os critérios aplicados não estão levando em conta as circunstâncias predominantes no momento. Tais circunstâncias indicam que os critérios para a aceitação do risco são inadequados e convém que sejam revistos, se possível. No entanto, nem sempre é possível rever os critérios para a aceitação do risco no tempo apropriado. Nesses casos, os tomadores de decisão podem ter que aceitar riscos que não satisfaçam os critérios normais para o aceite.
- **Implementação de controles:** A implementação de controles no processo de gestão de riscos da segurança da informação é uma etapa crucial para garantir a proteção dos ativos e a continuidade dos negócios. Essa etapa envolve a aplicação prática das medidas planejadas durante a análise de riscos. A implementação de controles no processo de gestão de riscos é um ciclo contínuo que requer adaptação constante para lidar com as mudanças no ambiente de segurança da informação.
- **Monitoramento e revisão:** Os riscos não são estáticos. As ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar abruptamente, sem qualquer indicação. Portanto, o monitoramento constante é necessário para que se detectem essas mudanças. Serviços de terceiros que forneçam informações sobre novas ameaças ou vulnerabilidades podem prestar um auxílio valioso. Convém que quaisquer melhorias ao processo ou quaisquer ações necessárias para melhorar a conformidade com o processo sejam comunicadas aos gestores apropriados, para que se possa ter a certeza de que nenhum risco ou elemento do risco será ignorado ou subestimado, que as ações necessárias estão sendo executadas e

que as decisões corretas estão sendo tomadas a fim de se garantir uma compreensão realista do risco e a capacidade de reação.

- **Comunicação e conscientização:** A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos. A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões que devem ser tomadas. A comunicação assegurará que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito tenham um bom entendimento do porquê as decisões são tomadas e dos motivos que tornaram certas ações necessárias.
- **Documentação e relatórios:** A etapa de documentação e relatórios no processo de gestão de riscos desempenha um papel fundamental na transparência, comunicação e tomada de decisões informadas. Convém que sejam documentados todos os resultados da análise de riscos, incluindo a identificação de ameaças, vulnerabilidades, impactos potenciais e a avaliação de riscos. Convém registrar todos os controles recomendados para mitigar, transferir, aceitar e evitar os riscos identificados, e fornecer informações detalhadas sobre a implementação planejada de cada controle. A documentação e os relatórios não apenas fornecem uma base para tomadas de decisões informadas, mas também são essenciais para a prestação de contas, auditorias e demonstração de conformidade com padrões de segurança. É importante manter essa documentação atualizada e acessível para garantir uma resposta eficaz a eventos de segurança e para apoiar a evolução contínua do programa de segurança da informação.
- **Melhoria contínua:** Convém realizar revisões regulares do processo de gestão de riscos para avaliar sua eficácia, identificando áreas que podem ser aprimoradas e ajustar os procedimentos se necessário. Convém avaliar regularmente a implementação e eficácia dos controles, identificando e corrigindo quaisquer desvios ou falhas nos controles. A melhoria contínua no processo de gestão de riscos da segurança da informação é um ciclo iterativo que visa manter a organização resiliente contra ameaças em constante evolução. A adaptabilidade e a capacidade de aprender com a experiência são elementos-chave nesse processo.

### **Matriz de Probabilidade e Impacto**

Matriz de probabilidade e impacto é uma ferramenta utilizada para realizar a gestão de riscos de uma organização, é composta por duas informações, que se trata justamente da probabilidade de um risco ocorrer, que é representada por porcentagem, escala ou qualquer outra forma preferível pela organização, e caso ele ocorra, qual será o impacto e as consequências para a organização, geralmente representado por escala (baixa, média, alta).

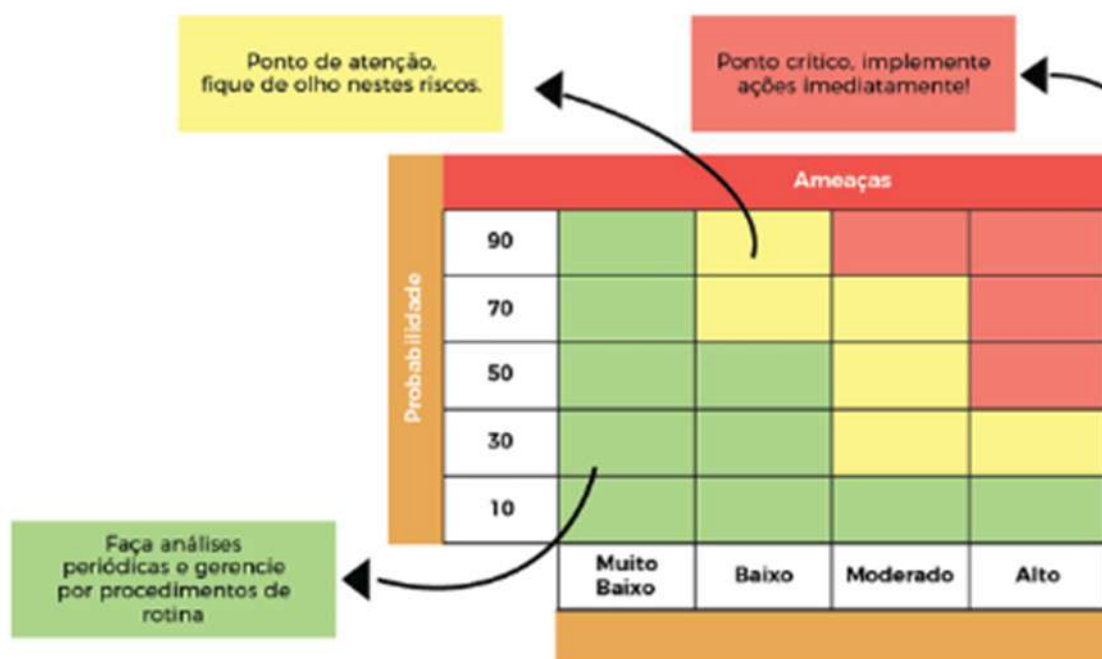
Serve para auxiliar na priorização do tratamento dos riscos, facilitando a tomada de decisões sobre qual risco deverá ser eliminado primeiro, bem como fornece uma visão clara e objetiva do cenário e quais os riscos mais sensíveis para todos os envolvidos. Com a matriz devidamente preenchida, é possível também de forma mais objetiva definir ações de resposta a esses riscos, contribuindo para direcionar os responsáveis aos esforços que realmente fazem sentido para os objetivos da organização.

Abaixo um exemplo de matriz:

Probabilidade	90%	Média	Média	Alta	Alta	Alta
	70%	Baixa	Média	Média	Alta	Alta
	50%	Baixa	Baixa	Média	Alta	Alta
	30%	Baixa	Baixa	Média	Média	Alta
	10%	Baixa	Baixa	Baixa	Baixa	Média
		Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Impacto						

(Napoleão, 2019)

A tratativa dos riscos deve ser feita de acordo com a disposição desses riscos na matriz. A figura apresenta um guia de como ler a matriz e ajudar na priorização da tratativa dos riscos classificados pela ferramenta.



(Napoleão, 2019)

Após realizar o mapeamento de todos os riscos da organização, deve-se usar a matriz para elencar o nível de criticidade do risco, seguido da priorização para então aplicar o plano de respostas mapeado para os riscos mais prioritários.

### **ISO/IEC 27005**

A norma ISO/IEC 27005 é um padrão internacional que fornece diretrizes e princípios para a gestão de riscos de segurança da informação.

Ela especifica os processos e as atividades para a gestão de riscos de segurança da informação, com o objetivo de ajudar as organizações a identificar, avaliar e tratar os riscos associados à segurança da informação.

Abaixo alguns dos pontos-chave abordados pela ISO/IEC 27005:

A norma destaca a importância de entender o contexto organizacional, incluindo os objetivos, as partes interessadas e o ambiente em que a organização opera.

Enfatiza a abordagem baseada em riscos para a gestão da segurança da informação, o que significa que as medidas de segurança devem ser proporcionais aos riscos identificados.

Fornece um framework para a gestão de riscos, incluindo processos como avaliação de riscos, tratamento de riscos e monitoramento contínuo.

Destaca a importância da comunicação e consulta com as partes interessadas durante todo o processo de gestão de riscos.

Inclui a necessidade de estabelecer e manter um processo de melhoria contínua para garantir que a gestão de riscos de segurança da informação evolua com as mudanças no ambiente organizacional e nas ameaças.

Ou seja, a ISO/IEC 27005 é valiosa para organizações que desejam estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de riscos de segurança da informação eficaz. Ela pode ser usada em conjunto com outros padrões da série ISO/IEC 27000 para fornecer uma abordagem abrangente para a segurança da informação em uma organização.

No documento Descritivo de processos – Gestão de riscos há a descrição de todas as etapas das diretrizes da norma.

### **ISO/IEC 27002**

A norma ISO/IEC 27002 representa um padrão internacional que orienta a gestão da segurança da informação, oferecendo diretrizes e princípios. Seu propósito é auxiliar as organizações na implementação de controles de segurança da informação e na criação de um Sistema de Gestão da Segurança da Informação (SGSI).

Abaixo alguns pontos fundamentais abordados pela norma:

Garantir a confidencialidade das informações quando necessário, preservar a integridade e assegurar a disponibilidade quando requerido.

Identificar e avaliar os riscos associados à segurança da informação, implementando controles para mitigar esses riscos.

Fornecer um conjunto de controles e boas práticas para proteger as informações contra ameaças.

Promover a melhoria contínua na gestão da segurança da informação por meio de avaliações regulares e ajustes no sistema de gestão.

Ao adotar as orientações da ISO 27002, as organizações conseguem reforçar sua postura em relação à segurança da informação, reduzir riscos, aumentar a confiança de clientes e partes interessadas, e atender aos requisitos regulamentares ligados à segurança da informação.

Dessa forma, é possível estruturar os processos do SOC com base na ISO 27002, alinhando todo o setor e suas atividades aos padrões internacionais.

### Gestão de Conformidade

O processo de gestão de conformidade tem como objetivo garantir que a organização esteja seguindo os padrões regulatórios, leis, normas, políticas, frameworks adotados, ou qualquer outra diretriz relacionada a segurança da informação que a empresa esteja comprometida.

Cada organização está destinada a seguir leis e regulamentos específicos, mas além deles, há também a obrigatoriedade de cumprimento da LGPD por exemplo, que é a Lei Geral de Proteção de Dados, que visa basicamente assegurar que as organizações cumpram os requisitos legais para proteção da privacidade e dados pessoais e sensíveis.

Além da LGPD temos as políticas nacionais (como a Política Nacional de Cibersegurança) estaduais (como a Política Estadual de Segurança da Informação) e/ou municipais, que visam regular as práticas relacionadas à segurança da informação. Há também as normas e padrões regulatórios da segurança da informação, como a ISO/IEC 27001, PCI DSS, entre outros.

Recomenda-se que toda organização escreva sua política de segurança da informação particular e suas políticas complementares, como política de backup, política de BYOD, e todas as que a organização entender serem necessárias para o cenário.

Para todos os casos, é necessário que tenha um time olhando para a conformidade com esses padrões e regulamentos, realizando auditorias periódicas, análise de conformidade e efetividade, bem como treinamentos para os colaboradores e usuários, para que estes estejam alinhados com os objetivos da organização no que diz respeito ao cumprimento do regulamento.

Abaixo as etapas do processo de gestão de conformidade:

- **Avaliar:** A avaliação envolve identificar sistemas, processos, fornecedores ou aplicativos que não estejam em conformidade. Isso pode incluir sistemas vulneráveis ou sem aplicação de patches ou, simplesmente, os que não atendem aos requisitos normativos de outras maneiras.
- **Priorizar:** Ao classificar os problemas de conformidade com base no risco envolvido para o negócio e nos recursos necessários para corrigi-los, as organizações podem trabalhar para resolver primeiro os problemas mais fáceis de acessar, antes de avançar para outros que podem não ser tão urgentes ou tão simples.
- **Responder:** A conformidade se concentra em monitorar, priorizar e relatar problemas, em vez de corrigi-los. Quando os problemas de conformidade são detectados, a equipe de gerenciamento de conformidade deve analisar os detalhes e decidir se deve transferi-los para a TI ou para outra equipe para fins de correção ou, simplesmente, aceitar o risco associado e deixar o problema de conformidade não resolvido.
- **Relatar:** Quando todas as mudanças tiverem sido feitas e os sistemas tiverem sido reavaliados, crie um relatório que confirma que as mudanças foram efetivadas e que o sistema agora está em conformidade.
- **Melhoria contínua** - O monitoramento contínuo ajudará a identificar tendências, reconhecer problemas de não conformidade mais rapidamente e apresentar atualizações em tempo real de resoluções e exceções. (ServiceNow, 2024)

A gestão de conformidade é de extrema importância para qualquer organização, não apenas por mitigar as chances de multas e penalidades, mas para auxiliar na disseminação da construção de uma cultura organizacional orientada a segurança e proteção de dados, bem como consolidar uma imagem de confiança para todos os stakeholders.

### Gestão da Qualidade da Segurança da Informação

O processo de gestão da qualidade da segurança da informação consiste na integração do processo de gestão da qualidade com as boas práticas de segurança da informação na organização.

Ao unir essas duas abordagens, estabelecemos um conjunto de atividades e práticas destinadas a assegurar a proteção eficaz dos ativos e informações contra ameaças, bem como o gerenciamento eficiente desses recursos. Para garantir uma aplicação plena desse processo e promover melhorias contínuas nos procedimentos, é recomendável utilizar o ciclo PDCA.

Na fase de planejamento (Plan), é essencial realizar o mapeamento e a identificação de ativos e riscos, desenvolver estratégias, criar políticas, estabelecer planos de continuidade, atribuir responsabilidades e conduzir outros procedimentos relacionados ao planejamento dos processos de segurança da informação.

Na fase de execução (Do), como sugere o próprio nome, ocorre a implementação do planejamento. Nessa etapa, são colocadas em prática as ações mapeadas dos processos, envolvendo seus executores, sejam ferramentas ou pessoas.

A fase de checagem (Check) incorpora relatórios, auditorias e testes para garantir a entrega nos níveis acordados, assegurando a tríade da segurança da informação: confidencialidade, integridade e disponibilidade.

Por último, mas não menos importante, a fase de ação (Act) entra em cena. Com base nas verificações anteriores, ajustes são aplicados em falhas e brechas identificadas, visando fortalecer as camadas de proteção da rede.

Dessa maneira, o processo de gestão da qualidade da segurança da informação assegura a observância de todo o ciclo, abrangendo todos os processos mapeados em cada fase mencionada acima. Isso possibilita a aplicação da melhoria contínua nos processos de segurança, preservando a qualidade do serviço e a proteção da informação. Além do PDCA, normas como a família ISO/IEC oferecem suporte nesse processo.

ISO 27001 vs. ISO 9001: Onde estão as conexões?

As duas normas internacionais, ISO 27001 para segurança da informação e ISO 9001 para gestão da qualidade, tratam dos temas relevantes no Capítulo 6.1 "Medidas para lidar com os riscos e oportunidades". Em essência, o objetivo é assegurar três aspectos essenciais no sistema de gestão:

- Atingir os resultados pretendidos pela sua organização
- Prevenir ou reduzir os efeitos indesejáveis
- Atingir a melhoria contínua através do cumprimento de certas normas

A segurança da informação vai de encontro à gestão da qualidade - quais são os benefícios?

- Um processo que olha fundamentalmente os riscos de segurança da informação pode servir como um primeiro e importante passo para um sistema de gestão abrangente de segurança da informação de acordo com a ISO/IEC 27001.
- Ao implementar tal processo, a alta gestão fortalece a consciência da segurança da informação e dos dados (proteção de dados) a todos os níveis.
- Com a consideração orientada dos riscos de segurança da informação, uma empresa tem a oportunidade de descobrir a necessidade de ação e de tomar as medidas adequadas (orientadas para a ISO 27001, Anexo A).
- A avaliação de risco ampliada para incluir a segurança da informação, por exemplo, como parte da gestão da qualidade, reforça a abordagem global baseada no risco de uma empresa.
- Tanto os recursos financeiros como humanos necessários para a implementação e os testes de eficácia são manejáveis. (DQS Global, 2022)

## Setorial

Equipe responsável por monitoramento proativo do SOC, bem como atividades relacionadas a configurações de segurança, relatoria e atendimento de incidentes e requisições reativos. O time deverá atuar 24x7, com todos os processos, tecnologias e pessoas (mesmos conhecimentos) do SOC da ATI (equipe coordenadora). Levando em consideração os modelos de times do NIST para resposta a incidentes de segurança da informação, para o time setorial pode ser adotado o modelo Equipe (equipes distribuídas de resposta a incidentes) – Equipe coordenadora, onde o SOC da ATI atuaria como um SOC central coordenando os SOCs setoriais no modelo parcialmente terceirizado.

De acordo com o Computer Security Incident Handling Guide do NIST, existem as seguintes estruturas possíveis para o time de resposta a incidentes:

- **Equipe Central de Resposta a Incidentes:** Uma única equipe de resposta a incidentes lida com incidentes em toda a organização. Este modelo é eficaz para pequenas organizações e para organizações com diversidade geográfica em termos de recursos computacionais.
- **Equipes distribuídas de resposta a incidentes:** A organização possui diversas equipes de resposta a incidentes, cada uma responsável por um determinado segmento lógico ou físico da organização. Este modelo é eficaz para grandes organizações (por exemplo, uma equipe por divisão) e para organizações com grandes recursos em locais distantes (por exemplo, uma equipe por região geográfica, uma equipe por instalação principal). Contudo, as equipes devem fazer parte de uma única entidade coordenada para que o processo de resposta a incidentes é consistente em toda a organização e as informações são compartilhadas entre as equipes. Isto é particularmente importante porque várias equipes podem ver componentes do mesmo incidente ou podem lidar com problemas semelhantes incidentes.
- **Equipe Coordenadora:** Uma equipe de resposta a incidentes fornece aconselhamento a outras equipes sem ter autoridade sobre essas equipes – por exemplo, uma equipe de todo o departamento pode ajudar equipes de agências individuais. Este modelo pode ser considerado um CSIRT para CSIRTs.

As equipes de resposta a incidentes também podem usar qualquer um dos três modelos de pessoal:

- **Funcionários:** A organização realiza todo o seu trabalho de resposta a incidentes, com recursos técnicos e apoio administrativo de empreiteiros.
- **Funcionários:** A organização realiza todo o seu trabalho de resposta a incidentes, com recursos técnicos e apoio administrativo de empreiteiros.
  - O acordo mais comum é a organização terceirizar o monitoramento 24 horas por dia, 7 dias por semana (24 horas por dia, 7 dias por semana) de sensores de detecção de intrusão, firewalls e outros dispositivos de segurança para uma empresa provedor de serviços de segurança gerenciados externos (MSSP). O MSSP identifica e analisa suspeitos atividade e relata cada incidente detectado à equipe de resposta a incidentes da organização.
  - Algumas organizações realizam trabalhos básicos de resposta a incidentes internamente e solicitam aos empreiteiros que ajudar no tratamento de incidentes, especialmente aqueles que são mais graves ou generalizados.
- **Totalmente Terceirizado:** A organização terceiriza completamente seu trabalho de resposta a incidentes, normalmente para um empreiteiro no local. Este modelo é mais provável de ser usado quando a organização precisa de um funcionário em tempo integral, equipe de resposta a incidentes no local, mas não possui funcionários qualificados e disponíveis em número suficiente. É assumido que a organização terá funcionários supervisionando e supervisionando o trabalho do terceirizado.

Comunicação entre equipes:

- Equipe – Equipe: As organizações que participam neste tipo de relacionamento são geralmente pares sem qualquer autoridade umas sobre as outras e optam por partilhar informações, reunir recursos e reutilizar conhecimentos para resolver problemas comuns para ambos os times. O tipo de informação mais frequentemente compartilhado no relacionamento entre equipes é tático e técnico (por exemplo, indicadores técnicos de compromisso, ações de remediação sugeridas), mas também pode incluir outros tipos de informações (planos, procedimentos, lições aprendidas), se conduzido como parte da fase de preparação.
- Equipe - Equipe coordenadora: Este tipo de relacionamento pode incluir algum grau de relatório exigido das organizações membros pelo órgão coordenador, bem como a expectativa de que a equipe coordenadora divulgue informações oportunas e úteis às organizações membros participantes. As equipes e as equipes de coordenação frequentemente compartilham táticas, técnicas e informações sobre ameaças, vulnerabilidades e riscos para a comunidade atendida pela equipe coordenadora. A equipe de coordenação também pode necessitar de informações específicas sobre o impacto dos incidentes, a fim de ajudar a tomar decisões sobre onde concentrar os seus recursos e atenção.
- Equipe coordenadora - Equipe coordenadora: As equipes de coordenação atuam em nome das respectivas organizações membros da comunidade para partilhar informações sobre a natureza e o âmbito dos incidentes transversais e estratégias de mitigação reutilizáveis para ajudar na resposta intercomunitária. O tipo de informação compartilhada pelas equipes de coordenação com os seus homólogos consiste frequentemente em resumos periódicos durante operações de “estado estacionário”, pontuados pela troca de informações táticas, técnicas, detalhes, planos de resposta, e impacto ou avaliação de risco de informação durante coordenação de atividades de resposta a incidentes. (Technology)

## Liderança

Profissional que atuará liderando e gerenciando as operações de segurança do SOC para garantir que as atividades sejam realizadas de maneira eficiente e eficaz.

A liderança é responsável por:

- Liderança técnica da equipe de SOC
- Orientar os times acerca das suas responsabilidades
- Motivação e supervisão dos times para alcance dos objetivos
- Identificar as necessidades de treinamento, facilitar o desenvolvimento profissional
- Assegurar que a equipe tenha os recursos necessários para desempenhar suas funções
- Monitorar se as atividades estão sendo realizadas de maneira eficiente e eficaz
- Colaborar na definição e melhoria contínua dos processos e políticas de segurança
- Implementar melhores práticas e padrões
- Coordenar respostas eficazes a incidentes críticos
- Recrutamento, treinamento e desenvolvimento de novos profissionais para o SOC
- Fornece aconselhamento técnico a gerência sobre estratégias de segurança e investimentos em tecnologias
- Planeja e participa de testes de intrusão para testar a prontidão do time e identificar melhorias
- Participa de auditorias de segurança e conformidade

Deverá ser exigido o seguinte nível de conhecimento mínimo da liderança:

- Formação em redes de computadores ou segurança da informação

- Certificações ISFS, CompTIA Security+, ISMP, CISM ou superiores
- Experiência em função anterior em segurança da informação, liderança de equipes, criação e implantação de políticas de segurança e liderança de resposta a incidentes.

### **Especialista de atenção**

O especialista de atenção será responsável por atender de forma especializada os clientes, prestando um atendimento personalizado e de qualidade, entendendo suas necessidades específicas. Analisando os requisitos de conectividade e segurança e propondo soluções adequadas. Oferecendo suporte técnico especializado, auxiliando na resolução de problemas e dúvidas. Coordenando as equipes técnicas responsáveis pela implementação das soluções propostas. Monitorando e realizando manutenção das soluções implementadas, garantindo seu correto funcionamento.

### **Service Desk**

O time do Service Desk será responsável por receber e registrar os tickets de incidentes e solicitações dos clientes, além de fornecer suporte inicial e encaminhar os tickets para a equipe especializada, quando necessário. Suas principais funções são registrar os incidentes e solicitações dos clientes de forma precisa e completa, classificar e priorizar os tickets de acordo com a gravidade e impacto nos serviços, fornecer suporte inicial aos clientes, tentando resolver os problemas de forma rápida e eficiente, encaminhar os tickets para a equipe especializada, manter os clientes informados sobre o status de seus tickets e garantir uma comunicação clara e eficiente.

### **Analista de suporte residente**

O analista de suporte residente será responsável por gerenciar o escalonamento dos tickets para o suporte da provedora de links, garantindo que os problemas sejam resolvidos dentro dos prazos acordados, ou seja, suas atribuições são:

- Receber os tickets do service desk ou da operação de segurança e escaloná-los para o suporte da provedora de links;
- Acompanhar o status dos tickets escalonados, garantindo que sejam resolvidos dentro dos prazos acordados;
- Manter o service desk ou a operação de segurança informados sobre o status dos tickets, garantindo uma comunicação clara e eficiente com o suporte da provedora de links;
- Analisar os tickets escalonados para identificar tendências e propor melhorias nos processos de reparo e escalonamento.

### **Qualidade**

O setor de qualidade será responsável por garantir a qualidade do projeto e a satisfação do cliente, gerenciando os demais times e garantindo que os processos estejam alinhados com as melhores práticas.

- Definir e manter os processos de qualidade, garantindo que sejam seguidos por todos os times envolvidos no projeto;
- Realizar inspeções e avaliações para garantir a qualidade das entregas e dos serviços prestados;
- Identificar oportunidades de melhoria nos processos e nas entregas, visando sempre a excelência e a satisfação do cliente;
- Identificar e mitigar os riscos relacionados à qualidade do projeto, garantindo a entrega dentro dos padrões estabelecidos;

- Manter uma comunicação eficiente com os demais times e com o cliente, garantindo que as expectativas sejam atendidas;
- Emitir relatórios e gerenciar indicadores de desempenho do serviço.

### **Suporte da operadora**

O setor de suporte da operadora de links será responsável por fornecer suporte técnico especializado para resolver problemas relacionados à conectividade e garantir o funcionamento adequado dos links de comunicação. O suporte deverá:

- Receber e registrar os incidentes relatados pelo técnico de reparos relacionados à conectividade dos links;
- Realizar diagnósticos para identificar a causa dos problemas e implementar soluções ou escalar para o time de campo;
- Monitorar continuamente a conectividade e o desempenho dos links para identificar e resolver problemas antes que impactem os clientes;
- Realizar manutenções preventivas nos links para garantir seu funcionamento adequado;
- Manter o técnico de reparos informado sobre o status dos tickets.

### **Proteção de DNS**

Uma solução de proteção de DNS (Domain Name System) é uma medida de segurança projetada para proteger a infraestrutura de DNS de uma organização contra ameaças cibernéticas e garantir a integridade e disponibilidade do serviço de resolução de nomes.

Principais características da solução:

- Filtragem de conteúdo: Bloqueia o acesso a sites maliciosos ou inadequados com base em categorias predefinidas ou listas negras;
- Proteção contra malware e phishing: Identifica e bloqueia conexões a domínios associados a malware, phishing, e outras ameaças cibernéticas;
- Mitigação de Ataques DDoS: Protege contra ataques de negação de serviço direcionados aos servidores DNS, que visam sobrecarregar e tirar o serviço do ar;
- Segurança e Integridade: Utiliza tecnologias como DNSSEC (DNS Security Extensions) para autenticar respostas DNS e proteger contra ataques de envenenamento de cache e spoofing;
- Monitoramento e Relatórios: Fornece visibilidade sobre o tráfego DNS, permitindo a detecção de atividades suspeitas e a geração de relatórios para análise e conformidade;
- Políticas de Acesso: Permite a definição de políticas de acesso para controlar quem pode acessar determinados recursos na rede.

### **Guarda de LOGs e Relatoria**

Sistema utilizado para coletar, armazenar, gerenciar e analisar logs de eventos e atividades gerados por diferentes sistemas, dispositivos e aplicativos dentro de uma organização. Os logs são registros detalhados de ações que ocorreram em um sistema, como acessos a dados, mudanças de configuração, atividades de usuários, eventos de rede e muito mais.

Principais características da solução:

- **Coleta de Logs:** Captura logs de várias fontes, incluindo servidores, firewalls, sistemas operacionais, aplicativos, dispositivos de rede, entre outros;
- **Armazenamento Seguro:** Armazena logs de forma segura e protegida, garantindo que os dados não sejam alterados ou corrompidos. Isso é essencial para auditorias e investigações de segurança;
- **Retenção e Conformidade:** Mantém os logs por um período de tempo especificado para atender a requisitos de conformidade e regulamentações legais, como a LGPD, GDPR e outros;
- **Análise e Correlação:** Permite a análise dos logs para identificar padrões, anomalias e comportamentos suspeitos. Ferramentas avançadas podem correlacionar eventos de diferentes fontes para detectar incidentes de segurança;
- **Relatórios e Visualização:** Gera relatórios detalhados e visualizações para ajudar na interpretação dos dados, facilitar auditorias e apoiar a tomada de decisões. Esses relatórios podem ser personalizados de acordo com as necessidades da organização.

### **Operação de rede**

Operação proativa para dados e voz na Nova Rede, sob a coordenação do Centro Integrado de Inteligência e Segurança Cibernética. A operação funciona 24/7, incluindo feriados, e envolve o tratamento de tickets, manutenção dos indicadores de recuperação e tempo entre falhas, fornecimento de peças e reparos, auditorias e monitoramento de serviços. A contratada deve realizar backup e recuperação de configurações, testar serviços reparados e manter o padrão de qualidade, além de fornecer ferramentas de gerenciamento e suporte técnico. A ativação e implantação de novos serviços serão realizadas em horário comercial, com equipes dedicadas para coordenação e integração.

### **Coordenação**

O serviço de Coordenação do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede funcionará em horário comercial, com possíveis atuações fora desse horário conforme solicitado pela ATI. As principais atividades incluem apresentar relatórios periódicos sobre o desempenho da rede e apoiar a integração das equipes especializadas com a ATI. O coordenador também será responsável pelo planejamento e gestão das equipes, cumprimento dos fluxos de trabalho, validação de indicadores de desempenho, acompanhamento de eventos, solicitações e mudanças, além de garantir a qualidade dos serviços. Outras funções incluem manter o catálogo de serviços atualizado, supervisionar a instalação e manutenção das plataformas, monitorar backups e fornecer suporte técnico contínuo às equipes e sistemas.

### **Gerenciamento do projeto**

O serviço de gerenciamento do projeto envolve a gestão contínua do portfólio e subprojetos da Nova Rede, incluindo a realização de workshops, consolidação de portfólio, implantação de ferramentas de planejamento e acompanhamento, e o desenvolvimento de cronogramas detalhados. As principais atividades incluem alocação e garantia de recursos, monitoramento do progresso, controle de custos e orçamento, além de comunicação eficaz entre as partes interessadas. O gerente será responsável por identificar riscos, implementar estratégias de mitigação, assegurar que as entregas atendam aos padrões de qualidade, preparar relatórios de status, e documentar lições aprendidas.

### **Análise Forense**

O serviço de Análise Forense para incidentes cibernéticos envolve a identificação, coleta, análise e preservação de evidências digitais de forma rigorosa e legalmente aceitável, apoiando investigações de segurança e possíveis ações legais. As atividades incluem a identificação e preservação de sistemas afetados, uso de ferramentas forenses para coleta e análise de dados, reconstituição de incidentes, e análise de malware. O trabalho resulta em relatórios téc-

nicos detalhados, recomendações de mitigação de vulnerabilidades e documentação legal. Requer profissionais certificados, experiência comprovada e o uso de ferramentas forenses reconhecidas.

### **Evolução da maturidade em segurança da informação**

O serviço de evolução da maturidade em segurança da informação visa implementar e aprimorar a segurança cibernética nos órgãos do Poder Executivo de Pernambuco, usando normas e frameworks como MITRE ATT&CK, NIST, ISO/IEC 27001 e CMMI. O processo será estruturado em cinco níveis de maturidade, desde a implementação inicial de políticas de segurança até uma gestão otimizada e proativa. Cada nível foca em aspectos como segmentação de redes, controle de acesso, detecção de ameaças e resposta a incidentes. O projeto inclui avaliação de conformidade, riscos cibernéticos, processos de segurança e tecnologias, além de propor melhorias contínuas em maturidade e gerenciamento de segurança.

### **SASE (Secure Access Service Edge)**

SASE (Secure Access Service Edge) é uma tecnologia de proteção em nuvem com foco em usuários móveis, remotos e distribuídos com acesso direto à Internet, sua principal aplicabilidade é para ambientes de trabalho remoto, usuários com elevada mobilidade e consumo significativo de aplicações em nuvem. No contexto deste projeto verifica-se pouca aderência desta tecnologia, pois os serviços são disponibilizados e convergem em cada PCS (Ponto Conectado Seguro) respectivamente com toda a base de usuários acessando os serviços digitais de maneira centralizada em cada site.

Soluções de SASE, normalmente implementam licenciamento por usuário e largura de banda consumida, enquanto em soluções de conectividade segura o dispositivo é licenciado de maneira única e integral independentemente da quantidade de usuários e/ou largura de banda consumida, diminuindo portanto os custos de aquisição e de propriedade ao longo do ciclo de vida do contrato.

Uma vez que existem diversas soluções e plataformas no mercado que fornecem de maneira integrada recursos avançados de conectividade e segurança, não se faz necessário incorrer em custos adicionais para executar estas funções em nuvem sendo que as mesmas podem ser implementadas diretamente no próprio dispositivo de conectividade, consolidando assim recursos de SD-WAN com Next-Generation firewall no mesmo hardware, com foco em otimização de custos de propriedade e redução de custos operacionais, em plena sintonia com o princípio de economicidade.

Um dos princípios básicos da cybersegurança é que os controles e a visibilidade, sempre que possível, sejam implementados o mais próximo da origem, em soluções de SASE todo o tráfego é transferido para um ambiente de análise em nuvem e a partir dele são aplicados os controles e filtros específicos para finalmente o tráfego fluir para a Internet, introduzindo portanto um estágio adicional e desnecessário quando toda a análise e controle poderia ser feito diretamente, em estágio único, por uma solução local de proteção no PCS (Ponto Conectado Seguro).

As soluções de SASE possuem como foco principal a análise e controle de tráfego externo direcionado à Internet, não implementam controle e visibilidade do tráfego local interno (LAN/WIFI), tratando-se de um recurso fundamental dentro do PCS (Ponto Conectado Seguro) devido ao volume e tipo de fluxos entre serviços e sistemas internos, comunicação direta entre dispositivos dentro do PCS, dentre outros, sendo necessário portanto uma solução integrada que consolide a análise tanto de fluxo interno quanto externo.

As soluções de SASE possuem como foco principal a análise e controle de tráfego externo direcionado à Internet, não implementam controle e visibilidade do tráfego local interno (ambiente LAN/WIFI), tratando-se de um recurso fundamental dentro do PCS (Ponto Conectado Seguro) devido ao volume e tipo de fluxos entre serviços e sistemas internos, assim como diversos dispositivos, a saber: câmeras, telefones, impressoras, etc. para os quais não há necessidade de enviar este tráfego para análise em nuvem que inclusive pode impactar no funcionamento adequado dos mesmos, sendo necessário, portanto, uma solução integrada que consolide a análise tanto do fluxo local quanto externo.

Com base no levantamento de mercado, a tabela a seguir apresenta as soluções estudadas, acompanhadas das justificativas técnicas e econômicas que fundamentam a escolha final. As opções avaliadas levam em conta a vantagem econômica, os ganhos em eficiência administrativa, as experiências de contratações similares em outros órgãos, e a adoção de tecnologias inovadoras que possam aprimorar a eficiência, segurança e transparência dos serviços prestados. Esta tabela oferece uma visão completa das alternativas, facilitando a comparação e apoiando a tomada de decisão sobre a solução mais apropriada para o projeto da nova rede corporativa.

Id	Descrição da solução (ou cenário)
1	<p>Solução de Rede Corporativa com Segurança, banda larga redundante e serviços de voz em três lotes.</p> <p>Modelo de contratação composto por links banda larga redundantes, solução de segurança centralizada com equipamento de última milha, solução de rede sem fio, solução de detecção e resposta a dispositivos finais, serviços de voz, contact center, comunicação unificada, monitoramento das operações de segurança, gestão de qualidade e uso dos serviços, processos, pessoas e tecnologias de segurança providos por uma única empresa ou consórcio. Além destes, haverão também itens de serviço complementares, compostos por links multitecnologias redundantes e conectividade de Datacenter em lotes distintos.</p> <p>A contratação dividida em três lotes — <b>Segurança + Conectividade Redundante + Voz, Conectividade entre Datacenters, e Avaliação e Mitigação de Riscos Cibernéticos</b> — oferece vantagens significativas, como a atração de fornecedores especializados, a redução de riscos para o Governo com maior previsibilidade dos serviços inter-relacionados e a simplificação da gestão contratual. Essa abordagem permite maior eficiência, flexibilidade e transparência, além de garantir que cada área seja executada por empresas com expertise dedicada, aumentando a qualidade e a competitividade das soluções propostas.</p>
2	<p>Solução de Rede Corporativa em modelo de contratação dos itens de serviço por lotes totalmente distintos.</p> <p>Os serviços podem ser oferecidos por empresas distintas com perfis específicos conforme os itens contidos no termo de referência. Os itens consistem em links multitecnologias, solução de segurança centralizada com equipamento de última milha, solução de rede sem fio, serviços de voz, contact center, comunicação unificada, monitoramento das operações de segurança e uso dos serviços e telefonia fixa.</p> <p>As vantagens da contratação em lotes totalmente separados são: prestação de serviço com empresas e profissionais especializados com foco em um único item de serviço.</p>
3	<p>Solução de Rede Corporativa em modelo de contratação de acesso dedicado com ponto único de acesso à Internet.</p> <p>Os itens de serviço consistem em equipamento de segurança última milha com link dedicado redundante e solução de rede sem fio convergindo para os pontos de presença básico e principal, infraestrutura de segurança de rede centralizada, serviços de voz, contact center e comunicação unificada fornecidos por uma única empresa ou consórcio.</p> <p>As vantagens dos itens de serviço acima são: operação centralizada em todos os itens de serviços contratados, resolução de incidentes por um único ponto de comunicação com a empresa ou consórcio.</p>
4	<p>Solução de Rede Corporativa com Segurança em Modelo de Contratação por Empresa Única ou Consórcio com SASE Integrado:</p>

Esta solução envolve a contratação de uma única empresa ou consórcio para fornecer uma infraestrutura integrada que abrange links de banda larga redundantes, uma solução de segurança baseada em SASE (Secure Access Service Edge) para proteger o tráfego da rede de maneira centralizada e na nuvem, rede sem fio, serviços de voz, contact center, comunicação unificada, detecção e resposta a ameaças em dispositivos finais, monitoramento contínuo das operações de segurança, e gestão da qualidade e do uso dos serviços. Além disso, inclui serviços complementares, como links redundantes e comunicação de voz/telefonia, organizados em lotes distintos.

As principais vantagens desse modelo incluem a simplificação do gerenciamento e da comunicação, com um ponto único de contato para todos os envolvidos no consórcio. A utilização de SASE proporciona uma segurança mais flexível e escalável, permitindo que as políticas de segurança sejam aplicadas de forma consistente em qualquer local ou dispositivo. Além disso, a centralização da segurança na nuvem facilita o acompanhamento e a resolução de incidentes, garantindo que todos os itens de serviço especificados no termo de referência sejam geridos eficientemente por uma única entidade.

#### Fundamentação:

- Art. 18º, § 1º, inciso V, da Lei nº 14.133, de 01 de abril de 2021;
- Art. 8º, inciso IV, do Decreto Estadual nº 53.384, de 22 de agosto de 2022;
- Atlassian. (s.d.a). Fonte: <https://www.atlassian.com/br/itsm/it-asset-management>;
- Atlassian. (s.d.b). Fonte: <https://www.atlassian.com/br/itsm>;
- Atlassian. (01 de Janeiro de 2024). Atlassian. Acesso em Janeiro de 2024, disponível em Atlassian: <https://www.atlassian.com/br/itsm/it-asset-management>;
- Brasiline. (08 de Outubro de 2021). Fonte: <https://brasiline.com.br/blog/compreendendo-a-diferenca-entre-edr-siem-soar-e-xdr/>;
- Castilho, M. (2015). Continuidade dos Serviços de TI. Americana, SP. Acesso em 31 de Janeiro de 2024, disponível em [https://ric.cps.sp.gov.br/bitstream/123456789/887/1/20152S\\_REVERSIMateusCastilho\\_CD2501.pdf](https://ric.cps.sp.gov.br/bitstream/123456789/887/1/20152S_REVERSIMateusCastilho_CD2501.pdf);
- CheckPoint. (s.d.). Fonte: <https://www.checkpoint.com/downloads/products/horizon-mdr-mpr-solution-brief.pdf>;
- CrowdStrike. (s.d.). Fonte: <https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/managed-xdr-mxdr/>;
- Crowdstrike. (28 de Novembro de 2023). Crowdstrike. Fonte: Crowdstrike: <https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/managed-xdr-mxdr/>;
- CYBERSECURITY & INFRASTRUCTURE. (2023). CISA and NSA Release Joint Guidance on Defending Continuous Integration/Continuous Delivery (CI/CD) Environments. Fonte: <https://www.cisa.gov/news-events/alerts/2023/06/28/cisa-and-nsa-release-joint-guidance-defending-continuous-integrationcontinuous-delivery-cicd>;
- Deloitte. (s.d.). Fonte: <https://www2.deloitte.com/br/pt/pages/risk/solutions/mxdr-seguranca-cibernetica.html>;
- DQS Global. (25 de Outubro de 2022). DQS Global. Acesso em 31 de Janeiro de 2024, disponível em <https://www.dqsglobal.com/pt-br/academy/blog/seguranca-da-informacao-e-gestao-da-qualidade>;

- EcoTrust. (24 de Maio de 2023). EcoTrust. Fonte: EcoTrust: <https://blog.ecotrust.io/gerenciamento-de-vulnerabilidade/>;
- G2. (2024a). G2. Fonte: G2: <https://www.g2.com/compare/demisto-vs-ibm-security-qradar-soar-vs-splunk-soar-security-orchestration-automation-and-response-vs-swimlane>;
- G2. (2024b). G2. Fonte: G2: <https://www.g2.com/compare/openvas-vs-insightvm-nexpose-vs-tenable-nessus>;
- G2. (2024c). G2 Compare. Fonte: G2 Compare: <https://www.g2.com/compare/crowdstrike-falcon-endpoint-protection-platform-vs-sentinelone-singularity-vs-sophos-intercept-x-next-gen-endpoint-vs-microsoft-defender-for-endpoint>;
- G2 Compare. (2024a). Fonte: <https://www.g2.com/compare/crowdstrike-falcon-endpoint-protection-platform-vs-sentinelone-singularity-vs-sophos-intercept-x-next-gen-endpoint-vs-microsoft-defender-for-endpoint>;
- G2 Compare. (2024b). Fonte: <https://www.g2.com/compare/demisto-vs-ibm-security-qradar-soar-vs-splunk-soar-security-orchestration-automation-and-response-vs-swimlane>;
- InformaTI. (2024). Fonte: <https://informati.com.br/qual-a-importancia-do-backup/>;
- InformaTI. (01 de Janeiro de 2024). InformaTI Soluções em TI. Fonte: InformaTI: <https://informati.com.br/qual-a-importancia-do-backup/>;
- InterOp. (21 de Novembro de 2022). Acesso em 31 de Janeiro de 2024, disponível em InterOp: [https://www.interop.com.br/blog/processos-itol-da-plataforma-4biz/#15\\_Gerenciamento\\_de\\_Continuidade\\_de\\_Servicos\\_de\\_TI](https://www.interop.com.br/blog/processos-itol-da-plataforma-4biz/#15_Gerenciamento_de_Continuidade_de_Servicos_de_TI);
- Kavlac, M. (21 de Junho de 2023). Psycurity: Awareness as a Protection. Acesso em 23 de Janeiro de 2024, disponível em Site da Psycurity: <https://psycurity.com.br/5-passos-para-realizar-uma-campanha-de-seguranca-da-informacao/>;
- NET CONSULTING. (s.d.). A Importância da Educação em Segurança Cibernética. Fonte: <https://netconsulting.com.br/a-importancia-da-educacao-em-seguranca-cibernetica/>;
- NIST. (s.d.). Computer Security Incident Handling Guide.;
- NovaRed. (s.d.). Fonte: <https://novared.com.br/autenticacao-de-multiplos-fatores-a-aliada-da-protecao-de-dados-no-teletrabalho/>;
- NovaRed. (01 de Janeiro de 2024). NovaRed. Fonte: NovaRed: <https://novared.com.br/autenticacao-de-multiplos-fatores-a-aliada-da-protecao-de-dados-no-teletrabalho/>;
- Radack, S. (s.d.). CONTINUOUS MONITORING OF INFORMATION SECURITY: AN ESSENTIAL COMPONENT OF RISK MANAGEMENT. National Institute of Standards and Technology, 7. Fonte: [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=909992](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909992);
- Red Hat. (5 de Maio de 2023). Red Hat. Acesso em Janeiro de 2024, disponível em Red Hat: <https://www.redhat.com/pt-br/topics/security/what-is-vulnerability-management>;
- Service Now. (01 de Janeiro de 2024). ServiceNow. Acesso em 23 de Janeiro de 2024, disponível em ServiceNow: <https://www.servicenow.com/br/products/governance-risk-and-compliance/what-is-compliance-management.html>;
- SITE 1. (s.d.a). Fonte: <https://network-king.net/pt-pt/dez-principais-ferramentas-de-gerenciamento-de-ativos-de-ti/>;

- SITE 1. (20 de Janeiro de 2024). Fonte: <https://www.guru99.com/pt/best-itsm-tools.html>;
- SITE 1. (s.d.b). SITE 1. Fonte: <https://cecyber.com/scanner-de-vulnerabilidades-conheca-as-melhores-ferramentas/>;
- SITE 2. (s.d.a). Fonte: <https://www.guru99.com/pt/it-asset-management-software.html>;
- SITE 2. (s.d.b). Fonte: <https://www.getapp.com.br/directory/292/it-service-management-itsm/software?sort=popularity>;
- SITE 2. (s.d.c). Fonte: <https://rootsec.com.br/5-scanners-de-vulnerabilidade-de-rede-gratuitos/>;
- SITE 3. (s.d.a). Fonte: <https://www.linkedin.com/pulse/quais-sofware-de-ti-uma-empresa-precisa-para-funcionar/?originalSubdomain=pt>;
- SITE 3. (s.d.b). Fonte: <https://www.blog.vibetecnologia.com/ferramenta-itsm>;
- SITE 3. (s.d.c). Fonte: <https://blog.neotel.com.br/sem-categoria/5-scanners-de-vulnerabilidade-gratuitos-que-voce-deve-conferir/>;
- SITE 4. (s.d.a). Fonte: <https://itforum.com.br/noticias/top-12-ferramentas-de-gerenciamento-de-servicos-de-ti/>;
- SITE 4. (s.d.b). Fonte: <https://minutodaseguranca.blog.br/as-10-melhores-ferramentas-de-verificacao-de-vulnerabilidades-para-testes-de-penetracao-2019/>;
- TrendMicro. (s.d.). Fonte: <https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-features-and-benefit#GUID-31DA0A64-A5AD-438C-A333-0CC15C252BEE>;
- Wikipedia. (06 de Janeiro de 2024). ISO 22301. Acesso em 31 de Janeiro de 2024, disponível em [https://en.wikipedia.org/wiki/ISO\\_22301](https://en.wikipedia.org/wiki/ISO_22301);
- Zendesk. (20 de Abril de 2023). Blog da Zendesk. Fonte: <https://www.zendesk.com.br/blog/gerenciamento-de-incidente-til/#:~:text=Tamb%C3%A9m%20chamado%20de%20gest%C3%A3o%20de,do%20servi%C3%A7o%20n%C3%A3o%20seja%20prejudicada>.

## 7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

A definição das quantidades a serem contratadas para a implementação dos serviços de segurança cibernética, conectividade, comunicação de voz e unificada, contact center, bem como dos Serviços de Operação de Segurança (SOC) e de Operação de Rede (NOC), foi elaborada considerando a necessidade de garantir a plena operação e proteção da segurança cibernética do Governo do Estado de Pernambuco. A contratação incluirá, de forma integral, a implantação, operação, manutenção e suporte de todos os serviços, juntamente com o fornecimento dos equipamentos necessários, que deverão ser retirados ao término do contrato.

### Premissas Fundamentais

As premissas que fundamentam as estimativas dos quantitativos de serviços foram definidas considerando os critérios abaixo:

1. **Necessidade Institucional:** A análise dos serviços atuais e das lacunas identificadas no ambiente de TI da instituição, considerando a expansão e o fortalecimento das operações de segurança cibernética e a garantia de alta disponibilidade dos serviços de rede com seus serviços suportados (voz e wifi, por exemplo).

2. **Capacidade Instalada:** Considerando que os equipamentos e infraestruturas do contrato vigente de telemática serão totalmente devolvidos à Contratada ao fim do contrato, a nova contratação deve prever a instalação de novos equipamentos de telemática e segurança de redes. Dessa forma, os serviços contratados devem incluir todas as atividades necessárias para a configuração, instalação, e adaptação da infraestrutura existente.
3. **Serviços Complementares:** A contratação deverá prever a capacitação dos colaboradores para operar e manter as novas soluções implementadas, além da aquisição de licenças de software necessárias para o pleno funcionamento dos serviços de SOC e NOC, provisionamento de equipamentos com todos os componentes necessários, sem dependência com a infraestrutura atual, além de integrar todos os serviços como parte do escopo contratual.
4. **Evolução Tecnológica e Escalabilidade:** Foi considerada a necessidade de escalabilidade das soluções contratadas, permitindo futuras expansões ou adaptações, conforme a evolução das necessidades institucionais e o avanço tecnológico.
5. **Fornecimento Completo de Infraestrutura:** Não há capacidade instalada na infraestrutura atual da instituição para suportar as novas demandas de segurança cibernética, conectividade e comunicação de voz. Portanto, todos os equipamentos, licenças e recursos necessários para a operação dos serviços deverão ser fornecidos pelo contratante, durante o período contratual. Esses equipamentos incluirão, mas não se limitarão a servidores, dispositivos de segurança, roteadores, switches, centrais telefônicas, aparelhos de voz, access points e qualquer outro equipamento crítico para a operação dos serviços de SOC e NOC.
6. **Serviços Especializados e Suporte Integral:** Além do fornecimento da infraestrutura, o contrato incluirá serviços especializados de instalação, configuração, operação contínua, manutenção preventiva e corretiva, bem como suporte técnico dedicado. Esses serviços garantirão que os sistemas operem com alta disponibilidade e segurança, ao longo do contrato e respeitando aos parâmetros de Níveis Mínimo de Serviço definidos.
7. **Retirada de Equipamentos ao Término do Contrato:** Ao final do período contratual, todos os equipamentos fornecidos para a execução dos serviços deverão ser removidos, sem qualquer custo adicional para o Governo do Estado de Pernambuco, sem gerar passivos futuros.

## Cálculo dos Quantitativos

A estimativa dos quantitativos baseia-se em uma análise detalhada das demandas previstas e na correlação direta com o volume de serviços prestados pelo contrato atual acrescentando o que se espera contratar e a dependência dos serviços contratados para a operação dos sistemas de TI. Para cada serviço identificado, foram calculadas as quantidades necessárias a partir de:

Para cada serviço identificado, foram calculadas as quantidades necessárias com base nos seguintes eixos metodológicos:

- **Estudos de Demanda:** Avaliação de relatórios históricos de consumo, incidentes e desempenho dos serviços, bem como da taxa de utilização dos recursos de rede e segurança, para dimensionamento adequado dos componentes de SOC, NOC, conectividade e segurança de rede.
- **Análise de Capacidade e Dependência Operacional:** Consideração da interdependência entre serviços — por exemplo, a relação direta entre o número de links, pontos de acesso e elementos de segurança — de modo a assegurar compatibilidade técnica e continuidade operacional entre os diversos módulos do projeto.
- **Estatísticas e Benchmarks de Mercado:** Utilização de dados comparativos de mercado e estudos de referência em instituições públicas e privadas de porte similar, ajustados à realidade tecnológica e orçamentária do Estado de Pernambuco.

Os quantitativos resultantes foram definidos com base em métodos consolidados de dimensionamento de serviços de TI e telemática, observando boas práticas de engenharia de tráfego, segurança da informação e gestão de infraestrutura, de forma a garantir consistência técnica, viabilidade financeira e aderência às diretrizes estratégicas da Nova Rede Corporativa.

### Justificativas dos Quantitativos

Os quantitativos estimados para a Nova Rede Corporativa foram definidos com base nas necessidades identificadas no ambiente de Tecnologia da Informação do Governo do Estado de Pernambuco e nas exigências regulatórias aplicáveis. A definição resultou de uma consolidação técnico-analítica, que combinou dados operacionais, levantamentos de campo, pesquisas junto aos órgãos estaduais, bases contratuais vigentes e projeções orçamentárias revisadas, com o objetivo de assegurar um dimensionamento realista, eficiente e sustentável dos serviços previstos.

O estudo contemplou os eixos de segurança cibernética, conectividade, telefonia fixa (voz), rede sem fio (Wi-Fi), além das operações de SOC e NOC, assegurando coerência técnica entre os diversos componentes da infraestrutura.

Os serviços de instalação, configuração, capacitação e licenciamento de software foram tratados como partes integrantes e indissociáveis do escopo, de modo a garantir entrega completa, funcionamento pleno e aderência às restrições financeiras do projeto.

A metodologia adotada baseou-se em múltiplas fontes oficiais e documentais, cada uma desempenhando papel específico na construção da base técnica e quantitativa do ETP, conforme descrito a seguir:

1. **“Informação 3 – Resumo dos Processos” (SEI nº [72965319](#))**

Documento que consolida os contratos vigentes e planejados referentes à Rede de Telemática do Estado, com foco no projeto da Nova Rede Corporativa. Após a apresentação da estimativa orçamentária global de R\$ 2,45 bilhões para 60 meses de contrato, identificou-se a necessidade de readequação do escopo físico e financeiro para compatibilização com os limites de execução orçamentária considerados sustentáveis para o Estado. Este documento foi utilizado para balizamento da capacidade orçamentária e consequente ajuste quantitativo das soluções.

2. **“Relatório de Pesquisa de Demanda da Nova Rede Corporativa” (SEI nº [69510789](#))** Pesquisa conduzida com 35 órgãos estaduais participantes (37,6% do total de 93), mediante levantamento direto junto aos Gestores de Telemática, com o objetivo de dimensionar as necessidades de conectividade, segurança e serviços de rede.

A coleta foi realizada entre dezembro/2024 e fevereiro/2025, incluindo reuniões de esclarecimento técnico e reenvio da pesquisa após baixo índice inicial de resposta. Para compensar a amostra parcial, aplicou-se extrapolação estatística proporcional, estimando a demanda total com base na representatividade da amostra. Em casos específicos, essa extrapolação foi ajustada por métodos estatísticos complementares ou adaptada conforme as restrições orçamentárias estabelecidas para o projeto.

As informações consolidadas encontram-se detalhadas no documento “Pesquisa de Demanda” (SEI nº [69186852](#)), que constitui o principal insumo de projeção de demanda para os quantitativos do projeto.

3. **“Mapa de Preços” (SEI nº [69512608](#))**

Base utilizada como referência de valores unitários atualizados, representando o levantamento mais recente de custos de mercado à época da revisão do ETP, assegurando aderência às condições reais de contratação e ao princípio da economicidade.

4. **“Planilha Base de Links de Acesso - 231025” (SEI nº [76072589](#))**

Extraída do Portal de Relatórios (<https://portalderelatorios.peconectado.pe.gov.br>), contém a base atuali-

zada dos links de acesso instalados no contrato PE-Conectado II, discriminando velocidades, tipologia de acesso e cobertura, incluindo escolas indígenas e unidades especiais, servindo como referência primária para o redimensionamento do escopo de conectividade.

5. **“Relatório Tipos de Acesso VSAT - PE-Conectado II”** (SEI nº [69187260](#))  
Registra 220 localidades atendidas por acessos satelitais até maio/2025, sendo essencial para o dimensionamento da conectividade em áreas remotas e de difícil acesso, como regiões rurais, indígenas e quilombolas.

6. **“Planilha Links Temporários – ADT – Contrato PE-Conectado II”** (SEI nº [76075149](#))  
Apresenta o histórico de 19 circuitos temporários contratados entre 2020 e 2025, permitindo a identificação de demandas sazonais e contingenciais que serviram de referência para projeções de reserva técnica.

7. **“Planilha Serviço de Ponto de Voz Fixo – 29/10/2025”** (SEI nº [76077388](#))

Apresenta extração da base de ativos realizada em 29/10/2025, por meio do Portal de Relatórios da ATI (<https://portalderelatorios.peconectado.pe.gov.br>).

O levantamento registrou **20.473 PVFs** de serviços ativos, onde esses dados serviram como base comparativa para a revisão e consolidação dos quantitativos finais de pontos de voz a serem contratados.

8. **“Relatório do Quantitativo do Serviço 0800”** (SEI nº [69528405](#))  
Produzido a partir do “Relatório de Tarifação de Consumo do Serviço 0800” (SEI nº [68621724](#)), com dados consolidados entre dezembro/2023 e abril/2025. Fundamentou as projeções de chamadas médias e picos de utilização para definição da capacidade contratual do serviço.

9. **“Relatório de Dispositivos para o NAC”** (SEI nº [69507098](#))  
Documento técnico elaborado com base no protocolo SOL 786517 (SEI nº [69190154](#)), apresentando contagem real de dispositivos por localidade para implementação do NAC (Network Access Control). A coleta de dados, realizada entre 30/01/2025 e 05/02/2025, forneceu a base quantitativa para o dimensionamento das licenças de controle de acesso.

Além das referências acima, destaca-se que novas bases e revisões de dados foram extraídas para atualização dos quantitativos, considerando o lapso temporal entre a elaboração inicial e a versão atual deste estudo, bem como a necessidade de adequação às diretrizes orçamentárias vigentes. Em razão disso, foram tornados sem efeito os artefatos e relatórios preliminares que apresentavam descompasso com as informações mais recentes ou com o escopo revisado, tais como:

- Relatório de Acessos Instalados (SEI nº [69508491](#));
- Relatório Tipos de Acesso VSAT (SEI nº [69187260](#));
- Relatório de Acessos PE-Conectado II – 100 Mbps ou Maior (SEI nº [69187334](#));
- Relatório de Acessos Instalados – PE-Conectado II em 22/05/2025 (SEI nº [69187364](#));
- Relatório Serviços de Wi-Fi PE-Conectado II – Switch/AP Planta (SEI nº [69187033](#));
- Relatório de Dimensionamento de Switch Wi-Fi (SEI nº [69539640](#));
- Relatório Tarifação Serviço 0800 – dez/23 a abr/25 (SEI nº [73831138](#));
- Pesquisa de Demanda (SEI nº [67064769](#)) – versão substituída pelo levantamento atualizado de 2025.

Isto posto, apresenta-se a seguir a tabela com os quantitativos estimados, contendo os códigos e-Fisco, a descrição dos itens, as quantidades e as respectivas unidades de medida, organizadas conforme os Adendos do Termo de Referência. Após a tabela, serão apresentadas as justificativas das estimativas correspondentes.

## 1) ADENDO III - SEGURANÇA DE REDE LOCAL

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598669-9	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1	1759	Unidade
2	598670-2	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2	1299	Unidade
3	598672-9	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço	193	Unidade
4	598675-3	Solução para gerenciamento de acessos à rede local - NAC	24427	Unidade

### 1.1 Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1:

O dimensionamento deste serviço foi definido de forma proporcional à quantidade de Pontos Conectado Seguro (PCS) atendidos por links de acesso LAP Tipo 1, considerando a possibilidade de implantação em redundância por site, quando solicitado.

Conforme o mapeamento consolidado da rede estadual, a base total compreende 2.865 sites, dos quais 1.759 possuem links LAP Tipo 1 e 1.106 possuem links LAP Tipo 2.

Dessa forma, o quantitativo do serviço Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 foi estabelecido em 1.759 unidades, assegurando a cobertura integral de todos os pontos classificados como LAP Tipo 1 e suas eventuais redundâncias por localidade, se necessário.

### 1.2 Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2:

De forma análoga, o dimensionamento da Solução de Segurança de Última Milha – Tipo 2 foi diretamente correlacionado à quantidade de sites com links LAP Tipo 2, totalizando 1.106 unidades, conforme as definições do Adendo V – Serviço de Conectividade de Rede Local.

Adicionalmente, foram consideradas 193 localidades com necessidade de configuração em alta disponibilidade (HA – High Availability), implicando a implantação de um equipamento UTM adicional por localidade para garantir resiliência e continuidade operacional.

Assim, o total consolidado para o serviço Tipo 2 é de **1.299 unidades**, correspondendo à soma das 1.106 localidades LAP Tipo 2 e das 193 unidades adicionais destinadas à configuração HA.

### 1.3 Serviço de configuração de high availability (HA)

O dimensionamento deste serviço foi estabelecido em 193 localidades, abrangendo:

- 93 sedes de órgãos estaduais, conforme Despacho 18 (SEI nº [67440382](#));
- 70 sites da Secretaria Estadual de Saúde (SES), conforme identificado na Pesquisa de Demanda da Nova Rede Corporativa (SEI nº [69510789](#));
- 25 delegacias especiais, e
- 5 localidades vinculadas ao Gabinete do Governador (GABGOV).

A seleção dessas localidades considerou criticidade operacional, necessidade de continuidade de serviços e requisitos de segurança e disponibilidade.

### 1.4 Solução para gerenciamento de acessos à rede local - NAC

O dimensionamento deste serviço foi definido exclusivamente para as 193 localidades com configuração HA, por se tratarem de ambientes que exigem controle de acesso mais avançado.

Com base no Relatório de Dispositivos ATI (SEI nº [69190154](#)), foram identificados 21.010 dispositivos em 166 localidades. Aplicando-se extrapolação proporcional à totalidade das 193 localidades, projetou-se um total estimado de 24.427 dispositivos a serem contemplados pela solução de Network Access Control (NAC), assegurando a cobertura de todos os dispositivos corporativos e institucionais dessas localidades.

## 2) ADENDO IV - SERVIÇO DE REDE SEM FIO

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598692-3	Serviço de Rede Sem Fio Interno com Segurança	10042	Unidade
2	598693-1	Serviço de Rede Sem Fio Externo com Segurança	500	Unidade
3	598694-0	Serviço de Rede Sem Fio Temporário com Segurança	10	Unidade
4	602034-8	Serviço de fornecimento e implantação de Switch	591	Unidade

### 2.1 Serviço de Rede Sem Fio Interno com Segurança

O dimensionamento do Serviço de Rede Sem Fio Interno com Segurança foi realizado com base em critérios técnicos, estatísticos e orçamentários, considerando a realidade operacional da rede governamental e as diretrizes de racionalização de custos definidas no documento “Informação 3 – Resumo dos Processos” (SEI nº [72965319](#)).

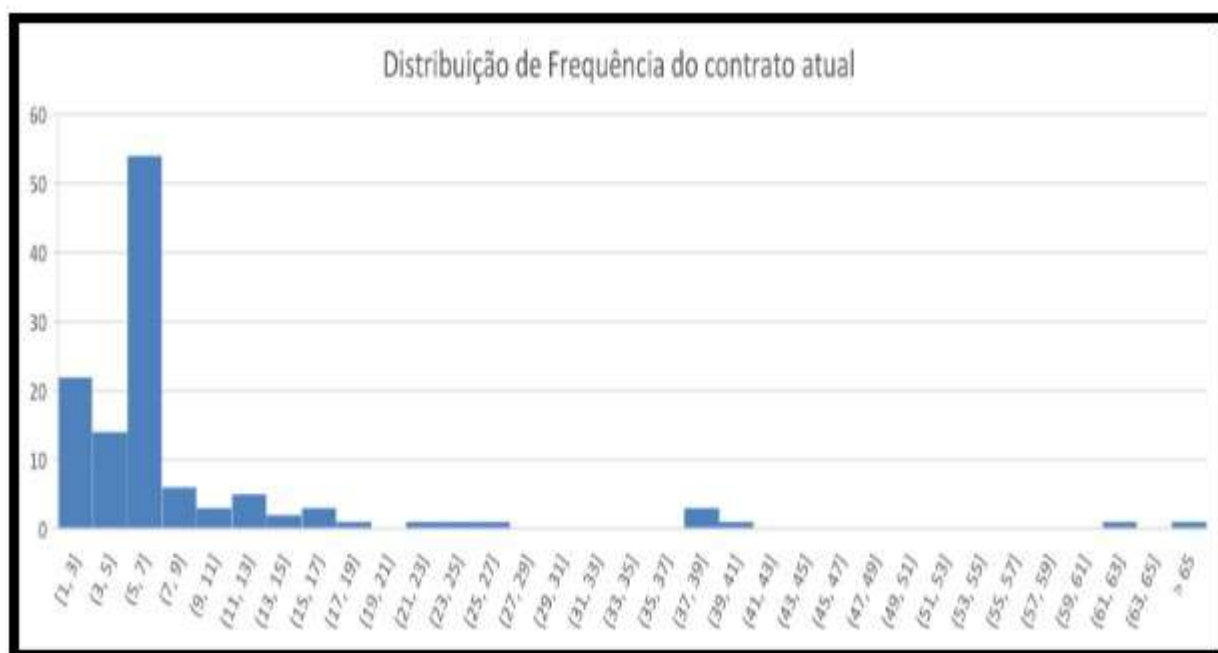
O objetivo é garantir cobertura Wi-Fi eficiente, segura e escalável, assegurando viabilidade econômica e continuidade dos serviços públicos essenciais.

### Análise Técnica e Estatística

A etapa inicial de dimensionamento considerou dados consolidados de 118 sites operacionais do contrato PE-Conectado II, a partir dos quais foi conduzida uma análise estatística sobre a quantidade de Access Points (APs) por site.

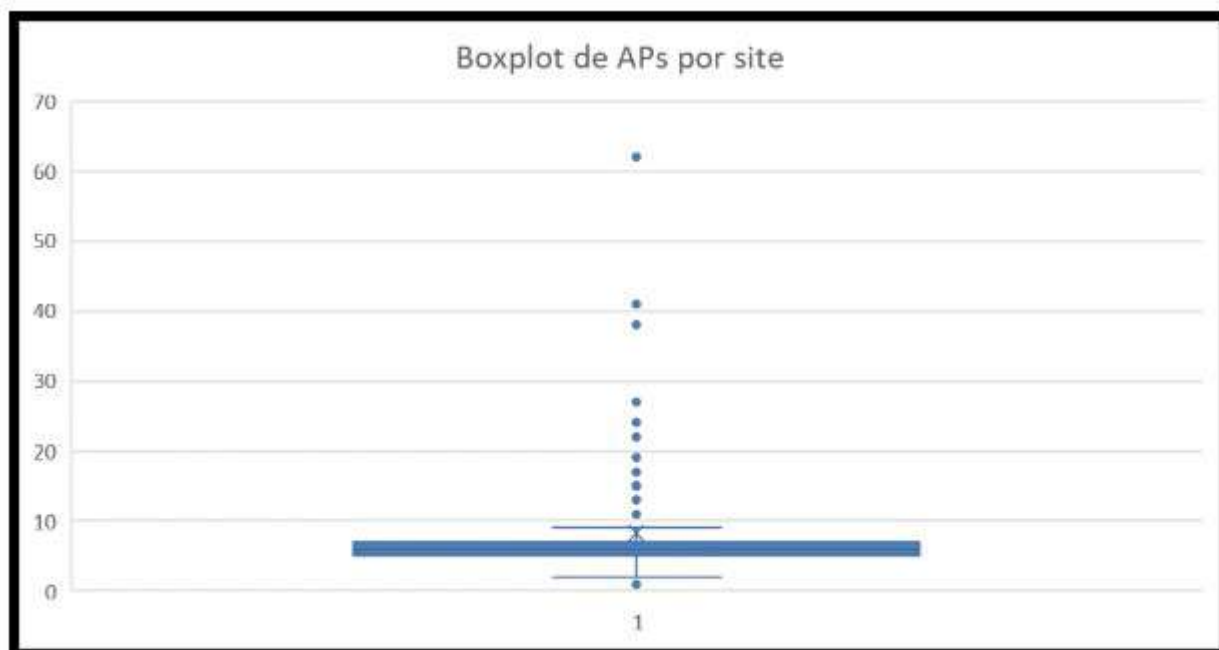
Os resultados apontaram mediana de 6 APs por site, com concentração da frequência entre 5 e 7 APs, conforme demonstrado em histograma e boxplot elaborados a partir dessa amostra.

- **Histograma** – Mostra a distribuição de APs por site, com maior frequência entre 5 e 7 APs;



(Nota: O gráfico mostra a quantidade de APs por site, com maior frequência entre 5 e 7 APs)

- **Boxplot** – Evidencia a mediana em 6 APs por site, com um intervalo interquartil (IQR) de 5 a 7 APs e poucos outliers acima de 10 APs, confirmando baixa dispersão.



(Nota: O boxplot mostra a distribuição central dos dados, com a mediana em 6 APs e poucos outliers acima de 10 APs, caracterizados como exceções operacionais.)

Essa distribuição confirmou baixa dispersão e estabilidade na densidade de APs, consolidando 6 APs por site como parâmetro técnico ideal para cobertura adequada em ambientes internos típicos da rede estadual.

### Revisão Orçamentária e Ajuste do Dimensionamento

Durante a fase de revisão do planejamento e adequação orçamentária global do projeto, foi realizada uma reavaliação dos quantitativos originais.

Considerando o valor unitário médio de R\$ 568,35 por Access Point (AP), conforme o Mapa de Preços (SEI nº [69512608](#)), e a redução do parâmetro de 6 APs para 4,5 APs por site, obteve-se uma diminuição de 1,5 APs por site.

O impacto financeiro dessa redução pode ser expresso da seguinte forma:

**Economia por site:**  $(6 - 4,5) \text{ APs} \times \text{R\$ } 568,35 = \text{R\$ } 852,53$

**Economia mensal total:**  $2.865 \text{ sites} \times \text{R\$ } 852,53 = \text{R\$ } 2.442.484,13$

**Economia global em 48 meses:**  $\text{R\$ } 2.442.484,13 \times 48 = \text{R\$ } 117.239.238,00$

Portanto, o ajuste no parâmetro médio de APs por site resultou em **redução de aproximadamente R\$ 120 milhões** ao longo da execução contratual, sem comprometer a cobertura técnica ou o desempenho esperado, em razão dos ganhos de eficiência e capacidade esperados pela nova tecnologia Wi-Fi 7 (802.11be).

Com base nesse novo parâmetro, obteve-se o quantitativo total revisado de 12.892 APs internos, conforme abaixo:

**Estimativa revisada:**  $4,5 \text{ APs} \times 2.865 \text{ sites} = \mathbf{12.892 \text{ APs}}$

### Fundamentação Técnica da Redução

A redução do número médio de APs por site é tecnicamente viável em função dos avanços introduzidos pela tecnologia Wi-Fi 7 (IEEE 802.11be), especialmente quando comparada à infraestrutura atual do contrato PE-Conectado II, baseada em Wi-Fi 5 (IEEE 802.11ac). O novo padrão traz ganhos substanciais em eficiência espectral, largura de banda, capacidade de clientes simultâneos e cobertura física, permitindo uma utilização mais racional dos equipamentos.

Os principais fatores técnicos que justificam o uso otimizado de APs são:

1. **Aumento expressivo de throughput** – O Wi-Fi 7 opera com larguras de canal de até 320 MHz, quatro vezes superiores às do Wi-Fi 5 (80 MHz) utilizado atualmente no contrato PE-Conectado II, e o dobro das do Wi-Fi 6 e 6E — tecnologias mais amplamente adotadas no mercado corporativo. Esse avanço, aliado ao uso otimizado e ampliado da banda de 6 GHz (introduzida no Wi-Fi 6E e aprimorada no Wi-Fi 7), permite velocidades superiores a 5 Gbps reais por AP, reduzindo significativamente o risco da necessidade de densificação de pontos.
2. **Multi-Link Operation (MLO)** – Recurso que permite comunicação simultânea em múltiplas bandas (2,4, 5 e 6 GHz), aumentando a resiliência do sinal e a eficiência de uso de espectro, **ampliando a área efetiva de cobertura**.
3. **Maior capacidade de clientes simultâneos** – Cada AP pode atender até 2,5 vezes mais dispositivos com baixa latência, graças ao uso aprimorado de OFDMA e MU-MIMO em múltiplas direções.
4. **Eficiência energética e menor interferência** – O padrão implementa pacing temporal e coordenação de canal (TPC), **otimizando transmissões em ambientes densos e reduzindo overlap (sobreposição) entre células**.
5. **Melhor penetração e estabilidade de sinal** – A adoção da banda de 6 GHz e antenas de maior ganho proporciona melhor cobertura indoor, diminuindo a necessidade de sobreposição de APs.
6. **Ferramentas avançadas de gerenciamento (NMS)** – As plataformas de gestão de nova geração, com análise de espectro em tempo real, permitem balancear automaticamente a carga de clientes e ajustar potências de transmissão, otimizando o desempenho de cada AP instalado.

Esses fatores, somados à obrigatoriedade contratual de site survey técnico presencial e medições pós-implantação, mitigam eventuais riscos de subdimensionamento e asseguram cobertura plena, desempenho estável e escalabilidade futura para a rede sem fio da Nova Rede Corporativa.

### Garantia de Cobertura e Flexibilidade Operacional

Mesmo com a redução estimada, a modelagem adotada mantém robustez técnica e flexibilidade operacional, assegurando que a contratada execute site surveys técnicos presenciais e relatórios fotográficos, sem custo adicional, conforme previsto no Termo de Referência.

Esses levantamentos permitirão ajustes precisos por ambiente, evitando tanto subdimensionamento quanto superdimensionamento de APs e garantindo aderência às boas práticas internacionais de redes corporativas.

Assim, a estimativa de 4,5 APs por site, totalizando 12.892 APs, representa uma projeção tecnicamente coerente e financeiramente responsável, assegurando a funcionalidade, o desempenho e a escalabilidade da rede sem fio no âmbito da Nova Rede Corporativa do Estado de Pernambuco.

### 2.2. Serviço de Rede Sem Fio Externo com Segurança

O Serviço de Rede Sem Fio Externo com Segurança tem como finalidade prover conectividade autenticada, criptografada e de alta disponibilidade em ambientes externos, incluindo pátios, áreas de convivência, estacionamentos, praças de atendimento, áreas esportivas e espaços públicos de circulação. O serviço amplia o alcance da Rede Corporativa Estadual para áreas abertas, garantindo continuidade de conectividade segura e integrando-se de forma transparente à infraestrutura de autenticação e controle de acesso utilizada na rede interna (802.1X, RADIUS e NAC).

A solução constitui um componente essencial do modelo de Governo Digital e de mobilidade institucional, viabilizando conectividade segura para operações de campo, eventos institucionais, atendimentos presenciais, serviços itinerantes e integração interórgãos, mantendo a conformidade com os requisitos de segurança da informação e sigilo de dados.

### Metodologia de Estimativa e Fundamentação Técnica

Com base nas respostas da Pesquisa de Demanda (SEI nº [69510789](#)), foram identificadas 395 unidades com solicitação formal de cobertura Wi-Fi externa. Aplicando-se a projeção estatística proporcional — a partir da taxa de adesão de 37,6% dos órgãos consultados — estimou-se uma demanda potencial máxima de 1.050 unidades para todo o Estado.

Na planta atual do contrato PE-Conectado II (vigente desde 2020), observam-se apenas 60 Access Points (APs) externos instalados, o que demonstra baixa penetração histórica desse tipo de serviço e potencial de expansão ainda incipiente.

Diante desse cenário, e considerando os seguintes fatores:

- A necessidade de implantação gradual, compatível com a maturidade operacional da rede;
- As restrições orçamentárias globais do projeto, registradas no documento “Informação 3 – Resumo dos Processos” (SEI nº [72965319](#));
- A evolução tecnológica do padrão Wi-Fi 6 (802.11ax) para aplicações externas, que proporciona ganhos relevantes em alcance, estabilidade e capacidade simultânea de conexões;
- E a necessidade de garantir equilíbrio entre demanda potencial e sustentabilidade financeira.

Desta forma, foi definido o quantitativo de 500 Access Points (APs) externos para o Termo de Referência, por restrição orçamentária e maturidade tecnológica, correspondendo a uma projeção técnica e economicamente equilibrada.

### Justificativa Técnica da Adoção do Wi-Fi 6

O dimensionamento adota a tecnologia Wi-Fi 6 (802.11ax) para aplicações externas, substituindo o padrão Wi-Fi 5 (802.11ac) atualmente em uso no contrato PE-Conectado II. O Wi-Fi 6 oferece maior alcance, estabilidade de sinal e eficiência espectral, permitindo redução no número de APs necessários sem comprometer desempenho, cobertura ou segurança.

Principais características técnicas que justificam o dimensionamento:

- **OFDMA (Orthogonal Frequency Division Multiple Access)** – permite que um único AP atenda múltiplos dispositivos simultaneamente, otimizando o uso do canal e reduzindo latência;
- **MU-MIMO aprimorado (Multi-User Multiple Input Multiple Output)** – possibilita transmissões paralelas de dados para vários usuários, ampliando a eficiência espectral;

- **Target Wake Time (TWT)** – melhora o gerenciamento de energia e o tempo de resposta, ideal para ambientes com grande variação de clientes conectados;
- **BSS Coloring** – reduz interferências entre células adjacentes, permitindo ampliar o raio efetivo de cobertura de cada AP;
- **Maior robustez física e resistência ambiental** – equipamentos outdoor Wi-Fi 6 possuem **proteção IP67** e design industrial, assegurando operação contínua sob intempéries e reduzindo custos de manutenção.

Essas melhorias permitem que um menor número de APs seja suficiente para cobrir áreas externas extensas com alto desempenho e confiabilidade, reduzindo significativamente o risco de necessidade de densificação de APs, especialmente em aplicações de baixa e média densidade de usuários (como pátios, estacionamentos ou áreas abertas de atendimento).

Dessa forma, o quantitativo de **500 unidades de APs externos Wi-Fi 6** representa uma projeção técnica e economicamente equilibrada, capaz de:

- Atender plenamente às demandas ativas e potenciais;
- Garantir cobertura eficiente e segura em ambientes externos;
- Reduzir custos de implantação e manutenção; e
- Permitir expansão gradual conforme o crescimento do uso e a evolução tecnológica.

### 2.3. Serviço de Rede Sem Fio Temporário com Segurança

O Serviço de Rede Sem Fio Temporário com Segurança foi concebido para operações sob demanda e de curta duração, com vigência de até seis meses por ciclo, conforme disposto na Seção 6 do Adendo IV. O serviço é destinado a eventos institucionais, programas públicos itinerantes, situações emergenciais e ações sazonais que demandam conectividade segura, criptografada e de rápida disponibilização em locais sem infraestrutura fixa.

A Pesquisa de Demanda (SEI nº [69510789](#)), registrou 121 solicitações para esse serviço. Entretanto, considerando:

- O histórico do contrato PE-Conectado II (vigente desde 2020), no qual foram registradas 19 contratações de serviços temporários, **nenhuma delas de rede sem fio**;
- A variabilidade natural das demandas de caráter eventual;
- O custo unitário de R\$ 542,95 (conforme Mapa de Preços – SEI nº [69512608](#));
- E as restrições orçamentárias já mencionadas;

Dessa forma, fixou-se o quantitativo de **10 unidades** por ciclo de seis meses, correspondendo a **60 implantações temporárias** ao longo do contrato, o que assegura equilíbrio entre capacidade operacional, flexibilidade de atendimento e sustentabilidade financeira.

Esse volume garante atendimento ágil e flexível, compatível com a frequência histórica e dentro dos limites orçamentários estabelecidos, cobrindo as demandas mais recorrentes observadas em órgãos, eventos estaduais e aos atendimentos emergenciais ou de grande porte.

As ativações temporárias deverão observar as mesmas premissas de segurança, autenticação e segregação de tráfego aplicáveis à rede corporativa permanente, assegurando que as conexões eventuais mantenham o mesmo padrão de conformidade e rastreabilidade operacional.

Por fim, a efetiva necessidade de cada implantação deverá ser validada mediante site survey técnico, executado pela contratada sem custos adicionais, assegurando dimensionamento preciso e aderência às condições do ambiente.

## 2.4. Serviço de fornecimento e implantação de Switch

O Serviço de Fornecimento e Implantação de Switch foi concebido como item autônomo dentro do Adendo IV, em razão de sua relevância técnica e impacto financeiro direto na infraestrutura da Rede Sem Fio da Nova Rede Corporativa.

Durante a análise de mercado e as simulações de composição de preços e topologia, verificou-se que a inclusão dos switches diretamente no custo global dos serviços de rede sem fio (Wi-Fi Interno e Externo) elevava significativamente os valores unitários, sem contrapartida técnica proporcional.

Para mitigar riscos de sobrepreço e garantir transparência e rastreabilidade dos custos, optou-se por tratar esse componente como um serviço independente, com contratação vinculada à necessidade técnica efetivamente validada.

Esse modelo permite controle individualizado pela ATI, que verificará, por meio de relatórios de site survey, a real necessidade de instalação do equipamento em cada localidade.

Essa estratégia garante:

- **Racionalidade técnica**, evitando aquisição desnecessária de equipamentos;
- **Otimização da topologia Mesh**, reduzindo a necessidade de cabeamento e o consumo de portas físicas nos switches;
- **Flexibilidade operacional**, permitindo adequação ao porte e topologia de cada site;
- **Controle financeiro**, com pagamento apenas mediante validação e instalação comprovada;
- **E prevenção de sobrepreço**, promovendo aderência às boas práticas de governança e à Lei nº 14.133/2021.

## Cálculo do Quantitativo e Fundamentação/ Critérios Técnicos e Estatísticos considerados:

O dimensionamento total foi estabelecido em **716 unidades de switches**, com base na arquitetura de interconexão dos Access Points (APs) e na distribuição estatística da quantidade de Access Points (APs) dos sites do atual contrato PE-Conectado II.

### 1. Necessidade Técnica para uso do Switch:

- Cada nó de APs da rede pode conectar até 8 APs na topologia Mesh (1+7), sendo 1 AP conectado fisicamente à UTM e os 7 demais conectados via tecnologia Mesh;
- Ou seja, para sites com mais de 8 APs, teremos a necessidade de uso de Switch, pois teremos a necessidade técnica de conectar fisicamente mais de um AP.
- Sendo assim, os sites com mais de 8 APs terão a necessidade técnica de usar Switch;

### 2. Análise técnica e estatística:

- Considerando a análise estatística citada no gráfico de **Boxplot** – Evidencia a mediana em 6 APs por site, com um intervalo interquartil (IQR) de 5 a 7 APs e poucos outliers acima de 10 APs, confirmando baixa dispersão, podemos concluir que:
- Estatisticamente, o Primeiro (Q1), Segundo (Q2) e Terceiro Quartil (Q3), que representam 75% dos sites, possuem até 7 APs;
  - Tecnicamente, nesses sites, com até um nó de APs em topologia Mesh, o AP pode ser conectado diretamente à UTM, dispensando o uso de switch adicional na maioria dos casos;
  - Considerando o menor porte e densidade de APs nesses locais, a necessidade de switches será residual e pontual.
- Estatisticamente, o Quarto Quartil (Q4), que representa 25% dos sites, possuem 8 ou mais APs;
  - Tecnicamente, os sites com mais de 8 APs, ou seja, com 2 ou mais nós, terão a necessidade de switch para conectar os APs;

### 3. Cálculo da Necessidade Potencial de Switch:

- Considerando que cada site que possui mais de 8 APs terá a necessidade de switch, temos que:
- **Total de sites:**  $2.865 \text{ sites} \times 25\% (Q4) = 716 \text{ sites}$
- **Estimativa revisada no quantitativo de switches : 716**

### Validação Técnica e Supervisão Operacional

A ATI deverá avaliar o resultado de todos site survey realizados pela contratada, validando os relatórios técnicos e determinando, de forma criteriosa, onde o uso de switches é efetivamente indispensável.

Essa verificação técnica permitirá:

- Confirmar a aderência às premissas de interconexão por UTM;
- Ajustar o número de switches conforme o porte real da localidade;
- Evitar superdimensionamentos e compras desnecessárias;
- E garantir a máxima eficiência técnica e financeira do projeto.

Cabe ressaltar que a projeção de 716 unidades representa um limite teórico de dimensionamento, baseado na topologia de referência em mesh e nas capacidades dos equipamentos previstos.

Entretanto, em campo podem ocorrer variações pontuais, motivadas por fatores como layout físico, obstáculos estruturais, demandas específicas de cobertura ou restrições de cabeamento, as quais deverão ser tratadas caso a caso, mediante validação conjunta entre a ATI e a Contratada.

Por fim, a adoção da tecnologia Wi-Fi 7 mesh (802.11be) nas aplicações indoor do projeto reduz de forma significativa a necessidade de interconexão densa por switches, em razão dos avanços técnicos que ampliam a eficiência e a capacidade de cada AP, diminuindo a pressão sobre a infraestrutura cabeada. Assim, a estimativa de 716 switches revela-se tecnicamente fundamentada, operacionalmente plausível e financeiramente responsável, em plena aderência aos princípios de eficiência, economicidade e sustentabilidade contratual.

### 3) ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598281-2	Link de Acesso Permanente (LAP - Tipo 1)	2968	link
2	598282-0	Link de Acesso Permanente (LAP - Tipo 2)	2212	link
3	598755-5	Link Multitecnologia Especial (LME) - Tipo 1	250	link
4	598757-1	Link Multitecnologia Especial (LME) - Tipo 2	20	link
5	598758-0	Link Multitecnologia Especial (LME) - Tipo 3	20	link
6	598761-0	Link Acesso Temporário (LAT) - Tipo 1	30	link
7	598762-8	Link Acesso Temporário (LAT) - Tipo 2	20	link
8	598763-6	Link Acesso Temporário (LAT) - Tipo 3	20	link

#### 3.1. Link de Acesso Permanente (LAP - Tipo 1) , e

#### 3.2. Link de Acesso Permanente (LAP - Tipo 2)

O dimensionamento dos serviços de conectividade vinculados ao Adendo V – Links de Acesso Permanente (LAP Tipo 1 e Tipo 2) foi realizado com base em critérios técnicos, operacionais, financeiros e de continuidade de serviço, considerando a planta atual da Rede Estadual, os dados históricos de utilização, as projeções de crescimento com as redundâncias e as restrições orçamentárias vigentes.

A definição dos quantitativos para os serviços LAP Tipo 1 e LAP Tipo 2 teve como principal referência a planta consolidada do contrato PE-Conectado II, extraída em 23/10/2025, conforme **Planilha Base de Links de Acesso - 231025 (SEI nº 76072589)** e obtida por meio do Portal de Relatórios (<https://portalderelatorios.peconectado.pe.gov.br>).

#### Critérios Técnicos de Classificação

Foram adotados dois critérios principais para migração dos links existentes para o novo modelo contratual:

- Critério 1 – Velocidade contratada:**  
Todos os sites com links do tipo **ADC** (principal ou básico) operando com velocidades **iguais ou superiores a 60 Mbps** foram classificados como **LAP Tipo II**.  
→ **Resultado: 934 sites.**

2. **Critério 2 – Órgãos da Administração Indireta com contratos próprios:**  
Foram incorporados como **LAP Tipo II** os circuitos atualmente contratados pelos seguintes órgãos, ainda que operando com velocidades inferiores a 60 Mbps, conforme planilha-base:

- Tribunal de Justiça de Pernambuco (TJPE): **164 sites**
- Tribunal de Contas do Estado (TCE-PE): **7 sites**
- Assembleia Legislativa de Pernambuco (ALEPE): **1 site**

→ **Total adicional: 172 sites**

Assim, obteve-se um total de **1.106 sites LAP Tipo II (934 + 172)**.

### Classificação dos Sites LAP Tipo I

Os sites com velocidade **inferior a 60 Mbps** (40, 20 e 10 Mbps) foram classificados como **LAP Tipo I**, totalizando **1.596 sites**, conforme planilha, aba "Links x Velocidade".

A esses foram adicionados **163 links de Escolas Indígenas** — sendo **139 instaladas** (aba "Esc. Indígenas - Instaladas") e **24 com ordens de instalação em andamento** (aba "OSs abertas - Esc Indígenas") — resultando em um total de **1.759 sites LAP Tipo 1**.

### Aplicação de Premissas de Redundância e Ajustes de Dimensionamento

A partir da base consolidada de **2.865 sites** (1.759 LAP 1 + 1.106 LAP 2), aplicaram-se as seguintes premissas:

1. **Redundância** **por** **site:**

Considerando a possibilidade de **dupla abordagem**, para aumentar a disponibilidade, o dimensionamento inicial previu **duas conexões independentes (links redundantes)** por site, totalizando **5.730 links** potenciais ( $2 \times 2.865$ ).

2. **Ajustes para controle de custos e racionalização de uso:**

- Foram removidas redundâncias em **306 sites** classificados como de baixa criticidade operacional, distribuídos da seguinte forma:

- IPA: 180 sites
- ADAGRO: 73 sites
- Projeto Mãe Coruja: 53 sites

→ **Total excluído: 306 redundâncias.**

- **SEE (Secretaria de Educação):**

**244 sites** com conectividade via satélite (Starlink) tiveram a redundância substituída pelo link satelital.

3. **Resultado consolidado:**

- Total de links LAP Tipo II: **2.212 links (1.106 sites  $\times$  2)**
- Total de links LAP Tipo I ajustado: **5.730 (total teórico) – 2.212 (LAP II) – 550 (redundâncias retiradas) = 2.968 links LAP Tipo 1**

- O total de **550 redundâncias removidas** corresponde à soma dos 306 sites de baixa utilização (IPA, ADAGRO e Projeto Mãe Coruja) e dos 244 sites da SEE com conectividade substituída por VSAT (Starlink).

#### Resumo Quantitativo Final

Tipo de Link	Critério de Classificação	Sites Base	Redundância Aplicada	Total de Links Contratados
LAP Tipo I	< 60 Mbps e Escolas Indígenas	1.759	Parcial (com restrições) 550 sites(306 + 244)	2.968
LAP Tipo II	≥ 60 Mbps ou órgãos da Adm. Indireta (TJPE, TCE, ALEPE)	1.106	2×	2.212
<b>Total Geral</b>	—	<b>2.865 sites</b>	—	<b>5.180 links</b>

Por fim, o dimensionamento proposto assegura equilíbrio técnico, operacional e financeiro, garantindo capacidade adequada ao perfil de cada site, flexibilidade para redundância onde tecnicamente justificada, e compatibilidade com a estrutura de custos e diretrizes de priorização da Nova Rede Corporativa do Estado de Pernambuco.

#### 3.3. Link Multitecnologia Especial (LME) - Tipo 1

#### 3.4. Link Multitecnologia Especial (LME) - Tipo 2

#### 3.5. Link Multitecnologia Especial (LME) - Tipo 3

O dimensionamento do **Serviço de Link Multitecnologia Especial (LME)** foi estruturado para assegurar conectividade a localidades que, por restrições técnicas, geográficas ou operacionais, não podem ser atendidas pelos modelos LAP Tipo 1 e 2, os quais dependem obrigatoriamente de infraestrutura de fibra óptica para entrega do serviço.

Foram consideradas as condições atuais de cobertura e infraestrutura da rede estadual, bem como a evolução tecnológica de soluções satelitais — especialmente as constelações de baixa órbita (LEO) — e das redes móveis 5G e FWA (Fixed Wireless Access). Tais tecnologias, ainda que apresentem limitações de latência, jitter e estabilidade em ambientes de alta demanda, demonstram tendência de rápida maturação, ampliação de capilaridade e redução de custo ao longo da vigência contratual, podendo contribuir de forma estratégica para a universalização da conectividade governamental.

#### Fontes de Dados Utilizadas

O dimensionamento partiu da **Pesquisa de Demanda (SEI nº [69186852](#))**, que identificou **340 localidades** com necessidade de atendimento via LME, distribuídas da seguinte forma:

- **42 LME Tipo 1**
- **209 LME Tipo 2**

- **89 LME Tipo 3**

Complementarmente, foi analisado o documento SEI nº [69187260](#), referente à base de conectividade do contrato PE-CONECTADO II, o qual registra 220 sites atualmente atendidos por acessos satelitais, indispensáveis à manutenção da conectividade em regiões remotas, áreas rurais, comunidades indígenas, quilombolas e demais localidades de difícil acesso geográfico ou logístico.

Esses 220 sites, por sua natureza e localização, tenderão a permanecer com atendimento via tecnologias não-fibra (LME Tipo 01), dependendo da tecnologia adotada da empresa vencedora.

#### Readequação de Quantitativos

Considerando os aspectos operacionais (continuidade de serviço e abrangência territorial) e os limites financeiros do projeto (conforme documento “Informação 3 – Resumo dos Processos”, SEI nº [72965319](#)), efetuou-se a readequação dos quantitativos originalmente estimados, preservando a cobertura essencial, a conectividade de localidades críticas e assegurando margem de flexibilidade para atendimento à Pesquisa de demanda, evolução tecnológica progressiva e demandas regionais.

Tipo de LME	Descrição Técnica	Base de Origem	Quantidade Final
<b>LME Tipo 01</b>	Atendimento satelital (LEO/MEO) ou tecnologia equivalente para regiões remotas e rurais	220 sites da rede atual + 30 da Pesquisa de Demanda	<b>250</b>
<b>LME Tipo 02</b>	Atendimento híbrido (4G/5G/FWA) para áreas semiurbanas	Parcial da Pesquisa de Demanda	<b>20</b>
<b>LME Tipo 03</b>	Atendimento de alta capacidade multitecnologia	Parcial da Pesquisa de Demanda	<b>20</b>
<b>Total Geral</b>	—	—	<b>290 links</b>

Dessa forma, o dimensionamento do serviço LME promove equilíbrio entre cobertura geográfica, viabilidade técnica e sustentabilidade financeira, garantindo continuidade operacional e conectividade em áreas fora do alcance da infraestrutura óptica convencional.

A priorização de 250 LME Tipo 1 preserva a conectividade de serviços públicos essenciais hoje suportados por soluções satelitais, enquanto os 40 circuitos adicionais (LME Tipo 2 e Tipo 3) asseguram capacidade de expansão controlada, acompanhando a maturação tecnológica das redes satelitais, móveis e híbridas ao longo da vigência contratual.

#### 3.6. Link Acesso Temporário (LAT) - Tipo 1

#### 3.7. Link Acesso Temporário (LAT) - Tipo 2

### 3.8. Link Acesso Temporário (LAT) - Tipo 3

O dimensionamento dos **Serviços de Link de Acesso Temporário (LAT)**, em seus três tipos (Tipo 1, Tipo 2 e Tipo 3), foi estruturado considerando a natureza emergencial, transitória e de pronta resposta desse serviço, destinado a atender demandas pontuais, como eventos institucionais, programas governamentais, ações emergenciais, situações de calamidade pública, demandas populares e outras necessidades extraordinárias da Administração Pública Estadual.

Essa modelagem encontra-se formalmente definida nos Adendos II e V do Termo de Referência, que estabelecem que a Contratada deverá garantir a ativação de qualquer solicitação do serviço em até **quinze (15) dias corridos**, independentemente da tecnologia empregada. A escolha do meio físico de transporte — seja fibra óptica, enlace rádio, satélite, 4G/5G, FWA (Fixed Wireless Access) ou outro — é de **livre decisão da CONTRATADA**, desde que sejam observados integralmente os Níveis Mínimos de Serviço (NMS) e os parâmetros operacionais definidos no Termo de Referência.

A definição de três tipos de LAT foi adotada justamente para garantir flexibilidade tecnológica e operacional, permitindo que as soluções sejam adaptadas às características específicas de cada localidade e necessidade. Esse modelo favorece a competitividade e a neutralidade tecnológica, permitindo que as licitantes apresentem soluções baseadas nas tecnologias mais viáveis sob os aspectos técnico, econômico e logístico para cada situação específica.

Essa abordagem está alinhada às melhores práticas de contratações de TIC, assegurando neutralidade tecnológica, foco em resultados, escalabilidade e mitigação de riscos operacionais e jurídicos.

#### Dimensionamento dos Quantitativos

O dimensionamento dos quantitativos teve como base a Pesquisa de Demanda (SEI nº [69510789](#)), que identificou **133 unidades** com potencial necessidade de atendimento via LAT, distribuídas conforme segue:

- **11 LAT Tipo 01**
- **20 LAT Tipo 02**
- **102 LAT Tipo 03**

Entretanto, com base no histórico contratual do PE-CONECTADO II, que registrou apenas 19 circuitos temporários contratados desde 2020 (conforme Planilha “Links Temporários – ADT – Contrato PE-CONECTADO II”, SEI nº [76075149](#)), e considerando as restrições orçamentárias do projeto (Informação 3 – SEI nº [72965319](#)), definiu-se um dimensionamento prudente e realista, ajustando o quantitativo total para 70 unidades, distribuídas conforme tabela a seguir:

Tipo de LAT	Quantidade Final
LAT Tipo 01	30
LAT Tipo 02	20
LAT Tipo 03	20

Total Geral

70 links

A definição dos quantitativos do serviço LAT busca garantir cobertura equilibrada para as demandas efetivamente observadas, mantendo margem de flexibilidade operacional para atendimento a novas solicitações durante a vigência contratual, sem comprometer o equilíbrio financeiro do projeto.

A medida garante a capacidade do Estado de atender com agilidade e segurança às necessidades temporárias e emergenciais, assegurando racionalidade orçamentária, aderência às boas práticas de planejamento público e conformidade com os princípios de economicidade e eficiência.

#### 4) ADENDO VI - SEGURANÇA DE DATACENTER

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598673-7	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER	6	Unidade
2	598674-5	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço	3	Unidade
3	598677-0	Solução de segurança de confiança zero - ZTNA	1221	Unidade
4	598678-8	Solução de proteção, detecção e resposta para servidores - EDR	4200	Servidor
5	598679-6	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR	3	Servidor
6	598680-0	Solução para gerenciamento de acessos à rede datacenter - NAC	1221	Unidade
7	598681-8	Solução de segurança de identidade privilegiada - PAM	1221	usuário
8	598682-6	Solução de filtro de mensagens indesejadas - ANTISPAM	129058	usuário
9	598683-4	Solução de Filtro de Aplicações WEB - WAF	3	Unidade

##### 4.1. Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER

As 6 (seis) unidades da solução unificada de segurança de rede para datacenter visa atender os 3 (três) datacenters do estado (ATI, SEE e SEFAZ) configurados em modo de alta disponibilidade.

#### **4.2. Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço**

O dimensionamento foi realizado com base na demanda real e atual, focando nos 3 (três) datacenters oficiais do Estado, os quais serão devidamente atendidos com soluções de alta disponibilidade dentro da capacidade contratada.

#### **4.3. Solução de segurança de confiança zero - ZTNA**

O quantitativo de 1.221 (mil duzentos e vinte e uma) unidades refere-se a quantidade atual de usuários administradores dos servidores dos datacenters atendidos, sendo 1.099 (mil e noventa e nove) usuários da ATI, 100 (cem) da SEE e 22 (vinte e dois) da SEFAZ.

#### **4.4. Solução de proteção, detecção e resposta para servidores - EDR**

A estimativa atual é de cobertura para 4.155 servidores dos datacenters do governo do Estado, sendo 3.349 (três mil, trezentos e quarenta e nove) da ATI, 456 (quatrocentos e cinquenta e seis) da SEE e 350 (trezentos e cinquenta) da SEFAZ.

#### **4.5. Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR**

A solução foi planejada para cobrir infraestruturas críticas que mantêm sistemas legados nos 03 (três) datacenters do Governo do Estado, monitorando e protegendo o tráfego de rede contra ameaças avançadas.

#### **4.6. Solução para gerenciamento de acessos à rede datacenter - NAC**

O quantitativo de 1.221 (mil duzentos e vinte e uma) unidades refere-se a quantidade atual de usuários administradores dos servidores dos datacenters atendidos, sendo 1.099 (mil e noventa e nove) usuários da ATI, 100 (cem) da SEE e 22 (vinte e dois) da SEFAZ.

#### **4.7. Solução de segurança de identidade privilegiada - PAM**

O quantitativo de 1.221 (mil duzentos e vinte e uma) unidades refere-se a quantidade atual de usuários administradores dos servidores dos datacenters atendidos, sendo 1.099 (mil e noventa e nove) usuários da ATI, 100 (cem) da SEE e 22 (vinte e dois) da SEFAZ.

#### **4.8. Solução de filtro de mensagens indesejadas - ANTISPAM**

- Aproximadamente 128.000 servidores públicos ativos + 1.058 usuários terceirizados da mão de obra de TI do estado atualmente.
- Mão de obra terceirizada em TI no estado: Painel força de trabalho de TIC 2024, elaborado pela ATI.

- Servidores:[https://www.pe.gov.br/noticias/administracao/2023/12/29/governo-do-estado-divulga-calendario-de-pagamento-dos-servidores-para-o-ano-de-2024/#:~:text=N%C3%BAmero%20de%20servidores%2D%20Atualmente%2C%20Pernambuco,pensionistas%20\(dados%20de%20novembro\).](https://www.pe.gov.br/noticias/administracao/2023/12/29/governo-do-estado-divulga-calendario-de-pagamento-dos-servidores-para-o-ano-de-2024/#:~:text=N%C3%BAmero%20de%20servidores%2D%20Atualmente%2C%20Pernambuco,pensionistas%20(dados%20de%20novembro).)

#### 4.9. Solução de Filtro de Aplicações WEB - WAF

O quantitativo contempla os 03 (três) datacenters do Estado (ATI, SEE e SEFAZ), garantindo proteção contra ataques direcionados às aplicações hospedadas nesses ambientes.

### 5) ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598642-7	Solução de gerenciamento e monitoramento de ativos - ITAM	1	Unidade
2	598685-0	Solução de gerenciamento de identidade de acesso - IAM	629058	Unidade
3	598686-9	Solução de monitoramento e análise de eventos de segurança - SIEM	480894	Unidade
4	598687-7	Solução de automação de resposta a incidentes de segurança - SOAR	1	Unidade
5	598643-5	Solução para guarda de LOGs	1	Unidade
6	598644-3	Serviço de disponibilização de ambiente de testes	1	Unidade
7	598645-1	Solução de gerenciamento de serviços de TI - ITSM	1	Unidade

#### 5.1. Solução de gerenciamento e monitoramento de ativos - ITAM

Visa atender ao monitoramento de todos os ativos contratados no projeto.

#### 5.2. Solução de gerenciamento de identidade de acesso - IAM

Proposta visa atender aproximadamente 500.000 alunos da rede estadual de educação do estado + 129.058 servidores públicos (incluindo a mão de obra terceirizada).

- Alunos:<https://portal.educacao.pe.gov.br/no-dia-da-escola-pernambuco-celebra-as-1061-unidades-de-ensino-da-rede-estadu->

al/#:~:text=Atualmente%2C%20Pernambuco%20conta%20com%201061,gest%C3%A3o%20da%20governad  
ora%20Raquel%20Lyra.

- Servidores:[https://www.pe.gov.br/noticias/administracao/2023/12/29/governo-do-estado-divulga-calendario-de-pagamento-dos-servidores-para-o-ano-de-2024/#:~:text=N%C3%BAmero%20de%20servidores%2D%20Atualmente%2C%20Pernambuco,pensionistas%20\(dados%20de%20novembro\).](https://www.pe.gov.br/noticias/administracao/2023/12/29/governo-do-estado-divulga-calendario-de-pagamento-dos-servidores-para-o-ano-de-2024/#:~:text=N%C3%BAmero%20de%20servidores%2D%20Atualmente%2C%20Pernambuco,pensionistas%20(dados%20de%20novembro).)

### 5.3. Solução de monitoramento e análise de eventos de segurança - SIEM

Visa atender ao monitoramento de todos os ativos contratados no projeto.

Cada usuário se conecta e reconecta cerca de 3 vezes ao dia, cada conexão gera de 2 a 4 eventos (conexão, autenticação, atribuição de perfil, liberação), estimativa de 6 a 12 eventos por dia por usuário. Cálculo usuários x eventos_do_dia / segundos_do_dia. Para o pico de uso foi considerado o mesmo cálculo porém considerando apenas 5% dos usuários em um período de 1h.	Usuários	Eventos por usuário	Total dia	EPS médio	Usuários em pico (5% em 1h)
<b>Solução para gerenciamento de acessos à rede local - NAC</b>	24427	12	293124	3,4	4,071
<b>Solução para gerenciamento de acessos à rede datacenter - NAC</b>	1221	12	14652	0,2	0,204
					4
Cada usuário realiza em média 3 logins por dia, cada login gera 3 eventos (solicitação, verificação, resultado), estimativa de 9 eventos por usuário por dia. Cálculo usuários x eventos_do_dia / segundos_do_dia. Para o pico de uso foi considerado o mesmo cálculo porém considerando apenas 5% dos usuários em um período de 1h.	Usuários	Eventos por usuário	Total dia	EPS médio	Usuários em pico (5% em 1h)
<b>Solução de gerenciamento de identidade de acesso - IAM</b>	629058	9	5661522	66	78,632
					79
UTM de 2 Gbps – Até 100 usuários EPS estimado bruto: 150 EPS Redução com filtros de segurança: 70% EPS final (filtrado): 45 EPS Filtros aplicados: exclusão de eventos de baixo impacto, retenção de logs relevantes para análise	UTM		Total dia	EPS médio	Usuários em pico (5% em 1h)

de incidentes e ameaças avançadas.					
<b>Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1</b> (Proteção combinada de ameaças 2Gb)	1759		6838993000	45	94986
					94986
UTM de 4 Gbps – Até 500 usuários					
EPS estimado bruto: 800 EPS					
Redução com filtros de segurança: 75%					
EPS final (filtrado): 200 EPS					
Filtros aplicados: exclusão de eventos de baixo impacto, retenção de logs relevantes para análise de incidentes e ameaças avançadas.					
<b>Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2</b> (Proteção combinada de ameaças 4Gb)	1299		22446720000	200	311760
					311760
UTM de 20 Gbps – Datacenter / 2.000+ usuários					
EPS estimado bruto: 4.000 EPS					
Redução com filtros de segurança: 80%					
EPS final (filtrado): 800 EPS					
Filtros aplicados: foco em logs de alto risco (como tráfego negado, IPS de severidade alta, eventos de VPN e anomalias), adequados à criticidade do ambiente.					
<b>Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER</b> (Proteção combinada de ameaças 20Gb)	6		414720000	800	5760
					5760
Para o EDR faz-se necessário algumas considerações:					
- Execução de processos: de 500 - 2000 eventos por dia					
- Criação/modificação de arquivos: 200 - 1000 eventos por dia					
- Conexões de rede: 300 - 1000 eventos por dia					

<p>- Eventos de segurança: 10 - 50 eventos por dia</p> <p>- Atualizações do agente: 24 - 100 eventos por dia</p> <p>Totalizando 4150 eventos por dia para cada servidor, porém, haverá filtros e priorização dos eventos, tomaremos por média 2000 eventos por dia por servidor.</p> <p>Cálculo: servidores x eventos_por_dia / segundos_do_dia</p> <p>Cálculo de pico: Para o pico de uso foi considerado o mesmo cálculo porém considerando apenas 5% dos eventos em um período de 1h.</p>					
<b>Solução de proteção, detecção e resposta para servidores - EDR</b>	4200	2000	8400000	97	117
					117
<p>Cada appliance de NDR é responsável por monitorar o tráfego de rede em tempo real, realizando inspeção profunda de pacotes (DPI), correlação de eventos, detecção de comportamentos anômalos e indicadores de comprometimento (IoC). Em ambientes corporativos com redes distribuídas e tráfego considerável, é comum estimar que um NDR gere entre 100 a 500 EPS, dependendo da quantidade de tráfego espelhado, volume de ativos monitorados e políticas de detecção configuradas. Para efeito de dimensionamento seguro e compatível com cenários de segurança avançada, foi adotada a média de 300 EPS por appliance de NDR.</p>					
<b>Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR</b>	3	300	77760000	900	1080
					1080
<p>Foi considerado uma média de 2 sessões por usuário por dia. Cada sessão gera cerca de 5 eventos (login, cofre, acesso remoto, encerramento, ações registradas), totalizando 10 eventos por usuário por dia. Cálculo usuários x eventos_do_dia / segundos_do_dia. Para o pico de uso foi considerado o mesmo cálculo porém considerando apenas 5% dos usuários em um período de 1h.</p>					
<b>Solução de segurança de identidade privilegiada - PAM</b>	1221	10	12210	0,1	0,170
					1
<p>Foi realizada a coleta de um extrato de uma semana para o WAF da ATI onde foi observado que o equipamento gera 111 EPS em média. Com isso, levando em conta que estamos considerando 6 appliances, foi realizado a multiplicação de 111 x 6.</p>					

<b>Solução de Filtro de Aplicações WEB - WAF</b>	3	111	28771200	333	400
					400
<p>Foi considerada uma média de 5 eventos por segundo (EPS) por access point Wi-Fi 7. Essa estimativa contempla eventos recorrentes em ambientes de rede sem fio corporativa com alta densidade de usuários, como associações e autenticações de dispositivos, roaming, alertas de interferência, detecção de APs suspeitos e eventos administrativos. Trata-se de um valor conservador e adequado para redes com segurança e monitoramento ativo, garantindo capacidade de ingestão no SIEM mesmo em cenários de pico ou investigações.</p>					
	<b>Unidade</b>	<b>EPS por AP</b>	<b>Total dia</b>	<b>EPS médio</b>	<b>Usuários em pico (5% em 1h)</b>
<b>Serviço de Rede Sem Fio</b>	10.528	5	454809600	52640	63168
					63168
<p>Foi considerada uma média de até 5 eventos por segundo por switch gerenciável. Essa estimativa contempla eventos operacionais frequentes, como alteração de estado de portas, autenticações 802.1X, troca de VLAN, alertas de segurança (DHCP snooping, STP, ARP inspection) e mudanças administrativas. O cálculo seguiu a fórmula: quantidade de switches × EPS médio. Para o pico de uso, foi aplicado o mesmo cálculo considerando que 5% dos eventos diários podem se concentrar em um período de 1 hora, resultando em um aumento pontual da carga de eventos sobre o SIEM.</p>					
	<b>Unidade</b>	<b>EPS por Switch</b>	<b>Total dia</b>	<b>EPS médio</b>	<b>Usuários em pico (5% em 1h)</b>
<b>Serviço de fornecimento e implantação de Switch</b>	590	5	254880000	2950	3540
					3540

#### 5.4. Solução de automação de resposta a incidentes de segurança - SOAR

Necessário a contratação de 1 solução para atender a demanda de operação de segurança da operação.

#### 5.5. Solução para guarda de LOGs

Necessário a contratação de 1 solução para atender a demanda de operação de segurança da operação.

#### 5.6. Serviço de disponibilização de ambiente de testes

Necessário a contratação de 1 solução para atender a demanda de operação de segurança da operação.

#### 5.7. Solução de gerenciamento de serviços de TI - ITSM

Necessário a contratação de 1 solução para atender a demanda de operação de segurança da operação.

6) ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598688-5	Serviço de resposta à incidentes de cibersegurança sob demanda	318	HORA
2	598646-0	Serviço de análise de segurança de primeiro nível	1	UNIDADE
3	598647-8	Serviço de análise de segurança especializada	1	UNIDADE
4	598648-6	Serviço de acompanhamento de reparos	1	UNIDADE
5	598649-4	Serviço de atenção especializada ao cliente	1	UNIDADE
6	598650-8	Service Desk	1	UNIDADE
7	598651-6	Serviço de operação da rede	1	UNIDADE
8	598653-2	Serviço de análise de qualidade	1	UNIDADE
9	598654-0	Serviço de Coordenação do CIISC	1	UNIDADE
10	598655-9	Núcleo de Redes e Segurança Setorial	5	UNIDADE
11	602102-6	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCSs)	22	UNIDADE
12	598656-7	Serviço de Evolução da Maturidade em Segurança da Informação	1	UNIDADE

6.1. Serviço de resposta à incidentes de cibersegurança sob demanda

Para estimativa de horas a serem consumidas de resposta a incidentes foi realizado um levantamento de quantos incidentes aconteceram num período de seis meses (março/2024 - agosto/2024) e quantas horas foram consumidas para resolução dos incidentes. Abaixo o levantamento:

- Março - 0 incidentes - 0h0min
- Abril - 3 incidentes - 19h20min
- Maio - 1 incidente - 03h23min
- Junho - 6 incidentes - 1705h56min
- Julho - 7 incidentes - 92h

- Agosto - 2 incidentes - 92h55min

Total: 19 incidentes - 1.913h34min

Média: 3 incidentes - 318h

#### **6.2. Serviço de análise de segurança de primeiro nível**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.3. Serviço de análise de segurança especializada**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.4. Serviço de acompanhamento de reparos**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.5. Serviço de atenção especializada ao cliente**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.6. Service Desk**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.7. Serviço de operação da rede**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.8. Serviço de análise de qualidade**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.9. Serviço de Coordenação do CIISC**

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

#### **6.10. Núcleo de Redes e Segurança Setorial**

O quantitativo estimado de 05 unidades para o Núcleo de Redes e Segurança Setorial foi definido com base na necessidade atual de monitoramento setorial, para atendimento de alguns dos clientes mais críticos como SEFAZ, SEE, ATI, SES e DETRAN, ou em potencial PCPE, SDS, PMPE, MPPE e TJPE.

#### **6.11. Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCSs)**

Item planejado para expansão sob demanda, para garantir escalabilidade e flexibilidade na operação, este item foi criado para permitir ampliação das unidades de monitoramento, conforme necessidade dos CONTRATANTES aderentes. O quantitativo estimado de 22 unidades para o Serviço Adicional de Monitoramento do Núcleo de Redes e Segurança Setorial foi definido com base na necessidade de escalabilidade e flexibilidade operacional ao longo da vigência contratual, atendendo aos diferentes perfis e portes dos Contratantes Aderentes. Quanto à definição do

quantitativo de 22 unidades para o Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial, foi pensado para contratação de 18 unidades para a SEE, 3 unidades para a PCPE e 1 unidade para a PMPE, visando atender ao parque completo do órgão após contratação do item Núcleo de Redes e Segurança Setorial.

#### 6.12. Serviço de Evolução da Maturidade em Segurança da Informação

Necessário a contratação de 1 serviço para atender a demanda de operação de segurança da operação.

### 7) ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598691-5	Serviço de Comunicação Unificada - SCU (Conta de usuário)	500	UNIDADE

#### 7.1. Serviço de Comunicação Unificada - SCU (Conta de usuário)

O Serviço de Comunicação Unificada (SCU) constitui um componente estratégico e inovador da Nova Rede Corporativa do Estado de Pernambuco, concebido para integrar os diversos canais de comunicação institucional (voz, vídeo, mensagens instantâneas e conferência), promover mobilidade funcional e aumentar a produtividade organizacional dos órgãos e entidades do Poder Executivo Estadual.

Atualmente, não há solução institucionalizada de comunicação unificada no Governo do Estado, o que reforça a necessidade de implantação gradual, planejada e financeiramente sustentável, de modo a garantir integração sistêmica, padronização tecnológica e aderência às boas práticas de governança em TIC.

O dimensionamento inicial do SCU foi definido com base nos resultados da Pesquisa de Demanda (SEI nº [69510789](#)), a qual registrou 10.395 solicitações formais de contas de usuários.

Entretanto, a análise histórica do contrato PE-CONECTADO II demonstrou que, embora houvesse previsão contratual de 15.000 licenças de comunicação unificada, apenas 8 licenças foram efetivamente contratadas ao longo de sua vigência, o que evidencia baixa maturidade de adoção desse tipo de solução no ambiente administrativo estadual.

Considerando esse cenário e a necessidade de preservar o equilíbrio técnico-operacional e orçamentário do projeto, foi definido o quantitativo inicial de **500 contas de usuário**, valor que permite implantação piloto controlada e validação gradual do modelo de uso, evitando custos ociosos e assegurando escalabilidade progressiva conforme a adesão dos órgãos.

Importante destacar que a Lei nº 14.133/2021 assegura flexibilidade contratual para ampliação futura de quantitativos, caso haja adesão crescente dos órgãos à solução, sem a necessidade de novo processo licitatório, desde que observados os limites legais de acréscimo e a disponibilidade orçamentária.

Dessa forma, o quantitativo proposto de **500 licenças** representa uma projeção tecnicamente prudente e financeiramente equilibrada, conciliando inovação tecnológica, responsabilidade fiscal e potencial de expansão, e permitindo a implantação gradual e sustentável do SCU, plenamente alinhada à realidade administrativa, orçamentária e de maturidade tecnológica do Estado de Pernambuco.

**8) ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE**

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598696-6	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)	7000	UNIDADE
2	598697-4	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	8000	UNIDADE
3	598698-2	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	202	UNIDADE
4	598699-0	Serviço de Ponto de Voz Fixo com aparelho de Voz DECT IP (PVF-DECT IP)	354	UNIDADE
5	598700-8	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)	3298	UNIDADE
6	598701-6	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)	500	UNIDADE
7	598703-2	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)	203	UNIDADE
8	598704-0	Serviço PVF-Fone-de-Cabeça	1223	UNIDADE
9	463377-6	Serviço Fixo Inter Estadual	364	MINUTO
10	467295-0	Serviço Fixo Intra Estadual	15303	MINUTO
11	467296-8	Serviço Fixo Local	84960	MINUTO
12	467297-6	Serviço Móvel Intra Estadual	137450	MINUTO
13	467300-0	Serviço Móvel Local	575533	MINUTO
14	467302-6	Serviço Móvel VC2	23051	MINUTO
15	467303-4	Serviço Móvel VC3	802	MINUTO
16	467304-2	Serviço Longa Inter Regional Fixo	475	MINUTO
17	598664-8	Serviço de interface de tronco SIP (SIP TRUNK)	21	UNIDADE

**8.1. Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)**

**8.2. Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)**

**8.3. Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)**

**8.5. Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)**

O dimensionamento dos Serviços de Ponto de Voz Fixo (PVF), previstos no Adendo XIII do Termo de Referência, foi definido com base em uma análise técnico-operacional e estatística da planta de telefonia atualmente instalada, complementada por dados reais de utilização de ramais e pelas tendências de modernização tecnológica e mobilidade corporativa observadas em ambientes públicos e privados.

Conforme a base extraída “Serviço de Ponto de Voz Fixo – 29/10/2025” (SEI nº [76077388](#)), que apontou 20.473 PVFs ativos, aplicou-se um filtro técnico para identificar os serviços com equivalência funcional entre o contrato atual (PE-Conectado II) e a Nova Rede Corporativa, possibilitando a consolidação do dimensionamento. A partir dessa base, obteve-se o seguinte quadro quantitativo:

Tipos de Aparelhos	Contagem de Ramal
Analógico	10867
Analógico Sem Fio	8199
Digital Básico	979
IP Básico	130
Digital Especial	114
Software	20
<b>Total Geral</b>	<b>20309</b>

Com base nesses resultados, realizou-se uma **redução marginal** de 20.309 para **19.699 unidades**, ajustando os quantitativos à realidade de uso e às diretrizes orçamentárias da contratação.

**Premissas da Redução e Ajuste de Quantitativos**

A decisão técnica foi fundamentada nas seguintes premissas:

- **Racionalização de custos e otimização de recursos**, com redução marginal de aproximadamente 3% da base instalada;
- **Tendência de migração para soluções de mobilidade**, softphones e comunicação unificada (UC), reduzindo gradualmente a dependência da telefonia fixa tradicional;
- **Flexibilidade tecnológica e contratual**, permitindo que cada órgão selecione a modalidade de PVF mais adequada ao seu perfil operacional;

- **Adoção de práticas de transformação digital**, em conformidade com a Estratégia de Governo Digital e as diretrizes de modernização da Administração Pública Estadual.

#### Distribuição dos Quantitativos por Modalidade

Com o objetivo de refletir a diversidade de perfis de uso e aproveitar as reduções de forma equilibrada, os serviços foram redistribuídos conforme o quadro a seguir:

Serviço	Descrição Técnica e Finalidade	Quantidade Definida
<b>PVF Wi-Fi IP Móvel</b>	Solução para usuários que demandam mobilidade total, operando exclusivamente via rede Wi-Fi, sem cabeamento físico.	<b>8.199 unidades</b>
<b>PVF Wi-Fi IP Mesa Tipo I</b>	Aparelho de mesa híbrido (Wi-Fi + Ethernet), adequado a ambientes administrativos convencionais.	<b>8.000 unidades</b>
<b>PVF Wi-Fi IP Mesa Tipo II</b>	Aparelho de mesa com recursos avançados e maior resiliência, mantendo conectividade híbrida.	<b>202 unidades</b>
<b>PVF Software</b>	Softphone em computadores/dispositivos móveis, substituindo aparelhos físicos; indicado para ambientes colaborativos, coworking e trabalho híbrido.	<b>3.298 unidades</b>
<b>Subtotal PVF</b>		<b>19.699 unidades</b>

#### Justificativas Técnicas Específicas por Modalidade

- **PVF Wi-Fi IP Móvel:** dimensionado com o mesmo quantitativo do serviço Analógico Sem Fio (**8.199 unidades**), dada a equivalência funcional e a característica principal de mobilidade do usuário, possibilitando inclusive compartilhamento entre colaboradores do mesmo setor.
- **PVF Wi-Fi IP Mesa Tipo I:** estimado com base na diferença entre os ativos atuais e os quantitativos migrados para as demais modalidades, com redução marginal de 3% para adequação financeira, resultando em **8.000 unidades**.
- **PVF Wi-Fi IP Mesa Tipo II:** destinado ao atendimento de perfis executivos e estratégicos da Administração Pública Estadual, conforme parâmetros definidos no processo SEI nº 0001200180.000889/2023-83 – Estudo Técnico Preliminar TIC (ETP) – Anexo IV (SEI nº 62772122). O quantitativo de **202 unidades** reflete a necessidade dos cargos em comissão vinculados aos níveis GOV (Governadora e Vice-Governadora) e DAS/DAS-1, conforme Lei nº 18.487/2024, Decreto nº 42.907/2016 e Portaria SAD nº 833/2026.

- **PVF Software (Softphone):** definido em **3.298 unidades**, sendo 3.000 destinadas à migração planejada a partir das modalidades de maior custo unitário (como o PVF Wi-Fi IP Mesa Tipo I) e 298 unidades provenientes da Pesquisa de Demanda (SEI nº 69510789). A solução, de baixo custo e alta flexibilidade, permite otimizar a comunicação institucional, especialmente em ambientes colaborativos, coworkings, teletrabalho e escritórios descentralizados.

### Serviços Complementares

Além das modalidades principais, o escopo contempla soluções complementares destinadas a ampliar a flexibilidade operacional e mitigar eventuais impactos da redução de quantitativos, conforme descrito abaixo:

Serviço Complementar	Descrição	Quantidade
<b>PVF DECT IP</b>	Solução de voz sem fio voltada a ambientes que exigem mobilidade local (ex.: atendimento ao público, áreas operacionais e serviços de campo).	<b>354 unidades</b>
<b>PVF Virtual</b>	Terminal lógico vinculado ao Serviço de Comunicação Unificada (SCU), permitindo integração direta entre voz, vídeo e colaboração.	<b>500 unidades</b>

Dessa forma, a nova modelagem permite ao Governo do Estado de Pernambuco dispor de um **total potencial de até 20.553** Pontos de Voz Fixa (19.699 + 354 + 500), distribuídos em diferentes modalidades tecnológicas, assegurando:

- Alinhamento à política de transformação digital e à adoção de soluções de comunicação unificada (UC);
- Eficiência financeira e operacional, com redução de custos sem perda de qualidade ou funcionalidade;
- Transição gradual e planejada da telefonia convencional para tecnologias Wi-Fi, IP e softphones;
- Aderência aos princípios da economicidade, eficiência e continuidade do serviço público, conforme estabelecido na Lei nº 14.133/2021;
- Mitigação de riscos operacionais e preservação da qualidade de atendimento à população.

O dimensionamento apresentado reflete, portanto, um equilíbrio entre inovação tecnológica, prudência fiscal e sustentabilidade operacional, consolidando a evolução da infraestrutura de voz do Estado de Pernambuco para um modelo digital, escalável e convergente com as metas de governo eletrônico.

### 8.4. Serviço de Ponto de Voz Fixo com aparelho de Voz DECT IP (PVF-DECT IP)

O dimensionamento do Serviço de Ponto de Voz Fixo com Aparelho DECT IP (PVF-DECT IP) foi dimensionado com base nos resultados da Pesquisa de Demanda (SEI nº [69510789](#)), que registrou formalmente a necessidade de **354 unidades**. Considerando o caráter específico dessa tecnologia, optou-se por adotar exatamente o quantitativo apontado na pesquisa, evitando extrapolações.

O PVF-DECT IP atende a cenários em que a mobilidade interna é essencial, mas onde a infraestrutura cabeada ou Wi-Fi apresenta limitações de cobertura ou estabilidade. Trata-se de uma solução adequada, por exemplo, para:

- Áreas externas de prédios públicos, pátios, almoxarifados e centros de distribuição;
- Escolas rurais, unidades em áreas indígenas, quilombolas ou zonas de difícil acesso;
- Hospitais de grande porte, onde a cobertura Wi-Fi não atende com estabilidade todos os setores;
- Ambientes com restrições físicas ou operacionais para instalação de cabeamento estruturado ou rede Wi-Fi.

O uso da tecnologia **DECT IP** traz benefícios relevantes:

- Operação em frequência dedicada, distinta da rede Wi-Fi, com menor interferência;
- Maior estabilidade e qualidade de chamadas em deslocamentos;
- Roaming transparente em grandes áreas.

Do ponto de vista econômico, o custo unitário identificado no mapa de preços (SEI nº [69512608](#)), de R\$ 136,62, é competitivo frente a soluções de PVF Wi-Fi IP, justificando sua adoção em escala reduzida e dirigida a aplicações específicas de maior benefício operacional.

A decisão de manter o quantitativo de 354 unidades reflete:

- Uma estratégia conservadora, reconhecendo que a tecnologia DECT IP, embora altamente útil para certos contextos, não é aplicável de forma ampla em toda a estrutura do Governo;
- Adoção escalável e controlada, permitindo que os órgãos utilizem a tecnologia em ambientes onde sua aplicação oferece o melhor custo-benefício;
- Alinhamento com o princípio da economicidade, evitando contratações em excesso que poderiam resultar em ociosidade de ativos.

Além disso, eventuais necessidades de expansão poderão ser atendidas durante a vigência contratual, conforme os instrumentos previstos na Lei nº 14.133/2021, dentro dos limites legais de acréscimos.

Assim, a inclusão do PVF-DECT IP no portfólio da Nova Rede Corporativa amplia a flexibilidade tecnológica do Estado, oferecendo uma solução sob medida para contextos desafiadores e garantindo continuidade dos serviços públicos com eficiência e racionalidade.

## 8.6. Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)

A definição dos quantitativos do Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual) foi fundamentada em sua dependência funcional direta do Serviço de Comunicação Unificada (SCU), atuando como terminal lógico vinculado à licença de usuário SCU.

Na Pesquisa de Demanda (SEI nº [69510789](#)), foram registradas **197 solicitações** para o serviço PVF-Virtual, número consideravelmente inferior às **500 licenças de SCU** previstas para contratação. Sob o ponto de vista técnico, essa diferença não se sustenta, uma vez que a funcionalidade de voz no SCU depende necessariamente do PVF-Virtual.

A discrepância entre as solicitações decorre, portanto, do desconhecimento técnico de parte dos gestores, que não associaram corretamente o PVF-Virtual como requisito funcional do SCU, e não de ausência de necessidade operacional.

Dessa forma, foi definido o quantitativo de **500 unidades**, em alinhamento integral ao número de licenças SCU previstas, assegurando coerência técnica e funcional entre os serviços e eliminando risco de subdimensionamento.

A inclusão do PVF-Virtual, ainda não contemplado no ETP anterior (SEI nº [55038477](#)), reflete a modernização da arquitetura de comunicação do Estado, alinhada às melhores práticas de comunicação unificada adotadas no setor privado e em outros entes públicos.

A decisão está amparada pelos seguintes pontos:

- **Dependência funcional direta** – o PVF-Virtual é o terminal lógico necessário para ativação da funcionalidade de voz em cada licença SCU;
- **Demanda subnotificada** – gestores podem não ter declarado corretamente o quantitativo de PVF-Virtual na pesquisa, por desconhecimento da tecnologia;
- **Adoção da maior base projetada** – para evitar restrições contratuais, o quantitativo foi alinhado ao total de SCU, garantindo que todas as licenças possam contar com terminais virtuais, se necessário.

A implantação do PVF-Virtual possibilita:

- Integração nativa com a plataforma SCU, garantindo uniformidade operacional e experiência de usuário aprimorada;
- Redução de custos operacionais, substituindo a necessidade de infraestrutura física de telefonia tradicional;
- Mobilidade e resiliência, permitindo o uso de ramais e funcionalidades de voz em qualquer localidade conectada à Nova Rede Corporativa.

Dessa forma, o quantitativo de 500 unidades de PVF-Virtual é tecnicamente coerente, operacionalmente necessário e estrategicamente adequado, assegurando a plena utilização da solução SCU, a interoperabilidade entre voz e dados e a sustentabilidade financeira do projeto.

## 8.7. Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)

## 8.8. Serviço PVF-Fone-de-Cabeça

Os serviços **PVF – Fone de Cabeça sem fio** e **PVF – Fone de Cabeça** com fio foram dimensionados com base nos resultados da Pesquisa de Demanda (SEI nº [69510789](#)), sem extrapolações estatísticas, refletindo exclusivamente as necessidades formais manifestadas pelos órgãos e entidades estaduais.

O Serviço Headset sem fio foi definido como componente essencial para garantir eficiência operacional e ergonomia em ambientes que exigem mobilidade interna, multitarefas e conforto auditivo prolongado. Essa modalidade é especialmente indicada para centros de comando, helpdesks, contact centers, centrais de atendimento remoto e posições de monitoramento contínuo, onde o operador precisa de liberdade de movimento sem perda de conectividade com o sistema de telefonia IP.

Por sua vez, o Serviço PVF – Fone de Cabeça com fio destina-se a estações fixas de trabalho, em que não há necessidade de mobilidade, mas onde é indispensável assegurar qualidade de áudio, isolamento de ruído e conforto er-

gonômico durante o uso intensivo de telefonia. Essa modalidade apresenta custo reduzido e menor demanda de manutenção, sendo adequada a ambientes administrativos, secretarias e unidades operacionais de suporte.

Ambos os serviços são complementares e indispensáveis para assegurar a plena operação da telefonia IP na Nova Rede Corporativa, garantindo que os Pontos de Voz Fixo (PVFs) sejam utilizados com qualidade, estabilidade e segurança acústica, em conformidade com os padrões técnicos e operacionais definidos no Adendo XIII do Termo de Referência.

A Pesquisa de Demanda consolidou a seguinte necessidade formal:

Item de Serviço	Quantidade Pesquisa de Demanda
Headset sem fio (PVF-sem fio Fone de Cabeça)	203
PVF-Fone-de-Cabeça	1.223

Esses quantitativos foram adotados integralmente, sem extrapolação, visto que o histórico do contrato PE-Conectado II demonstra 158 unidades contratadas apenas para fones de cabeça com fio, o que valida a ordem de grandeza e a proporcionalidade das novas estimativas.

A inclusão dos serviços de headset, tanto com fio quanto sem fio, está tecnicamente justificada pelos seguintes fatores:

- Requisitos de ergonomia e saúde ocupacional, reduzindo fadiga e melhorando a produtividade em postos de atendimento;
- Aprimoramento da qualidade de áudio e isolamento acústico, especialmente em ambientes ruidosos;
- Adequação às boas práticas de telefonia IP corporativa, conforme normas internacionais de conforto e desempenho;
- Compatibilidade plena com os dispositivos PVF Wi-Fi IP e com a arquitetura de Comunicação Unificada (SCU), permitindo interoperabilidade total;
- Escalabilidade: possibilidade de ampliação futura conforme o crescimento do número de ramais e centros de atendimento.

A adoção de 1.426 unidades no total (203 sem fio + 1.223 com fio) representa uma estimativa técnica equilibrada, assegurando:

- Condições ergonômicas adequadas para os usuários dos PVFs;
- Eficiência operacional e produtividade ampliada em ambientes críticos;
- Custo-benefício otimizado, respeitando o histórico contratual e as demandas reais;
- Aderência aos princípios da economicidade, eficiência e continuidade dos serviços públicos.

Assim, os serviços PVF – Fone de Cabeça sem fio e PVF – Fone de Cabeça com fio complementam o ecossistema de comunicação da Nova Rede Corporativa, garantindo desempenho acústico, conforto, confiabilidade no uso diário da telefonia IP estadual, continuidade dos serviços públicos e mitigação de riscos contratuais.

#### 8.9. Serviço Fixo Inter Estadual

#### 8.10. Serviço Fixo Intra Estadual

#### 8.11. Serviço Fixo Local

#### 8.12. Serviço Móvel Intra Estadual

#### 8.13. Serviço Móvel Local

#### 8.14. Serviço Móvel VC2

#### 8.15. Serviço Móvel VC3

#### 8.16. Serviço Longa Inter Regional Fixo

Os itens 8.9 a 8.16 referem-se ao Tráfego Telefônico Extrarrede Reverso de telefonia DDG (Discagem Direta Gratuita), tráfego de chamadas 0800, cuja definição dos quantitativos foi fundamentada através do comportamento de consumo da Administração Pública Estadual ao longo do período de dez23 até abr25, adquirido através de solicitação realizada para Operação Integrada do PE-Conectado II sob a solicitação SOL 804160. Para isso, foi realizada a consolidação do total de chamadas recebidas em números 0800 ativos nos diversos órgãos e entidades estaduais, considerando-se os registros efetivos de uso mês a mês. Tal abordagem garante uma visão atualizada, realista e precisa da demanda efetiva, uma vez que se baseia em dados operacionais recentes e diretamente vinculados às atividades executadas.

Como critério técnico central, adotou-se como referência o mês de maior tráfego registrado no referido período por item de serviço. Esta decisão foi motivada pela constatação, a partir da análise dos dados, de que há variações significativas no volume de chamadas entre os meses, decorrentes de fatores sazonais, campanhas institucionais, situações emergenciais, programas governamentais específicos ou picos de demanda não recorrentes, mas que fazem parte do contexto operacional do Estado. Assim, utilizar a média anual poderia subdimensionar o contrato, colocando em risco a continuidade dos serviços de atendimento ao cidadão em momentos de maior necessidade.

Portanto, a metodologia adotada priorizou garantir que o contrato seja capaz de suportar, desde sua implementação, os volumes de tráfego compatíveis com o cenário de maior exigência já observado, mitigando riscos de falhas operacionais, indisponibilidades ou necessidade de aditivos emergenciais. Essa estratégia permite assegurar a estabilidade dos serviços, a previsibilidade orçamentária e a eficiência no atendimento às políticas públicas, mantendo a Administração preparada para absorver tanto a demanda ordinária quanto os picos sazonais de utilização.

É importante destacar que, para além da manutenção da operação atual, a escolha do mês de maior tráfego como parâmetro assegura também escalabilidade, considerando o dinamismo das atividades governamentais e a possibilidade de surgimento de novas demandas ao longo da vigência contratual. Dessa forma, os quantitativos definidos refletem não apenas o histórico de utilização, mas também um planejamento robusto, alinhado às melhores práticas de gestão pública e aos princípios da economicidade, da eficiência e da continuidade dos serviços essenciais.

Os dados consolidados que fundamentaram essa definição encontram-se detalhados na tabela abaixo e no **Relatório Tarifação de consumo serviço 0800 - dez23 à abr25** (SEI nº [73831138](#)), que apresenta o volume total de chamadas por mês no período de dez23 até abr25, servindo como base técnica para as análises que determinaram os quantitativos finais deste ETP, na terceira coluna "Arredondamento p/ N° Inteiro".

ITEM SERVI ÇO E- FISCO	Uni dad e	Arredond amento p/ N° Inteiro	Mai or Tráf ego	dez- 23	jan- 24	fev- 24	mar- 24	abr- 24	mai- 24	jun- 24	jul- 24	ago- 24	set- 24	out- 24	nov- 24	dez- 24	jan- 25	fev- 25	mar- 25	abr- 25
---------------------------------	-----------------	----------------------------------------	--------------------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------

Serviço fixo interestadual	Min	364	363,6	211,40	213,10	206,20	363,60	250,50	195,30	239,60	167,30	252,50	299,80	207,30	182,90	224,70	130,10	126,90	98,60	58,20
Serviço fixo intraestadual	Min	15303	15302,4	15302,40	14683,90	12834,20	12899,30	10362,90	11733,10	11211,10	9120,60	7368,60	8028,50	7714,70	6372,10	7686,50	6636,20	6828,40	6486,30	7651,20
Serviço fixo local	Min	84960	84959,6	68694,70	68153,90	59209,00	84959,60	58543,50	55355,40	57779,30	60620,20	46835,40	50045,80	51471,60	47378,60	58687,50	46517,50	32722,10	37594,40	35482,00
Serviço móvel intraestadual	Min	137450	137449,8	106619,70	91949,40	90096,60	106970,50	96733,40	97666,80	77690,20	70096,70	71722,80	82041,50	86645,50	77754,40	110062,50	107320,00	137449,80	115532,90	123122,30
Serviço móvel local	Min	575533	575532,5	386354,50	498114,70	433306,00	575532,50	449654,60	501710,00	447898,70	314346,70	329751,70	305467,60	335686,00	305894,00	373390,90	378667,10	503782,90	489270,90	523471,00
Serviço móvel VC2	Min	23051	23051	8,00	3103,30	3262,60	6628,60	3692,20	23051,00	11427,10	8537,10	435,20	427,40	591,00	329,50	604,70	388,90	353,30	456,90	430,60
Serviço móvel VC3	Min	802	801,4	20,40	479,30	426,30	465,40	472,10	553,60	607,90	323,10	381,70	648,20	476,70	512,90	449,50	450,00	461,30	739,00	704,00
Serviço longa inter regional fixo	Min	475	474,4	300,50	292,90	357,20	458,30	297,00	350,90	474,40	417,60	410,90	178,80	314,20	206,50	184,90	133,10	83,40	77,10	123,70

### 8.17. Serviço de interface de tronco SIP (SIP TRUNK)

O dimensionamento do Serviço Adicional de Acesso SIP (SIPTRUNK) foi fundamentado em critérios objetivos derivados da Pesquisa de Demanda (SEI nº [69510789](#)), que registrou a necessidade formal de **20 unidades**. Esse quantitativo foi acrescido em **01 unidade**, correspondente ao acesso já em uso na ATI por meio do contrato PE-Conectado II, totalizando **21 unidades** no Termo de Referência (TR).

Esse serviço possui caráter especializado e de aplicação pontual, sendo utilizado principalmente:

- para integração de redes de telefonia legadas com plataformas VoIP;
- para garantir escalabilidade e flexibilidade em órgãos que mantêm PABX IP próprios;
- para assegurar continuidade de serviços críticos que demandam interoperabilidade com redes externas.

Considerando o uso consolidado no âmbito do contrato vigente (PE-Conectado II) e as perspectivas de evolução tecnológica, optou por manter o quantitativo exato da pesquisa acrescido do link funcional da ATI. Essa decisão está alinhada às seguintes constatações:

- trata-se de um serviço de demanda restrita, concentrada em órgãos com arquitetura de telefonia específica, não sendo solução de uso massivo;
- há uma tendência irreversível de migração para soluções nativas de comunicação unificada em IP, reduzindo gradativamente a necessidade de acessos SIP independentes;
- a manutenção no portfólio da Nova Rede Corporativa permanece essencial para garantir flexibilidade técnica, sobretudo em períodos de transição entre ambientes legados e soluções modernas.

Além disso, é importante destacar que o SIPTRUNK oferece vantagens operacionais significativas, como:

- Redução de custos operacionais, substituindo troncos convencionais TDM por uma infraestrutura baseada em IP;
- Facilidade de gerenciamento e controle, com integração direta às plataformas de telefonia IP existentes nos órgãos;
- Escalabilidade técnica, permitindo ajustes de capacidade de acordo com a demanda de tráfego de voz, sem necessidade de intervenções físicas ou alterações na infraestrutura básica de rede;
- Interoperabilidade garantida com a comunicação externa e outros ambientes governamentais que ainda operam soluções baseadas em PABX ou redes TDM.

Dessa forma, o quantitativo de 21 unidades encontra-se tecnicamente fundamentado no uso histórico, nas manifestações da pesquisa de demanda e na estratégia de assegurar uma operação estável, eficiente e escalável, em plena conformidade com os princípios da economicidade, eficiência e continuidade dos serviços públicos.

#### 9) ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598657-5	Serviço de Contact Center com Recurso de Voz	250	UNIDADE
2	598658-3	Serviço de Contact Center com recurso de Whatsapp	400	UNIDADE
3	598659-1	Serviço de Contact Center com recurso de Redes Sociais	50	UNIDADE
4	598660-5	Serviço de Unidade de Resposta Audível (URA)	100	UNIDADE
5	598661-3	Serviço de Comunicação por vídeo ou vídeo-chamada	60	UNIDADE
6	598662-1	Serviço de Automatizações e Integrações - Consultoria Inicial	5	UNIDADE

7	598663-0	Serviço de Automatizações e Integrações - Implantação	100	UNIDADE
---	----------	-------------------------------------------------------	-----	---------

**9.1. Serviço de Contact Center com Recurso de Voz**

**9.2. Serviço de Contact Center com recurso de Whatsapp**

**9.3. Serviço de Contact Center com recurso de Redes Sociais**

**9.4. Serviço de Unidade de Resposta Audível (URA)**

**9.5. Serviço de Comunicação por vídeo ou vídeo-chamada**

**9.6. Serviço de Automatizações e Integrações - Consultoria Inicial**

**9.7. Serviço de Automatizações e Integrações - Implantação**

O dimensionamento dos serviços previstos no Adendo XIV – Serviço de Infraestrutura de Tecnologia para Contact Center foi conduzido com o objetivo de assegurar a continuidade operacional dos atendimentos atualmente executados sob o contrato PE-CONNECTADO II, evitando descontinuidade de serviços públicos, riscos operacionais e impactos à população.

A definição dos quantitativos está alinhada às diretrizes estratégicas e financeiras do Governo do Estado de Pernambuco, que priorizam a modernização do atendimento público, a ampliação dos canais digitais e a otimização de custos operacionais, conforme o documento “Informação 3 – Resumo dos Processos” (SEI nº [72965319](#)).

**Metodologia de Dimensionamento**

O processo de definição dos quantitativos foi estruturado com base em três eixos complementares de análise:

- 1. Base de Dados e Pesquisa de Demanda Real**  
Os quantitativos consideram a operação real, preservando a capacidade de atendimento e a escalabilidade da solução, e a demanda formalmente registrada, ajustando a previsão para refletir o uso efetivo e o histórico dos serviços vigentes no PE-CONNECTADO II.
- 2. Análise de Tendência Tecnológica e Omnicanalidade**  
Foram observadas as tendências de transformação digital e os avanços nos modelos omnichannel, que integram múltiplos canais de comunicação (voz, WhatsApp, redes sociais, vídeo e URA), promovendo maior acessibilidade, inclusão e eficiência.
- 3. Critério Orçamentário e Sustentabilidade Financeira**  
Adotou-se uma modelagem conservadora e escalável, assegurando equilíbrio orçamentário e capacidade de expansão gradual, conforme a adesão dos órgãos e a maturidade tecnológica da Administração Pública.

**Objetivos e Benefícios do Serviço**

A nova infraestrutura de Contact Center tem como propósito modernizar o atendimento ao cidadão, substituindo gradualmente o modelo telefônico tradicional por uma plataforma omnichannel integrada e inteligente, com os seguintes benefícios:

- Melhoria da experiência do cidadão, atendimento multicanal e unificado, com integração entre voz, chat, vídeo, redes sociais e mensageria;

- Redução de filas e tempos de espera, por meio de chatbots, IA, URA inteligente e possibilidade de integração com sistemas legados;
- Aumento da produtividade dos operadores e centralização das interações;
- Rastreabilidade e controle de todo o fluxo de atendimento, conforme requisitos legais e de auditoria;
- Escalabilidade e economia, ampliando o alcance dos serviços sem necessidade de estrutura física adicional.

Essa abordagem está alinhada às melhores práticas de transformação digital do setor público, já consolidadas em diversos entes federativos e respaldadas nas diretrizes e Estratégia de Governo Digital.

Item de Serviço	Quantidade (TR)	Pesquisa de Demanda	Serviços Vigentes (PE- Conectado II) (*)	Observações Técnicas
<b>Contact Center com Voz</b>	250	368	245	Mantém o parque operacional atual, assegurando a continuidade dos serviços de voz ativos (SES, SAD, TCE, Sec. da Mulher e TJPE), com margem para expansão controlada e migração gradual para canais digitais.
<b>Contact Center com WhatsApp</b>	400	367	–	Atende integralmente à demanda apurada, com acréscimo de 10% para órgãos não respondentes, contemplando o crescimento do canal mais demandado nas interações com o cidadão.
<b>Contact Center com Redes Sociais</b>	50	115	–	Reduzido para refletir o estágio inicial de adoção e a capacidade operacional dos órgãos, permitindo implantação piloto e expansão conforme maturidade digital.
<b>Unidade de Resposta Audível (URA)</b>	100	74	30	Garante a manutenção das URAs ativas no PE-CONNECTADO II (TJPE e SES) e atende aos órgãos que responderam a Pesquisa de Demanda.
<b>Comunicação por Vídeo/Vídeo-Chamada</b>	60	154	–	Ajuste para compatibilizar com o uso efetivo e capacidade operacional, considerando implantação gradual e

				financeiramente equilibrada.
<b>Automatizações e Integrações – Consultoria Inicial</b>	5	15	–	Ajuste para compatibilizar com o uso efetivo e capacidade operacional, considerando implantação gradual e financeiramente equilibrada.
<b>Automatizações e Integrações – Implantação</b>	100	116	–	Ajuste para compatibilizar com o uso efetivo e capacidade operacional, considerando implantação gradual e financeiramente equilibrada.

(\*) Atualmente, o Estado mantém os seguintes serviços ativos no Contrato PE-CONNECTADO II:

- Contact Center com Voz: 245 unidades — SES (161), SAD-Sede (20), TCE-Sede (15), Sec. da Mulher (8) e TJPE (41);
- Unidade de Resposta Audível (URA): 30 unidades — TJPE (15) + SES (15).

Esses serviços serão integralmente mantidos e migrados gradualmente para o novo modelo omnichannel, sem interrupção de atendimento.

Por fim, o dimensionamento proposto no Adendo XIV garante:

- **Continuidade operacional** dos serviços hoje existentes;
- **Modernização gradual** da infraestrutura, com foco na integração de canais digitais;
- **Eficiência operacional**, permitindo expansão sob demanda;
- **Equilíbrio orçamentário e sustentabilidade financeira**, aderência à Lei nº 14.133/2021, especialmente aos princípios da economicidade, eficiência e continuidade dos serviços públicos;
- **Segurança jurídica e previsibilidade contratual**, mitigando riscos de subdimensionamento e evitando sobrecustos.

Assim, os quantitativos definidos representam um equilíbrio entre inovação tecnológica, prudência fiscal e compromisso com a melhoria da experiência do cidadão, consolidando o avanço do Governo de Pernambuco rumo a um modelo digital, acessível, seguro, integrado e centrado no cidadão.

#### 10) ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO DOS SERVIÇOS

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida

1	598640-0	Suporte de Manutenção (12h x 7d)	600	UNIDADE
2	598641-9	Suporte de Manutenção (24h x 7d)	500	UNIDADE

O dimensionamento dos Regimes de Suporte e Manutenção foi elaborado com base em critérios operacionais, estatísticos e econômicos, em conformidade com a nova modelagem técnica da Nova Rede Corporativa, estruturada sob o conceito dos Pontos Conectados Seguros (PCSs).

Essa abordagem considera a integração entre os serviços de conectividade, segurança, rede sem fio e voz, permitindo a racionalização técnica e financeira no gerenciamento dos serviços de suporte e manutenção.

Os regimes 12h x 7d e 24h x 7d foram definidos como opções facultativas, disponíveis para adesão dos órgãos conforme suas necessidades específicas, funcionando como mecanismos de elasticidade contratual para ajustar a disponibilidade de suporte de acordo com a criticidade das operações.

### 10.1. Suporte de Manutenção 12h x 7d

O regime 12h x 7d é uma extensão da configuração padrão obrigatória 12h x 5d, destinada aos órgãos que necessitam de atendimento também aos finais de semana, mas não demandam suporte ininterrupto.

A definição do quantitativo de 600 unidades foi baseada na consolidação de 479 unidades formalmente manifestadas na Pesquisa de Demanda (SEI nº [69510789](#)), representando 37,6% dos órgãos respondentes. Aplicando-se projeção proporcional aos órgãos não respondentes, obteve-se uma estimativa potencial de 1.274 unidades.

Contudo, diante dos limites orçamentários e da incerteza quanto à adesão efetiva dos órgãos que não participaram da pesquisa, optou-se pela contratação prudente de 600 unidades. De acordo com o Mapa de Preços (SEI nº [69512608](#)), essa decisão gera economia mensal estimada de R\$ 186.572,49, equivalente a R\$ 8.955.479,49 ao longo dos 48 meses de vigência contratual — sem comprometer a segurança operacional da rede estadual.

### 10.2. Suporte de Manutenção 24h x 7d

O regime 24h x 7d segue a mesma lógica facultativa, sendo destinado a órgãos cuja missão institucional exige suporte contínuo e ininterrupto, como centros de comando, unidades de segurança pública, estabelecimentos de saúde e datacenters.

A Pesquisa de Demanda (SEI nº [69510789](#)) registrou 362 solicitações formais, e a projeção estatística indicou uma demanda potencial de até 963 unidades.

Para a definição do quantitativo final de 500 unidades, foram observados os seguintes critérios:

- Base contratual vigente: o contrato PE-CONNECTADO II possui 447 sites com esse regime de suporte;
- Acréscimo prudencial de 10%, contemplando órgãos não respondentes e mantendo margem de flexibilidade para atender novas demandas críticas;
- Redução proporcional em relação à projeção total, devido ao custo unitário cerca de quatro vezes superior ao regime 12h x 7d, preservando o equilíbrio financeiro e a sustentabilidade contratual.

Essa decisão técnica proporciona economia mensal de R\$ 462.807,61, equivalente a R\$ 22.214.765,11 em 48 meses. Somando-se ao resultado obtido no item anterior, o impacto financeiro positivo totaliza R\$ 31,17 milhões ao longo da vigência contratual.

A tabela a seguir apresenta o comparativo entre os quantitativos projetados, contratados e os ganhos econômicos estimados:

Serviço	Pesquisa de Demanda (37,6%)	Projeção Total (100%)	Quantidade TR	Valor Unitário – Mapa de Preços (SEI nº 69512608)	Economia Mensal (Projeção – TR)	Economia 48 Meses (Projeção – TR)	Justificativa da Redução
Suporte de Manutenção (12h x 7d)	479	1274	600	R\$ 276,84	R\$ 186.572,49	R\$ 8.955.479,49	Alinhado à pesquisa de demanda e suficiente para atender órgãos não respondentes.
Suporte de Manutenção (24h x 7d)	362	963	500	R\$ 1.000,09	R\$ 462.807,61	R\$ 22.214.765,11	Alinhado à demanda atual (447 sites) e proporcionalmente ampliado em 10% para órgãos não respondentes.

O dimensionamento adotado para os regimes de suporte e manutenção representa um equilíbrio técnico-financeiro entre confiabilidade operacional, sustentabilidade orçamentária e escalabilidade contratual. A estratégia adotada assegura:

- Continuidade dos serviços essenciais, com suporte adequado às demandas de alta criticidade;
- Racionalização de custos, por meio da oferta facultativa e proporcional à adesão efetiva dos órgãos;
- Sustentabilidade contratual e previsibilidade financeira, em conformidade com os princípios da Lei nº 14.133/2021;
- Eficiência operacional e segurança tecnológica, alinhadas à arquitetura integrada da Nova Rede Corporativa.

#### 11) ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
------	-------------------	-------------------	------------	-------------------

1	598287-1	Link de Fibra Lan To Lan (L2L) (Endereços Definidos)	4	UNIDADE
2	598288-0	Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)	3	UNIDADE
3	598289-8	Link para Data Center de 4GB com AntiDDoS - Link Internet Trânsito (LIT)	3	UNIDADE
4	598290-1	Link para Data Center de 6GB com AntiDDoS - Link Internet Trânsito (LIT)	3	UNIDADE
5	598291-0	Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)	3	UNIDADE
6	598292-8	Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)	3	UNIDADE

O dimensionamento dos serviços vinculados ao ADENDO VII – Serviços de Conectividade para Data Center foi realizado com base na análise técnica da infraestrutura atual e das projeções estratégicas do Governo do Estado de Pernambuco para o horizonte de vigência do contrato, que é de 48 meses, podendo ser prorrogado até 120 meses, conforme dispõe a Lei nº 14.133/2021.

#### 11.1. Link de Fibra Lan To Lan (L2L) - para Interconexão de Datacenters

O serviço de Link de Fibra Lan To Lan (L2L) teve seu quantitativo ajustado de 3 para 4 unidades, sendo:

- 3 unidades destinadas aos datacenters atualmente em operação, localizados na ATI, SEE e SEFAZ;
- 1 unidade adicional, provisionada como reserva técnica e operacional, sem endereço previamente definido, porém restrita à Região Metropolitana do Recife.

Esta reserva foi planejada considerando os estudos em andamento que avaliam a instalação de até dois novos datacenters governamentais, com possibilidade de implantação na Secretaria de Saúde (SES) e/ou no DETRAN-PE.

Diante do longo horizonte contratual, é imperativo assegurar que o contrato possua flexibilidade suficiente para absorver futuras expansões da infraestrutura de TI crítica do Estado, que já estão sendo avaliadas, sem necessidade de novos processos licitatórios ou aditivos emergenciais.

Além disso, a previsão da 4ª unidade mitiga riscos operacionais, assegurando que, em caso de expansão da infraestrutura, os novos datacenters estejam imediatamente integrados à malha de interconexão de datacenters do Estado, preservando os padrões de segurança, desempenho e alta disponibilidade estabelecidos no projeto.

- 11.2. Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)
- 11.3. Link para Data Center de 4GB com AntiDDoS - Link Internet Trânsito (LIT)
- 11.4. Link para Data Center de 6GB com AntiDDoS - Link Internet Trânsito (LIT)
- 11.5. Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)
- 11.6. Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)

Para os serviços de conexão com a internet de alta capacidade, protegidos por soluções Anti-DDoS, foram mantidos os quantitativos de 3 unidades por serviço, aplicáveis aos perfis de capacidade de 2Gbps até 10 Gbps.

Esses serviços atendem exclusivamente os datacenters já consolidados (ATI, SEE e SEFAZ) e, neste caso específico, não se faz necessária a previsão de expansão para eventuais novos datacenters, considerando:

- A demanda atual e projetada de consumo de banda e serviços nesses três centros;
- A possibilidade de, futuramente, dimensionar novos contratos específicos de internet para eventuais novos datacenters, considerando que esses serviços são tecnicamente independentes da interconexão Lan To Lan (L2L) entre datacenters;

Isto posto, o modelo adotado assegura:

- Robustez técnica, ao garantir interconexão de datacenters com alta disponibilidade e baixa latência via L2L;
- Escalabilidade controlada, com a previsão da 4ª unidade de L2L antecipando-se a eventuais expansões estratégicas;
- Previsibilidade orçamentária e segurança jurídica, mitigando riscos de subdimensionamento, interrupções operacionais e necessidade de processos licitatórios emergenciais;
- Alinhamento às melhores práticas de governança de TIC, mantendo a sustentabilidade financeira e operacional da rede corporativa do Estado.

Portanto, os quantitativos propostos para os serviços de conectividade de datacenter são tecnicamente adequados, sustentáveis financeiramente e juridicamente respaldados, refletindo tanto a realidade atual quanto as projeções estratégicas do Governo do Estado de Pernambuco.

## 12) ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS

Item	Código do e-Fisco	Descrição do Item	Quantidade	Unidade de Medida
1	598665-6	Serviço de gestão de vulnerabilidades	4200	UNIDADE
2	598666-4	Serviço de análise forense	141	HORA
3	598667-2	Serviço de análise de segurança ofensiva (Red Team)	1	UNIDADE
4	598668-0	Serviço de testes de intrusão (Pentest)	10	UNIDADE

### 12.1. Serviço de gestão de vulnerabilidades

Visa atender a demanda de servidores dos datacenters do estado. A estimativa atual é de cobertura para 4.155 servidores dos datacenters do governo do Estado, sendo 3.349 (três mil, trezentos e quarenta e nove) da ATI, 456 (quatrocentos e cinquenta e seis) da SEE e 350 (trezentos e cinquenta) da SEFAZ.

### 12.2 Serviço de análise forense

Para estimativa de horas a serem consumidas de forense foi realizado um levantamento de mercado (Gartner, Best Practices for Security Operations Centers: Enabling Continuous Improvement, e How to Measure Incident Response Effectiveness / Forrester, The Forrester Wave: Security Incident Response Services, Q1 2020 e State of Security Operations 2021) alinhado com os principais frameworks de segurança da informação (NIST SP 800-61 / ISO/IEC 27035 / SANS Institute - Incident Response & Forensics Guidelines). Abaixo o levantamento:

- Coleta de evidências e preservação - 5h a 15h por incidente
- Análise de evidências e Correlação - 10h a 20h por incidente
- Relatório forense e documentação - 5h a 10h por incidente
- Reuniões e revisões pós-incidente - 1h a 2h por incidente

Considerando a média de 3 incidentes mensais, teremos uma estimativa de no mínimo 63h e máximo de 141h de análise forense por mês, dito isso, optamos por considerar o máximo estimado para o projeto para garantir a capacidade de resposta em períodos de maior demanda, assegurando continuidade na investigação de incidentes críticos e mantendo a integridade e rastreabilidade das infraestruturas governamentais.

### 12.3. Serviço de análise de segurança ofensiva (Red Team)

Necessário a contratação de 1 equipe para atender a demanda de operação de segurança da operação.

### 12.4. Serviço de testes de intrusão (Pentest)

Necessário a contratação de 1 serviço que atenda a 10 aplicações por mês para atender a demanda de operação de segurança de aplicações do estado.

## 8. ANÁLISE COMPARATIVA DAS SOLUÇÕES

A seguir, apresentamos uma análise crítica das diferentes soluções consideradas, levando em conta não apenas o aspecto econômico, mas também os aspectos qualitativos que contribuem para o alcance dos objetivos da contratação. Para facilitar a avaliação, a tabela a seguir oferece uma comparação dos principais requisitos entre as soluções identificadas.

Requisitos	Cenários			
	Cenário 1	Cenário 2	Cenário 3	Cenário 4

Negócio	NN 01	atende	atende	atende	atende
	NN 02	atende	atende	atende	atende
	NN 03	atende	atende	atende	atende
	NN 04	atende	atende	atende	atende
	NN 05	atende	atende	atende	atende
	NN 06	atende	atende	atende	atende
	NN 07	atende	atende	atende	atende
	NN 08	atende	atende	atende	atende
	NN 09	atende	atende	atende	atende
	NN 10	atende	atende	atende	atende
	NN 11	atende	atende	atende	atende
	NN 12	atende	atende	atende	atende
	NN 13	atende	atende	atende	atende
	NN 14	atende	atende	atende	atende
	NN 15	atende	atende	atende	atende
	NN 16	atende	atende	atende	atende
	NN 17	atende	atende	atende	atende
	NN 18	atende	atende	atende	atende
	NN 19	atende	atende	atende	não atende
Tecnológico	NT 01	atende	atende	atende	atende
	NT 02	atende	atende	atende	atende
	NT 03	atende	atende	atende	atende
	NT 04	atende	atende	atende	atende
	NT 05	atende	atende	atende	atende

NT 06	atende	atende	atende	atende
NT 07	atende	atende	atende	atende
NT 08	atende	atende	atende	atende
NT 09	atende	atende	atende	atende
NT 10	atende	atende	atende	atende
NT 11	atende	atende	atende	atende
NT 12	atende	atende	atende	atende
NT 13	atende	atende	atende	atende
NT 14	atende	atende	atende	atende
NT 15	atende	atende	atende	atende
NT 16	atende	atende	atende	atende
NT 17	atende	atende	atende	atende
NT 18	atende	atende	atende	atende
NT 19	atende	atende	atende	não atende
NT 20	atende	atende	atende	atende
NT 21	atende	atende	atende	atende
NT 22	atende	atende	atende	atende
NT 23	atende	atende	atende	atende
NT 24	atende	atende	atende	atende
NT 25	atende	atende	atende	atende
NT 26	atende	atende	atende	atende
NT 27	atende	atende	atende	atende
NT 28	atende	atende	atende	atende
NT 29	atende	atende	atende	atende

NT 30	atende	atende	atende	atende
NT 31	atende	atende	atende	atende
NT 32	atende	atende	atende	atende
NT 33	atende	atende	atende	atende
NT 34	atende	atende	atende	atende
NT 35	atende	atende	atende	atende
NT 36	atende	atende	atende	atende
NT 37	atende	atende	atende	atende
NT 38	atende	atende	atende	atende
NT 39	atende	atende	atende	atende
NT 40	atende	atende	atende	atende
NT 41	atende	atende	atende	atende
NT 42	atende	atende	atende	atende
NT 43	atende	atende	atende	atende
NT 44	atende	atende	atende	atende
NT 45	atende	atende	atende	atende
NT 46	atende	atende	atende	atende
NT 47	atende	atende	atende	atende
NT 48	atende	atende	atende	atende
NT 49	atende	atende	atende	atende
NT 50	atende	atende	atende	atende
NT 51	atende	atende	atende	atende
NT 52	atende	atende	atende	atende
NT 53	atende	atende	atende	atende

	NT 54	atende	atende	atende	atende
	NT 55	atende	não atende	atende	atende
<b>Resultado da Análise</b>		viável	não viável	viável	não viável

## 9. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

As seguintes soluções foram consideradas inviáveis para o projeto de rede corporativa do Governo de Pernambuco:

- Solução de Rede Corporativa com contratação dos itens de serviço por lotes distintos (Cenário 2)**
- Solução de Rede Corporativa com Segurança em modelo de contratação por Empresa Única ou Consórcio com SASE integrado (Cenário 4)**

Embora ambas apresentem vantagens significativas, enfrentam os seguintes desafios:

- Solução com Lotes Distintos (Cenário 2)**

A segmentação dos lotes compromete a sinergia entre os serviços de segurança, voz, contact center e comunicação unificada, gerando uma falta de coordenação eficiente entre os diversos componentes da rede. Essa fragmentação reduz a eficácia na mitigação de ameaças, aumenta o tempo de resposta a incidentes e dificulta a implementação de medidas corretivas. Além disso, expõe o projeto a riscos como ataques de negação de serviço, invasões direcionadas a serviços críticos e exploração de falhas zero-day, resultando em vulnerabilidades significativas e na incapacidade de responder rapidamente a ataques cibernéticos, colocando o Governo em uma posição de risco. Por exemplo, ataques direcionados ao serviço de voz corporativa podem ter sua mitigação ineficiente se os serviços de voz e de segurança forem desenhados em lotes distintos de um processo licitatório, dificultando a aplicação de contramedidas integradas e rápidas.

- Solução com SASE Integrado (Cenário 4)**

Embora ofereça a vantagem de centralização da segurança na nuvem e maior flexibilidade escalável, a solução com SASE integrado apresenta desafios consideráveis relacionados à previsibilidade de custos. Além dos custos iniciais de implantação, os custos de manutenção variam significativamente com base no uso da Internet, sendo influenciados por fatores como número de usuários, volume de tráfego e aplicações utilizadas. A heterogeneidade nos modelos de precificação entre os diferentes fabricantes torna o desenvolvimento de uma proposta viável mais demorado e complexo, comprometendo a previsibilidade dos custos para o Governo de Pernambuco.

Esses desafios demonstram a necessidade de buscar alternativas que ofereçam uma maior integração e previsibilidade, minimizando riscos operacionais e financeiros ao longo da implementação da rede corporativa.

## 10. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

A fim de proporcionar uma análise criteriosa das opções de contratação, realizamos uma **análise comparativa** entre diferentes itens de contratação para a **Nova Rede Corporativa do Estado de Pernambuco**. Essa análise tem como objetivo fornecer um embasamento **técnico e econômico** que permita a escolha da melhor estratégia de contratação, considerando os cenários viáveis e mais vantajosos para o Estado

As estimativas de custo projetadas ao longo do ciclo de vida das soluções permitiram uma avaliação detalhada dos impactos financeiros para o Estado. A seguir, serão apresentados os cenários propostos, estruturados de forma a refletir seus respectivos custos.

#### Cenários Propostos Viáveis:

**1) CENÁRIO 01:** Solução de Rede Corporativa em modelo de contratação dos itens de serviço com separação em três lotes distintos.

a. 1º Lote: Serviço de Segurança de toda rede + Serviço de conectividade com acessos Banda larga (link principal e redundante) + Solução de voz, contact center e comunicação unificada.

b. 2º Lote: Serviço de conectividade Datacenter e trânsito com AntiDDoS.

c. 3º Lote: Serviço de varredura de vulnerabilidades e análises forense.

**2) CENÁRIO 03:** Solução de Rede Corporativa em modelo de contratação de acesso dedicado (P2P) com ponto único de acesso à Internet e concentradores regionais.

## 10.1.CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

### • Procedimento de Cotação

Como parte do desenvolvimento da **nova rede corporativa do Estado de Pernambuco**, que substituirá a atual **rede PE-Conectado II**, a comissão técnica responsável pela elaboração desta **ETP** buscou, inicialmente, estabelecer uma visão clara sobre os requisitos técnicos e operacionais necessários para garantir uma rede **segura, ultrarrápida e resiliente**. Nesse sentido, elaboramos o **Termo para Cotação**, no qual foram detalhadas as especificações técnicas e os serviços fundamentais para implementar essa rede, abordando aspectos como segurança cibernética, conectividade e resiliência. Além disso, foram disponibilizados dois documentos complementares: a **Tabela de Preços do Termo de Cotação**, que lista os itens de serviço a serem cotados, e o **ANEXO I - LOCALIDADES INSTALADAS**, que inclui a relação completa dos endereços dos sites governamentais onde serão implementados os serviços de conectividade, voz e firewall.

Esses materiais foram enviados a diversas empresas interessadas em participar do processo licitatório. Como resposta, recebemos estimativas de preços de cinco fornecedores: **DB3 (GIGA+)**, **NTSec**, **OI**, **FBR Digital** e o consórcio **Brisanet**, **Inorpel** e **BidWeb**. Cada um desses fornecedores apresentou suas cotações, cobrindo os itens descritos no **Termo de Cotação**. Essas propostas iniciais serviram como base para a análise financeira que sustenta este **ETP** e permitiram o refinamento da estratégia de contratação a ser aplicada na futura licitação, visando garantir uma escolha eficiente e transparente. Para garantir a representatividade dos preços de mercado e minimizar distorções, foi utilizada a média das cotações recebidas.

Cabe destacar que, para a **cotação dos serviços de voz**, utilizou-se uma proposta do fabricante **MITEL**, que forneceu uma estimativa comercial com base na linha de equipamentos da marca **UNIFY**, proporcionando uma referência de valores de mercado antes do lançamento do Termo de Referência (TR). Além disso, para estimarmos o serviço de Link Satélite, utilizou-se como referência adicional a Ata de Registro de Preços Nº 027/2023 – DPE/AP (Defensoria

Pública do Estado do Amapá), vigente desde 06/set/23 e a Ata de Registro de Preços Nº 001/2024-SEDUC PA, vigente desde 14/mar/24, para links SDWAN ou 3ª redundância em sites críticos.

Todas as cotações recebidas, assim como os documentos originais — **Termo para Cotação, Tabela de Preços do Termo de Cotação** e o **ANEXO I - LOCALIDADES INSTALADAS**, estão anexados ao processo de construção desta ETP para garantir **transparência e coerência** no processo licitatório. As propostas recebidas forneceram uma base realista de precificação para os cenários avaliados.

Inicialmente, o processo de contratação foi pensado como um **lote único**, onde todos os itens de serviço seriam agrupados. No entanto, ao longo do estudo, verificamos que a **separação em apenas três lotes distintos** como **Segurança + Conectividade Redundante + Voz, Conectividade entre Datacenters e Avaliação e Mitigação de Riscos Cibernético** traria mais vantagens, tanto do ponto de vista técnico quanto econômico. Esta decisão de dividir a contratação foi motivada pela possibilidade de se obter uma maior atração de fornecedores especializados, a redução de riscos para o Governo com maior previsibilidade dos serviços inter-relacionados, simplificação da gestão contratual e melhores condições de preço, promovendo uma competitividade mais equilibrada entre os fornecedores.

No **cenário 01**, as cotações foram obtidas através do valor médio dos itens de serviço do Termo de Cotação, atas de registro de preços satelitais e proposta da Mitel (exclusivamente para os serviços de voz) levando em consideração a complexidade técnica, a integração entre os serviços e a especialização dos fornecedores.

No **Cenário 03**, a análise técnica foi fundamentada na aplicação de um **Fator de Equivalência** entre soluções de conectividade via banda larga e ponto a ponto (P2P), visando comparar as duas alternativas com base em critérios de **qualidade de serviço (QoS), estabilidade e garantia de banda**. Além disso, foi considerado o valor praticado no contrato do Tribunal de Justiça de Pernambuco (Contrato Nº 043/2023 – TJPE (40599481) e da renovação do contrato **PE-Conectado II** (SEI/GOVPE - 51836885, **TERMO DE APOSTILAMENTO Nº 002/2024 AO CONTRATO MATER Nº 002/SAD/SEADM/2020**).

Abaixo segue o racional utilizado para encontrar um **Fator de Equivalência** entre as soluções de conectividade banda larga e ponto a ponto (P2P):

- **Fator de Equivalência Proposto**

O **Fator de Equivalência** foi estabelecido para analisar a relação entre links de **banda larga** e **Ponto a Ponto (P2P)** com base em fatores técnicos que influenciam diretamente o desempenho da rede e a experiência do usuário final. Embora ambos os tipos de links possam oferecer velocidades nominais semelhantes, há diferenças substanciais que afetam a qualidade de serviço, estabilidade e disponibilidade de banda. Essas diferenças estão diretamente relacionadas a aspectos como **oversubscription, latência, jitter e banda garantida (CIR)**.

- **Cálculo do Fator de Equivalência**

O fator de equivalência foi proposto com base em uma análise técnica e empírica de mercado, sustentada por práticas de engenharia de redes. O fator entre **0,5 e 0,7** reflete o ajuste necessário para garantir que um link de **banda larga** forneça um desempenho equivalente a um link **P2P**, com foco em três parâmetros principais:

### 1. Banda Garantida (CIR - Committed Information Rate)

Os links **P2P** garantem 100% da banda contratada, enquanto os links de **banda larga** entregam entre **50% e 70%** da banda nominal contratada, dependendo da infraestrutura do provedor e do congestionamento da rede.

- Cálculo do Fator CIR:

$$\text{Fator CIR} = \frac{100\% \text{ (P2P)}}{50\% \text{ a } 70\% \text{ (banda larga)}} \approx 1,43 \text{ a } 2$$

Isso significa que, para oferecer uma banda garantida similar à de um link P2P, um link de banda larga precisaria ter uma velocidade nominal entre **1,43 e 2 vezes maior**.

## 2. Oversubscription Ratio

O **oversubscription ratio** reflete a quantidade de usuários que compartilham a largura de banda. Para links **P2P**, o ratio é **1:1** (não há compartilhamento), enquanto em links de **banda larga** o oversubscription pode variar de **1:4 a 1:20**. Consideramos aqui uma média de **1:4**.

- Cálculo do Fator Oversubscription:

$$\text{Fator Oversubscription} = \frac{1 : 1 \text{ (P2P)}}{1 : 4 \text{ (banda larga)}} = 4$$

Portanto, um link de banda larga precisaria de **4 vezes** a largura de banda nominal para fornecer um desempenho equivalente ao de um link P2P.

## 3. Qualidade de Serviço (QoS)

Estudos, como o da **Cisco Systems** no **Enterprise QoS Design Guide**, indicam que a variação de **QoS** em redes de banda larga pode ser compensada com um aumento de **50% a 100%** na largura de banda contratada. Isso leva em consideração fatores como **jitter** e **latência**.

- Ajuste do Fator QoS:

$$\text{Fator QoS} = 1,5 \text{ a } 2$$

Ou seja, a largura de banda de um link de banda larga precisaria ser entre **1,5 e 2 vezes maior** para compensar a variação de QoS em relação a um link P2P.

- Aplicação e Conclusão do Fator de Equivalência

Com base nas práticas de mercado, estudos técnicos e resultados de redes reais, foi possível concluir que, para garantir uma **experiência de uso equivalente** entre um link **P2P de 100 Mbps** e um link de **banda larga**, por exemplo, o link de banda larga deve operar com uma **velocidade nominal entre 150 Mbps e 200 Mbps**.

Isso significa que, para compensar as limitações de **oversubscription**, **banda garantida (CIR)** e **Qualidade de Serviço (QoS)** presentes nos links de banda larga, é necessário aumentar a largura de banda nominal entre **1,5 e 2 vezes**. Este aumento compensa o fato de que a banda larga, por ser compartilhada, entrega uma banda efetiva menor e está sujeita a maior variação de desempenho devido ao congestionamento e outros fatores.

- **Justificativa do Fator de Equivalência**

Após análise de três variáveis principais (**CIR**, **oversubscription** e **QoS**), foi estabelecido o **fator de equivalência entre 0,5 e 0,7**. Essa faixa reflete a necessidade prática de ajustar a largura de banda nominal em **150% a 200%** para que os links de banda larga atinjam um desempenho similar ao de links P2P, especialmente em contextos onde a estabilidade, latência e largura de banda garantida são essenciais.

- Para um link **P2P de 100 Mbps**, seria necessário contratar um link de banda larga com **velocidade nominal entre 150 Mbps e 200 Mbps** para oferecer a mesma experiência de usuário.
- Esse ajuste não apenas reflete as limitações técnicas inerentes aos links de banda larga (como **oversubscription** e **banda garantida**), mas também incorpora práticas de mercado amplamente adotadas por ISPs e grandes operadoras, que sugerem aumentar a capacidade nominal de banda larga para clientes corporativos que exigem alto desempenho.

- **Práticas de Mercado e Testes em Redes**

1. **Práticas de ISPs no dimensionamento de serviços corporativos**

- Provedores de serviços como **AT&T**, **Comcast** e **BT Group** recomendam aos clientes corporativos a contratação de links de banda larga com **150% a 200%** da capacidade nominal em relação a um link P2P equivalente. Esse ajuste é feito para compensar a oversubscription e garantir qualidade em serviços como VoIP e videoconferências.
- **Fonte: AT&T Business Internet Services e Comcast Business Solutions** especificam que redes de banda larga corporativa requerem banda adicional para garantir desempenho similar ao P2P.

2. **Testes em redes de operadoras de telecomunicações**

- Testes realizados pela **Cisco Systems** e **Juniper Networks** mostram que um aumento de **1,5 a 2 vezes** na banda nominal de links de banda larga resulta em desempenho próximo ao de links P2P em redes empresariais. Esses testes foram realizados em grandes operadoras como **Vodafone** e **Telefonica**, onde foram observados melhoras significativas no jitter e latência.
- **Fonte: Cisco Enterprise QoS Design Guide; Juniper Networks - QoS Solutions in Enterprise Networking.**

3. **Padrões de engenharia de redes empresariais**

- O documento **ITU-T G.1010** recomenda fatores de ajuste de banda em redes compartilhadas para compensar perdas de desempenho. Isso é particularmente relevante para redes com alta oversubscription, como os links de banda larga, onde o aumento de banda nominal entre **1,5 e 2 vezes** tem sido uma prática aceita para melhorar a qualidade do serviço.
- **Fonte: ITU-T G.1010: "End-user multimedia QoS categories"** - especifica fatores de ajuste de banda para redes de oversubscription elevada.

- **Combinação das Variáveis para o Cálculo do Fator de Equivalência**

Ao analisar os três fatores principais (**CIR, oversubscription e QoS**), chegamos aos seguintes ajustes:

- **Fator CIR:** Entre **1,43 e 2**, devido à menor banda garantida em links de banda larga.
- **Fator Oversubscription:** Entre **1 e 4**, devido ao compartilhamento da infraestrutura de banda larga.
- **Fator QoS:** Entre **1,5 e 2**, para compensar os efeitos de latência, jitter e perda de pacotes.

Ao multiplicar esses fatores, o cálculo teórico sugere um aumento significativo da banda necessária, mas na prática, considerando a correlação não linear entre as variáveis, o ajuste real necessário é o fator de 0,5 a 0,7. Isso se traduz em um aumento de 150% a 200% na largura de banda nominal em links de banda larga.

- **Aplicação Final do Fator de Equivalência**

O **fator de equivalência de 0,5 a 0,7** foi calculado para refletir as condições operacionais reais e as práticas de mercado, garantindo que os links de banda larga possam atender às mesmas demandas de um link P2P. Portanto, ao aplicar esse fator, para obter uma experiência de uso semelhante a um **link P2P de 100 Mbps**, é necessário contratar um link de banda larga com **velocidade nominal entre 150 Mbps e 200 Mbps**.

Essa faixa foi escolhida com base em práticas recomendadas por grandes provedores e padrões de engenharia de redes, e é amplamente usada em redes corporativas para maximizar a eficiência e garantir a qualidade de serviço, atendendo aos requisitos operacionais de tráfego crítico.

- **Fundamentações**

1. **"Network Congestion Control: Managing Internet Traffic"** – Michael Welzl: Discussões sobre oversubscription e seus impactos na performance de redes.
2. **Cisco Systems - Enterprise QoS Solutions:** Guia de engenharia para implementação de QoS em redes corporativas, reforçando a diferença no tratamento de tráfego entre redes dedicadas e compartilhadas.
3. **RFC 4594** – Classificação e gerenciamento de QoS em redes IP, descrevendo a importância da consistência de latência, jitter e throughput para diferentes aplicações.
4. **ITU-T G.1010** – Especifica os requisitos de qualidade e banda para diferentes tipos de serviços de rede, especialmente em relação a CIR.

- **Comparação de Custos**

A tabela comparativa abaixo apresenta os valores médios das propostas recebidas, extraídos do Termo de Cotação das empresas participantes, comparando um link de banda larga de 1 Gbps com os contratos do TJ-PE e do PE-Conectado II para links P2P de 100 Mbps, 300 Mbps e 500 Mbps. Foram utilizados fatores de equivalência de 0,1, 0,3 e 0,5, respectivamente, para os links P2P, sendo todos inferiores ao fator de equivalência determinado no estudo (entre 0,5 e 0,7). Observa-se que, em todas as comparações realizadas, o custo dos links P2P foi superior ao valor médio do link de banda larga, mesmo aplicando os menores fatores de equivalência (como 0,5 para 500 Mbps, e 0,1 e 0,3 para 100 Mbps e 300 Mbps, respectivamente). Assim, conclui-se que a solução de banda larga é mais econômica e proporciona maior capacidade de banda ao usuário final, destacando o potencial de economia financeira desta alternativa.

Descrição do Link	Valor Estudado	Diferença Percentual	Observação
-------------------	----------------	----------------------	------------

Link Banda Larga 1Gbps + Firewall e licença	R\$ 2.287,06	-	Valor estimado via Termo de Cotação
Link P2P 100 Mbps + Firewall e licença	R\$ 2.460,00	7,03%	Valores praticados no contrato TJ-PE (Nº 043/2023)
Link P2P 300 Mbps + Firewall e licença	R\$ 4.311,00	46,95%	
Link P2P 500 Mbps + Firewall e licença	R\$ 3.760,28	39,18%	Valor praticado no contrato PE-Conectado II (2024)

Ainda cumpre destacar que, para o **Cenário 03**, faz-se necessário incluir a linha de cobrança referente aos pontos de roteamento de tráfego multidigital, cujo custo para o mês de **JUL/24** foi de **R\$ 265.004,81** para as bandas atualmente contratadas. Estima-se que, para as novas bandas a serem contratadas, esses valores devem aumentar exponencialmente, em virtude do grande aumento de banda que será promovido pelas novas velocidades propostas pelo novo projeto, o que torna essa solução economicamente inviável para escalonamento.

**Adicionalmente**, para assegurar uma margem de segurança e transparência ao processo de tomada de decisão, a comparação de preços a ser realizada neste ETP considerará o desempenho de um **link P2P de 100 Mbps** em relação a um **link de banda larga de 1 Gbps**. Essa escolha permitirá uma avaliação econômica justa e comparável, garantindo que o processo de aquisição reflita tanto a eficiência operacional quanto a relação custo-benefício das soluções propostas.

**Abaixo seguem os dois cenários viáveis destacados:**

**CENÁRIO 01: Solução de Rede Corporativa em modelo de contratação dos itens de serviço com separação em três lotes distintos.**

LOTE I - SEGURANÇA + CONECTIVIDADE	ITENS DE SERVIÇO	UNIDADE DE MEDIDA	QUANTITATIVO	VALOR UNITÁRIO POR EMPRESA						VALOR UNITÁRIO MÉDIO	TOTAL MENSAL	TOTAL ANUAL	TOTAL DO CONTRATO
				BRISANET SERVIÇOS DE TELECOMUNICAÇÕES S/A	ITS TELECOMUNICAÇÕES LTDA.	UMTELECOM	OI	WORLDNET TELECOMUNICAÇÕES DE TELECOMUNICAÇÕES LTDA	VECTRA CONSULTORIA E SERVIÇOS				
<b>ADENDO III - SEGURANÇA DE REDE LOCAL</b>	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1	DISPOSITIVOS	1782	R\$ 1.325,23	R\$ 1.588,63	R\$ 2.135,76	-	-	R\$ 4.284,03	R\$ 1.456,93	R\$ 2.596.249,26	R\$ 31.154.991,12	R\$ 155.774.955,60

Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2	DISPOSITIVOS	1278	R\$ 3.821,30	R\$ 4.010,10	R\$ 6.673,28	-	-	R\$ 13.206,99	R\$ 3.821,30	R\$ 4.883.621,40	R\$ 58.603.456,80	R\$ 293.017.284,00
Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	193	-	R\$ 11.356,31	R\$ 72.227,66	R\$ 4.624,99	-	R\$ 27.529,65	R\$ 4.624,99	R\$ 892.623,07	R\$ 10.711.476,84	R\$ 53.557.384,20
Solução para gerenciamento de acessos à rede local - NAC	USUÁRIOS AUTENTICADOS	24427	R\$ 4,17	R\$ 3,00	R\$ 6,56	R\$ 3,50	-	R\$ 68,92	R\$ 3,18	R\$ 77.677,86	R\$ 932.134,32	R\$ 4.660.671,60
											Total ADEN DO III	R\$ 507.010.295,40

ADENDO IV - SERVIÇO DE REDE SEM FIO	Serviço de Rede Sem Fio Interno com Segurança	DISPOSITIVOS	10042	R\$ 568,35	R\$ 791,28	R\$ 950,78	R\$ 601,28	-	R\$ 2.642,55	R\$ 568,35	R\$ 5.707.370,70	R\$ 68.488.448,40	R\$ 342.442.242,00
	Serviço de Rede Sem Fio Externo com Segurança	DISPOSITIVOS	500	R\$ 1.165,25	R\$ 1.407,51	R\$ 1.450,74	R\$ 819,01	-	R\$ 3.143,57	R\$ 819,01	R\$ 409.505,00	R\$ 4.914.060,00	R\$ 24.570.300,00
	Serviço de Rede Sem Fio Temporário com Segurança	DISPOSITIVOS	10	-	R\$ 993,96	R\$ 7.271,68	R\$ 819,01	-	R\$ 2.646,66	R\$ 819,01	R\$ 8.190,10	R\$ 49.140,60	R\$ 49.140,60
	Serviço de fornecimento e implantação de Switch	UNIDADE	591	R\$ 861,81	-	R\$ 771,87	R\$ 650,00	-	R\$ 182,39	R\$ 581,43	R\$ 343.625,13	R\$ 4.123.501,56	R\$ 20.617.507,80
												Total ADENDO IV	R\$ 387.679.190,40
ADENDO V - CONECTIVIDADE DE REDE LOCAL	Link de Acesso Permanente (LAP - Tipo 1)	LINK	2987	R\$ 352,82	R\$ 359,72	R\$ 943,29	R\$ 794,62	-	-	R\$ 356,27	R\$ 1.064.178,49	R\$ 12.770.141,88	R\$ 63.850.709,40
	Link de Acesso Permanente (LAP - Tipo 2)	LINK	2170	R\$ 457,05	R\$ 551,75	R\$ 4.056,72	R\$ 910,62	-	-	R\$ 504,40	R\$ 1.094.548,00	R\$ 13.134.576,00	R\$ 65.672.880,00
	Link Multitecnologia Especial (LME) - Tipo 1	LINK	250	-	-	-	R\$ 3.225,78	-	-	R\$ 3.312,89	R\$ 828.222,50	R\$ 9.938.670,00	R\$ 49.693.350,00

	Link Multitecnologia Especial (LME) - Tipo 2	LINK	20	R\$ 600,00	R\$ 501,50	R\$ 1.257,72	R\$ 4.217,56	-	-	R\$ 501,50	R\$ 10.030,00	R\$ 120.360,00	R\$ 601.800,00
	Link Multitecnologia Especial (LME) - Tipo 3	LINK	20	R\$ 1.000,00	R\$ 2.102,10	R\$ 4.056,72	R\$ 911,01	-	-	R\$ 911,01	R\$ 18.220,20	R\$ 218.642,40	R\$ 1.093.212,00
	Link Acesso Temporário (LAT) - Tipo 1	LINK	30	-	-	R\$ 4.569,50	R\$ 3.225,78	-	-	R\$ 3.400,00	R\$ 102.000,00	R\$ 612.000,00	R\$ 612.000,00
	Link Acesso Temporário (LAT) - Tipo 2	LINK	20	R\$ 1.000,00	R\$ 1.202,40	R\$ 7.484,58	R\$ 795,66	-	-	R\$ 1.067,77	R\$ 21.355,40	R\$ 128.132,40	R\$ 128.132,40
	Link Acesso Temporário (LAT) - Tipo 3	LINK	20	R\$ 1.500,00	R\$ 1.903,80	R\$ 12.283,58	R\$ 910,58	-	-	R\$ 910,58	R\$ 18.211,60	R\$ 109.269,60	R\$ 109.269,60
												Total ADENDO V	R\$ 181.761.353,40
ADENDO VI - SEGURANÇA DE DADOS	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DADOS	DISPOSITIVOS	6	R\$ 60.168,19	R\$ 61.273,40	R\$ 109.880,38	-	-	R\$ 248.720,42	R\$ 60.720,80	R\$ 364.324,80	R\$ 4.371.897,60	R\$ 21.859.488,00

Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	3	R\$ 59.654,80	R\$ 50.200,91	R\$ 56.836,67	R\$ 149.200,12	-	R\$ 109.292,91	<b>R\$ 50.200,91</b>	<b>R\$ 150.602,73</b>	R\$ 1.807.232,76	R\$ 9.036.163,80
Solução de segurança de confiança a zero - ZTNA	DISPOSITIVOS	1221	R\$ 17,27	R\$ 10,04	R\$ 13,90	R\$ 4,50	-	R\$ 19,96	<b>R\$ 18,62</b>	<b>R\$ 22.735,02</b>	R\$ 272.820,24	R\$ 1.364.101,20
Solução de proteção, detecção e resposta para servidores - EDR	DISPOSITIVOS	4.200	R\$ 38,69	R\$ 40,01	R\$ 51,69	R\$ 20,03	-	R\$ 94,79	<b>R\$ 39,35</b>	<b>R\$ 165.270,00</b>	R\$ 1.983.240,00	R\$ 9.916.200,00
Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede	DISPOSITIVOS	3	R\$ 50.732,38	-	R\$ 104.601,98	R\$ 249.326,41	-	R\$ 219.141,97	<b>R\$ 50.732,38</b>	<b>R\$ 152.197,14</b>	R\$ 1.826.365,68	R\$ 9.131.828,40

	- NDR												
	Solução para gerenciamento de acessos à rede datacenter - NAC	USUÁRIOS AUTENTICADOS	1221	R\$ 8,22	R\$ 6,53	R\$ 11,11	R\$ 5.470,00	-	R\$ 758,89	R\$ 6,53	R\$ 7.973,13	R\$ 95.677,56	R\$ 478.387,80
	Solução de segurança de identidade e privileda da - PAM	USUÁRIOS	1221	R\$ 211,71	R\$ 282,16	R\$ 610,62	R\$ 303,64	-	R\$ 1.198,03	R\$ 294,06	R\$ 359.047,26	R\$ 4.308.567,12	R\$ 21.542.835,60
	Solução de filtro de mensagens indesejadas - ANTISPAM	CONTAS	129.058	R\$ 0,59	R\$ 2,01	R\$ 4,83	R\$ 1,25	-	R\$ 2,04	R\$ 1,74	R\$ 224.560,92	R\$ 2.694.731,04	R\$ 13.473.655,20
	Solução de Filtro de Aplicações WEB - WAF	UNIDADE	3	R\$ 13.028,34	R\$ 8.936,86	R\$ 34.425,76	R\$ 29.990,12	-	R\$ 72.579,83	R\$ 29.363,00	R\$ 88.089,00	R\$ 1.057.068,00	R\$ 5.285.340,00
												Total ADENDO VI	R\$ 92.088.000,00
ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO	Solução de gerenciamento e monitoramento de ativos	ATIVOS	1	R\$ 805.849,87	R\$ 651.300,00	R\$ 791.653,17			R\$ 1.687.281,33	R\$ 651.300,00	R\$ 651.300,00	R\$ 7.815.600,00	R\$ 39.078.000,00
	Solução de gerenciamento	USUÁRIOS	629.058	R\$ 0,92	R\$ 1,20	R\$ 5,03	R\$ 1,72		R\$ 2,61	R\$ 0,92	R\$ 578.733,36	R\$ 6.944.800,32	R\$ 34.724.001,60

	de identidad e de acesso												
	Solução de monitora mento e análise de eventos de seguran ça	EPS	444.822	R\$ 4,01	R\$ 3,11	R\$ 7,25	R\$ 1,85		R\$ 6,79	R\$ 1,85	R\$ 822.920,70	R\$ 9.875.048,40	R\$ 49.375.242,00
	Solução de automaç ão de resposta a incidentes de seguran ça	UNIDAD E	1	R\$ 211.060,22	R\$ 177.917,93	R\$ 235.945,07			R\$ 510.712,82	R\$ 177.917,93	R\$ 177.917,93	R\$ 2.135.015,16	R\$ 10.675.075,80
	Solução para guarda de LOGs	UNIDAD E	1	R\$ 569.470,71	R\$ 212.002,00	R\$ 393.268,64			R\$ 802.515,61	R\$ 212.002,00	R\$ 212.002,00	R\$ 2.544.024,00	R\$ 12.720.120,00
	Laborató rio de testes	UNIDAD E	1	R\$ 3.053.986,00	R\$ 19.176,40	R\$ 7.914,29	R\$ 117.979,69		R\$ 14.973,52	R\$ 7.914,29	R\$ 7.914,29	R\$ 94.971,48	R\$ 474.857,40
	Solução de gerencia mento de serviços de TI	UNIDAD E	1	R\$ 36.960,00	R\$ 39.900,35		R\$ 1.229.100,70		R\$ 285.496,51	R\$ 38.430,18	R\$ 38.430,18	R\$ 461.162,16	R\$ 2.305.810,80
												Total ADEN DO VIII	R\$ 149.353.107,60
ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E	Serviço de resposta à incidentes de ciberseg	HORA	318	R\$ 770,00	R\$ 673,67	-	-	-	R\$ 2.098,18	R\$ 673,67	R\$ 214.227,06	R\$ 2.570.724,72	R\$ 12.853.623,60

SEGURANÇA CIBERNÉTICA	segurança sob demanda												
	Serviço de análise de segurança de primeiro nível	EQUIPE	1	R\$ 187.500,41	-	-	R\$ 506.960,08	-	R\$ 1.842.800,27	R\$ 187.500,41	R\$ 187.500,41	R\$ 2.250.004,92	R\$ 11.250.024,60
	Serviço de análise de segurança especializada	EQUIPE	1	R\$ 623.433,32	R\$ 401.752,65	-	R\$ 1.126.603,94	-	R\$ 1.774.812,02	R\$ 401.752,65	R\$ 401.752,65	R\$ 4.821.031,80	R\$ 24.105.159,00
	Serviço de acompanhamento de reparos	EQUIPE	1	R\$ 53.900,00	-	-	R\$ 119.608,24	-	R\$ 95.567,94	R\$ 53.900,00	R\$ 53.900,00	R\$ 646.800,00	R\$ 3.234.000,00
	Serviço de atenção especializada ao cliente	EQUIPE	1	R\$ 77.000,00	R\$ 98.107,15	-	R\$ 99.561,43	-	R\$ 1.834.394,93	R\$ 77.000,00	R\$ 77.000,00	R\$ 924.000,00	R\$ 4.620.000,00
	Service Desk	EQUIPE	1	R\$ 153.887,09	R\$ 91.292,00	-	R\$ 507.679,19	-	R\$ 768.757,23	R\$ 91.292,00	R\$ 91.292,00	R\$ 1.095.504,00	R\$ 5.477.520,00
	Serviço de operação da rede	EQUIPE	1	R\$ 86.240,00	R\$ 193.406,41	-	R\$ 1.142.750,26	-	R\$ 2.216.811,26	R\$ 86.240,00	R\$ 86.240,00	R\$ 1.034.880,00	R\$ 5.174.400,00
	Serviço de análise de qualidade	EQUIPE	1	R\$ 77.000,00	-	-	R\$ 99.576,90	-	R\$ 177.540,80	R\$ 77.000,00	R\$ 77.000,00	R\$ 924.000,00	R\$ 4.620.000,00
	Serviço de Coordenação do	EQUIPE	1	R\$ 42.350,00	R\$ 27.351,92	-	R\$ 390.418,94	-	R\$ 1.727.807,80	R\$ 27.351,92	R\$ 27.351,92	R\$ 328.223,04	R\$ 1.641.115,20

	CIISC												
	Núcleo de Redes e Segurança Setorial	EQUIPE	5	R\$ 17.325,00	R\$ 51.345,45	-	R\$ 35.007,00	-	R\$ 119.734,85	R\$ 17.325,00	R\$ 86.625,00	R\$ 1.039.500,00	R\$ 5.197.500,00
	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCSs)	EQUIPE	22	R\$ 13.200,00	R\$ 12.836,36	-	R\$ 18.323,00	-	-	R\$ 12.836,36	R\$ 282.399,92	R\$ 3.388.799,04	R\$ 16.943.995,20
	Serviço de Evolução da Maturidade em Segurança da Informação	EQUIPE	1	R\$ 38.500,00	R\$ 32.049,45	-	R\$ 23.659,92	-	R\$ 187.580,76	R\$ 23.659,92	R\$ 23.659,92	R\$ 283.919,04	R\$ 1.419.952,20
												Total ADEN DO IX	R\$ 96.536.932,80
ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)	Serviço de Comunicação Unificada - SCU (Conta de usuário)	UNIDADE	10395	R\$ 54,21	R\$ 39,35	R\$ 90,56	R\$ 70,55	-	R\$ 487,91	R\$ 44,85	R\$ 466.215,75	R\$ 5.594.589,00	R\$ 27.972.945,00
												Total ADEN	R\$ 27.972.

												DO XII	945,00
<b>ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE</b>	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)	UNIDADE	7000	R\$ 134,28	R\$ 126,00	R\$ 370,88	R\$ 231,24	-	R\$ 482,26	R\$ 126,00	R\$ 882.00,00	R\$ 10.584.000,00	R\$ 52.920.000,00
	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	UNIDADE	8000	R\$ 102,24	R\$ 98,00	R\$ 231,36	R\$ 132,51	-	R\$ 289,46	R\$ 98,00	R\$ 784.00,00	R\$ 9.408.000,00	R\$ 47.040.000,00
	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	UNIDADE	203	R\$ 177,48	R\$ 167,00	R\$ 263,50	R\$ 148,46	-	R\$ 350,17	R\$ 148,46	R\$ 30.137,38	R\$ 361.648,56	R\$ 1.808.242,80
	Serviço de Ponto de Voz Fixo com Aparelho de Voz DECT IP (PVF-DECT IP)	UNIDADE	354	R\$ 136,62	R\$ 240,00	R\$ 305,42	R\$ 192,84	-	R\$ 1.073,23	R\$ 136,62	R\$ 48.363,48	R\$ 580.361,76	R\$ 2.901.808,80

Serviço de Ponto de Voz Fixo utilizando o Software de Voz (PVF SOFTWARE)	UNIDADE	2107	-	R\$ 38,00	R\$ 107,17	R\$ 78,10	-	R\$ 165,32	R\$ 38,00	R\$ 80.066,00	R\$ 960.792,00	R\$ 4.803.960,00
Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)	UNIDADE	10395	R\$ 7,80	R\$ 12,50	R\$ 4,52	R\$ 3,55	-	R\$ 8,48	R\$ 3,55	R\$ 36.902,25	R\$ 442.827,00	R\$ 2.214.135,00
Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)	UNIDADE	203	R\$ 129,40	R\$ 110,00	R\$ 154,05	R\$ 51,46	-	R\$ 182,87	R\$ 51,46	R\$ 10.446,38	R\$ 125.356,56	R\$ 626.782,80
Serviço PVF-Fone-de-Cabeça	UNIDADE	1223	R\$ 44,40	R\$ 55,00	R\$ 29,62	-	-	R\$ 36,80	R\$ 29,62	R\$ 36.225,26	R\$ 434.703,12	R\$ 2.173.515,60
Serviço Fixo Inter Estadual	MINUTO	364	R\$ 0,06	R\$ 0,03	R\$ 0,15	-	-	-	R\$ 0,05	R\$ 18,20	R\$ 218,40	R\$ 1.092,00
Serviço Fixo Intra Estadual	MINUTO	15303	R\$ 0,06	R\$ 0,03	R\$ 0,15	-	-	-	R\$ 0,05	R\$ 765,15	R\$ 9.181,80	R\$ 45.909,00
Serviço Fixo Local	MINUTO	84960	R\$ 0,06	R\$ 0,02	R\$ 0,15	-	-	-	R\$ 0,04	R\$ 3.398,40	R\$ 40.780,80	R\$ 203.904,00
Serviço Móvel Intra Estadual	MINUTO	137450	R\$ 0,50	R\$ 0,69	R\$ 0,42	-	-	-	R\$ 0,41	R\$ 56.354,50	R\$ 676.254,00	R\$ 3.381.270,00
Serviço Móvel Local	MINUTO	575533	R\$ 0,50	R\$ 0,45	R\$ 0,42	-	-	-	R\$ 0,35	R\$ 201.436,55	R\$ 2.417.238,60	R\$ 12.086.193,00
Serviço Móvel	MINUTO	23051	R\$ 0,36	R\$ 0,45	R\$	-	-	-	R\$	R\$ 7.376,	R\$ 88.515	R\$ 442.57

	VC2					0,42				0,32	32	,84	9,20
	Serviço Móvel VC3	MINUTO	802	R\$ 0,36	R\$ 0,45	R\$ 0,42	-	-	-	R\$ 0,32	R\$ 256,64	R\$ 3.079,68	R\$ 15.398,40
	Serviço Longa Inter Regional Fixo	MINUTO	475	R\$ 1,00	R\$ 0,13	R\$ 0,15	-	-	-	R\$ 0,14	R\$ 66,50	R\$ 798,00	R\$ 3.990,00
	Serviço Adicional de Acesso SIP (SIP TRUNK)	UNIDADE	21	R\$ 7.488,00	R\$ 350,00	-	R\$ 891,71	-	-	R\$ 350,00	R\$ 7.350,00	R\$ 88.200,00	R\$ 441.000,00
												Total ADEN DO XIII	R\$ 131.109.780,60
ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER	Serviço de Contact Center com Recurso de Voz	UNIDADE	250	R\$ 2.964,00	R\$ 1.420,00	R\$ 902,49	R\$ 693,23	-	R\$ 1.630,43	R\$ 693,23	R\$ 173.307,50	R\$ 2.079.690,00	R\$ 10.398.450,00
	Serviço de Contact Center com recurso de Whatsapp	UNIDADE	400	R\$ 1.588,28	R\$ 380,00	R\$ 753,83	R\$ 579,05	-	R\$ 1.361,84	R\$ 380,00	R\$ 152.000,00	R\$ 1.824.000,00	R\$ 9.120.000,00
	Serviço de Contact Center com recurso de Redes Sociais	UNIDADE	50	R\$ 4.680,00	R\$ 350,00	R\$ 741,32	R\$ 569,41	-	R\$ 1.339,19	R\$ 350,00	R\$ 17.500,00	R\$ 210.000,00	R\$ 1.050.000,00
	Serviço de Unidade de	UNIDADE	100	R\$ 6.685,71	R\$ 290,00	R\$ 323,74	R\$ 248,21	-	R\$ 408,64	R\$ 248,21	R\$ 24.821,00	R\$ 297.852,00	R\$ 1.489.260,00

	Respost a Audível (Porta de URA)												
	Serviço de Comunicação por vídeo ou vídeo- chamada	UNIDADE	60	R\$ 2.340,00	R\$ 1.950,00	R\$ 1.275,01	R\$ 979,96	-	R\$ 2.304,76	R\$ 979,96	R\$ 58.797,60	R\$ 705.571,20	R\$ 3.527.856,00
	Serviço de Automa- tizações e Integra- ções - Consulta Inicial	UNIDADE	5	R\$ 15.600,00	R\$ 15.200,00	R\$ 2.264,73	R\$ 1.015,40	-	R\$ 4.673,02	R\$ 1.015,40	R\$ 5.077,00	R\$ 60.924,00	R\$ 304.620,00
	Serviço de Automa- tizações e Integra- ções - Implan- tação	UNIDADE	100	R\$ 219,74	R\$ 5.600,00	R\$ 675,76	R\$ 303,05	-	R\$ 1.394,64	R\$ 219,74	R\$ 21.974,00	R\$ 263.688,00	R\$ 1.318.440,00
												Total ADEN- DO XIV	R\$ 27.208.626,00
ADENDO XVI - NÍVEIS MÍNIMOS DE SERVIÇO	Suporte de Manuten- ção (12h x 7d)	UNIDADE	600	R\$ 276,84	R\$ 509,03	-	-	-	R\$ 3.495,39	R\$ 276,84	R\$ 166.104,00	R\$ 1.993.248,00	R\$ 9.966.240,00
	Suporte de Manuten- ção (24h x 7d)	UNIDADE	500	R\$ 1.082,91	R\$ 1.000,09	-	-	-	R\$ 5.243,09	R\$ 1.000,09	R\$ 500.045,00	R\$ 6.000.540,00	R\$ 30.002.700,00
												Total ADEN- DO XVI	R\$ 39.968.940,00

LOTE II - CONECTIVIDADE DE DATA CENTER	ITENS DE SERVIÇO	UNIDADE DE MEDIDA	QUANTITATIVO	VALOR UNITÁRIO POR EMPRESA						VALOR UNITÁRIO MÉDIO	TOTAL MENSAL	TOTAL ANUAL	TOTAL DO CONTRATO
				BRISANET SERVIÇOS DE TELECOMUNICAÇÕES S/A	ITS TELECOMUNICAÇÕES LTDA.	UM TELECOM	OI	WORLDNET TELECOM SERVIÇOS DE TELECOMUNICAÇÕES LTDA	VECTRA CONSULTORIA E SERVIÇOS				
ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATA CENTER	Link de Fibra Lan To Lan (L2L)	UNIDADE	4	R\$ 6.220,36	R\$ 143.572,00	R\$ 6.575,30	R\$ 183.561,18	R\$ 40.000,00	-	R\$ 6.220,36	R\$ 24.881,44	R\$ 298.577,28	R\$ 1.492.886,40
	Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	3	R\$ 2.000,00	R\$ 4.404,40	-	-	R\$ 9.000,00	-	R\$ 5.253,72	R\$ 15.761,16	R\$ 189.133,92	R\$ 189.133,92
	Link para Data Center de 4GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	3	R\$ 4.000,00	R\$ 5.917,70	-	-	R\$ 17.400,00	-	R\$ 11.501,04	R\$ 34.503,12	R\$ 414.037,44	R\$ 414.037,44
	Link para Data Center de 6GB com AntiDDoS	UNIDADE	3	R\$ 6.000,00	R\$ 6.827,20	-	-	R\$ 25.200,00	-	R\$ 14.031,25	R\$ 42.093,75	R\$ 505.125,00	R\$ 505.125,00

	S - Link Internet Trânsito (LIT)												
	Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	3	R\$ 8.000,00	R\$ 7.221,60	-	-	R\$ 32.400,00	-	R\$ 14.435,84	R\$ 43.307,52	R\$ 519.690,24	R\$ 519.690,24
	Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	3	R\$ 10.000,00	R\$ 7.939,50	-	-	R\$ 39.000,00	-	R\$ 8.969,75	R\$ 26.909,25	R\$ 322.911,00	R\$ 322.911,00
												Total ADEN DO VII	R\$ 3.443.784,00

LOTE III - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS	ITENS DE SERVIÇO	UNIDADE DE MEDIDA	QUANTITATIVO	VALOR UNITÁRIO POR EMPRESA						VALOR UNITÁRIO MÉDIO	TOTAL MENSAL	TOTAL ANUAL	TOTAL DO CONTRATO
				BRISANET SERVIÇOS DE TELECOMUNICAÇÕES S/A	ITS TELECOMUNICAÇÕES LTDA.	UMTELECOM	OI	WORLDNET TELECOMUNICAÇÕES DE TELECOMUNICAÇÕES LTDA	VECTRA CONSULTORIA E SERVIÇOS				
ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE	Serviço de gestão de vulnerabilidades	UNIDADE	4200	R\$ 85,68	R\$ 125,38	-	-	-	-	R\$ 85,68	R\$ 359.856,00	R\$ 4.318.272,00	R\$ 21.591.360,00

RISCOS CIBERNÉTICOS	Serviço de análise forense	HORA	141	R\$ 844,96	R\$ 9.528,50	-	-	-	-	R\$ 844,96	R\$ 119.139,36	R\$ 1.429.672,32	R\$ 7.148.361,60
	Serviço de análise de segurança ofensiva (Red Team)	UNIDADE	1	R\$ 224.186,03	R\$ 324.292,00	-	-	-	-	R\$ 224.186,03	R\$ 224.186,03	R\$ 2.690.232,36	R\$ 13.451.161,80
	Serviço de testes de intrusão (Pentest)	UNIDADE	10	R\$ 15.829,30	R\$ 16.080,00	-	-	-	-	R\$ 15.829,30	R\$ 158.293,00	R\$ 1.899.516,00	R\$ 9.497.580,00
												<b>Total ADEN DO X</b>	R\$ 51.688.463,40

**CENÁRIO 03: Solução de Rede Corporativa em modelo de contratação de acesso dedicado (P2P) com ponto único de acesso à Internet e concentradores regionais.**

Conforme detalhado no item anterior, a solução analisada apresentou um custo significativamente mais alto em todas as faixas de velocidade avaliadas (500 Mbps, 300 Mbps e 100 Mbps). Para a velocidade de 100 Mbps, por exemplo, o custo foi mais de 7% superior, mesmo oferecendo uma largura de banda nominal 10 vezes menor e com um fator de equivalência entre 0,5 e 0,7, conforme identificado no estudo. Além disso, é importante salientar que o custo relacionado à instalação dos concentradores regionais ou concentrador único não foi incluído na análise, o que resultaria em um aumento ainda maior no valor final da solução.

Assim, conclui-se que esta alternativa apresenta um custo elevado e inviável economicamente, especialmente quando comparada aos preços de referência obtidos através dos contratos vigentes do TJ-PE e do PE-Conectado II. Esses fatores, juntamente com a necessidade de ampliação dos pontos de tráfego de roteamento digital, tornam a solução analisada financeiramente inviável, não atendendo às expectativas de otimização dos recursos públicos.

A tabela abaixo apresenta o custo médio estimado de R\$ 2.287,06, utilizado para comparação com os contratos referenciados do TJ-PE e do PE-Conectado II, oferecendo uma visão mais clara dos custos envolvidos e da falta de competitividade econômica desta alternativa.

ITENS DE SERVIÇOS	UNIDADE DE MEDIDA	VALOR UNITÁRIO					VALOR UNITÁRIO MÉDIO
		DB3 (GIGA+)	Brisanet/ Inorpel/BidWeb	NTSec	FBR Digital	OI	
Solução unificada de segurança de rede	DISPOSITIVOS	R\$ 1.000,00	R\$ 649,43	R\$ 3.000,00	-	R\$ 1.219,68	R\$ 1.467,28
Link Banda Larga (LBL) de 1GB	LINK	R\$ 1.000,00	R\$ 450,00	-	R\$ 902,78	R\$ 926,33	R\$ 819,78
TOTAL							R\$ 2.287,06

Abaixo está a tabela comparativa dos valores médios das propostas recebidas, extraídos do Termo de Cotação apresentado pelas empresas participantes, utilizando conectividade via banda larga e comparando-os com os valores praticados em contratos públicos vigentes para soluções de conectividade ponto a ponto (P2P). A tabela também apresenta a análise de economicidade, destacando os potenciais ganhos financeiros.

Descrição do Link	Valor Estudado	Diferença Percentual	Observação
Link Banda Larga 1Gbps + Firewall e licença	R\$ 2.287,06	-	Valor estimado via Termo de Cotação
Link P2P 100 Mbps + Firewall e licença	R\$ 2.460,00	7,03%	Valores praticados no contrato TJ-PE (Nº 043/2023)
Link P2P 300 Mbps + Firewall e licença	R\$ 4.311,00	46,95%	
Link P2P 500 Mbps + Firewall e licença	R\$ 3.760,28	39,18%	Valor praticado no contrato PE-Conectado II (2024)

## 10.2.MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Considerando que apenas o estudo do **Cenário 1** atendeu plenamente tanto aos requisitos de negócio quanto aos requisitos técnicos, além de demonstrar **viabilidade econômica**, segue abaixo o mapa consolidando os resultados financeiros deste cenário.

CENÁRIO 1 DIVISÃO LOTES x SERVIÇOS	ESTIMATIVA DE TCO AO LONGO DOS ANOS						
	SERVIÇOS	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	VALOR TOTAL DO CONTRATO 5 ANOS
1º LOTE	Segurança + Conectividade	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 2.222.150.328,72
	Comunicação de Voz	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 320.702.427,79
	Acesso Satélite	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 41.698.116,00
2º LOTE	Conectividade entre Datacenters	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 41.951.688,66
3º LOTE	Avaliação e Mitigação de Riscos Cibernéticos	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 38.614.527,66
TOTAL	-	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 2.665.117.088,83

## 11. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A decisão de separar a contratação da nova rede de segurança e conectividade do Estado de Pernambuco em três lotes distintos é fundamentada em uma análise criteriosa que abrange aspectos técnicos, econômicos e estratégicos, garantindo a maximização da eficiência, a segurança e a qualidade dos serviços prestados. A seguir, são detalhados os principais argumentos que sustentam essa abordagem.

**1º Lote: Serviço de Segurança de Toda a Rede + Conectividade com Banda Larga (Link Principal + Redundância) + Comunicação de Voz**

- **Integração Técnica e Operacional:** A segurança da rede e a conectividade principal são elementos críticos e interdependentes. Ao consolidar esses serviços em um único lote, garantimos que a implementação de soluções de segurança esteja diretamente alinhada com a gestão da conectividade principal, evitando incompatibilidades e simplificando a operação. Isso é vital para manter a integridade, a disponibilidade e a confidencialidade dos dados trafegados pela rede do governo.
- **Redução de Complexidade:** A gestão centralizada desses serviços por um único fornecedor ou consórcio reduz a complexidade administrativa e operacional, permitindo uma resposta mais rápida a incidentes e uma coordenação mais eficaz entre as equipes de segurança e de infraestrutura de rede.
- **Economia de Escala e Eficiência Operacional:** A unificação desses serviços permite ao fornecedor otimizar recursos e infraestrutura, resultando em uma redução significativa de custos operacionais. A economia de escala obtida através da centralização desses serviços também proporciona maior poder de negociação para o Estado, resultando em contratos mais vantajosos e eficientes.

## 2º Lote: Conectividade Datacenter com AntiDDoS

- **Especialização e Foco em Segurança Crítica:** A conectividade de Datacenter, com a proteção AntiDDoS, é um serviço altamente especializado, essencial para garantir a segurança e a continuidade das operações de TI do governo. A separação deste serviço em um lote dedicado permite a contratação de fornecedores com expertise específica em mitigação de ataques DDoS e gestão de infraestruturas de alta disponibilidade. Isso reduz significativamente os riscos de indisponibilidade e violações de segurança, protegendo dados sensíveis e serviços críticos do Estado.
- **Adaptação às Inovações Tecnológicas:** O setor de segurança cibernética e infraestrutura de Datacenter é dinâmico, com constantes inovações tecnológicas. A especialização deste lote permite que o Estado aproveite as últimas inovações em proteção de rede e gestão de Datacenter, garantindo que as soluções contratadas sejam robustas, atualizadas e eficazes contra ameaças emergentes.
- **Aumento da Competitividade:** Ao separar o serviço de Datacenter com AntiDDoS, o Estado atrai empresas especializadas que podem oferecer soluções inovadoras e economicamente competitivas. Isso não apenas melhora a qualidade das propostas recebidas, mas também amplia o leque de opções tecnológicas disponíveis para o governo.

## 3º Lote: Avaliação e Mitigação de Riscos Cibernéticos

- **Foco em segurança ofensiva:** Ao separar esses serviços, o estado pode contratar fornecedores com expertise avançada em segurança ofensiva e análise forense, garantindo a identificação de riscos antes que sejam explorados por agentes mal-intencionados, elevando a proteção da rede e dos dados governamentais.
- **Prevenção e análise a ameaças avançadas:** A gestão de vulnerabilidades, aliada aos testes de intrusão, permite ao governo antecipar falhas em suas infraestruturas críticas. A análise forense, por sua vez, assegura que, em caso de ataques, a origem e o impacto sejam investigados, aprimorando a segurança continuamente.
- **Flexibilidade e competitividade no mercado:** Ao separar o serviço de avaliação e mitigação de riscos cibernéticos, o estado atrai empresas especializadas, ampliando a competitividade no processo de contratação e obtendo soluções mais customizadas e adaptadas às necessidades de segurança, com maior qualidade dos serviços.

## 12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

A análise das contratações correlatas e interdependentes é essencial para assegurar que a nova solução de rede de segurança e conectividade do Estado de Pernambuco seja implementada de forma integrada e eficiente, evitando sobreposições, garantindo a continuidade dos serviços e maximizando os recursos disponíveis.

#### Identificação e Análise das Contratações Correlatas

A solução tecnológica proposta tem como objetivo principal substituir o contrato denominado **PE-Conectado II**, que atualmente contempla conectividade e segurança de perímetro. O novo contrato, além de substituir e ampliar a conectividade existente, introduz significativas melhorias na segurança cibernética. Assim, a análise das contratações correlatas deve considerar:

**1. Substituição e Ampliação dos Serviços:** O novo contrato visa substituir o PE-Conectado II, integrando a ampliação da banda contratada e a adição de redundância para os sites do Governo. A infraestrutura física das soluções estará inclusa nos preços dos serviços, como rede elétrica e rede interna (incluindo racks, gabinetes, fiação e etc...), minimizando a necessidade de novas contratações de infraestrutura física. Essa modalidade facilita a transição entre os contratos e assegura a eficiência na implantação das novas soluções.

**2. Integração com Ferramentas de Segurança Avançadas:** A nova solução incorpora um conjunto robusto de novas ferramentas e serviços de segurança, que ampliam significativamente as capacidades de cibersegurança do governo. Essas novas aquisições abrangem desde a proteção e detecção de ameaças em redes locais e datacenters, até soluções avançadas para o monitoramento, análise e resposta a incidentes de segurança. A integração dessas novas tecnologias com a infraestrutura existente deve ser cuidadosamente planejada para garantir uma implementação eficiente e maximizar os benefícios de segurança proporcionados por essas melhorias.

#### Identificação e Análise das Contratações Interdependentes

As contratações interdependentes são aquelas que, direta ou indiretamente, influenciam ou dependem do sucesso da nova solução proposta. Neste contexto:

**1. Impacto Positivo na Segurança Cibernética:** A nova solução trará um impacto extremamente positivo na segurança cibernética do Governo do Estado, avançando significativamente em relação à situação atual. O projeto contempla a implementação de serviços de monitoramento contínuo, resposta a incidentes, e análise forense, entre outros, que são essenciais para a proteção dos dados e serviços críticos do governo. A introdução desses novos serviços não apenas fortalece a defesa contra ameaças cibernéticas, mas também aumenta a resiliência da infraestrutura de TI do Estado.

**2. Continuidade de Serviços e Planejamento da Transição:** Para assegurar a continuidade dos serviços durante a transição do PE-Conectado II para o novo contrato, é necessário coordenar cuidadosamente os cronogramas de desativação dos serviços antigos e a ativação dos novos. A manutenção da infraestrutura existente facilita essa transição, enquanto as novas soluções de segurança são implementadas progressivamente, garantindo que o nível de proteção seja sempre mantido ou elevado.

**3. Compatibilidade e Integração das Soluções:** A compatibilidade entre as novas ferramentas de segurança e os sistemas de conectividade existentes é fundamental. A interdependência entre a infraestrutura física atual e as novas soluções de cibersegurança requer uma análise detalhada para assegurar que todos os componentes operem de maneira harmoniosa. A integração dessas novas tecnologias deve ser conduzida de forma a evitar interrupções nos serviços, ao mesmo tempo em que se maximiza o desempenho e a segurança da rede.

### 13. RESULTADOS PRETENDIDOS

A contratação da nova solução de rede de segurança e conectividade para o Estado de Pernambuco tem como objetivo central promover avanços significativos na eficiência operacional, na segurança cibernética, na resiliência da rede e na capacidade de atendimento dos serviços de TIC. Os resultados pretendidos são delineados de forma específica e mensurável, garantindo que o investimento realizado pela Administração Pública seja justificado e traga benefícios tangíveis e sustentáveis para o governo e a sociedade.

## 1. Fortalecimento da Segurança Cibernética

A segurança cibernética é um pilar fundamental para a proteção das infraestruturas críticas do Governo do Estado de Pernambuco. Com o crescente volume e sofisticação dos ataques cibernéticos, torna-se imperativo adotar uma postura proativa e integrada para proteger os ativos digitais e assegurar a continuidade dos serviços públicos. A contratação de novas soluções de segurança cibernética visa implementar um ecossistema de defesa abrangente, que integra proteção avançada, monitoramento contínuo e capacidade de resposta rápida a incidentes, garantindo a resiliência da infraestrutura de TIC e a segurança das informações governamentais.

### Resultados Esperados:

- **Implementação de um Sistema de Defesa em Profundidade:** Estabelecimento de uma arquitetura de defesa em múltiplas camadas, aumentando significativamente a resiliência contra ameaças cibernéticas.
- **Gerenciamento de Identidades e Acessos Robustos:** Garantia de acesso seguro e restrito a informações sensíveis, com rápida detecção e bloqueio de acessos não autorizados.
- **Resiliência Aumentada contra Ameaças Avançadas:** Preparação aprimorada para enfrentar ameaças sofisticadas, mitigando riscos em sistemas críticos.
- **Capacidade Avançada de Detecção e Resposta a Incidentes:** Monitoramento contínuo e resposta imediata a ameaças, minimizando danos e assegurando a recuperação rápida de serviços.
- **Melhoria da Postura de Cibersegurança com Inteligência Avançada:** Antecipação a ameaças com inteligência cibernética e análise forense, aplicando medidas preventivas e corretivas.
- **Desenvolvimento Contínuo da Maturidade em Segurança da Informação:** Integração de uma cultura de segurança cibernética em todos os níveis do governo, aumentando a conscientização e a preparação dos funcionários.
- **Capacidade de Resposta Rápida e Especializada a Incidentes Críticos:** Mobilização rápida de uma equipe especializada para enfrentar incidentes críticos, minimizando o impacto de ataques complexos.
- **Integração de um Centro de Gerenciamento de Segurança:** Criação de um núcleo centralizado para coordenar todas as atividades de segurança, proporcionando uma visão unificada e uma resposta coordenada a incidentes.
- **Impactos e Benefícios:** Essas medidas proporcionarão uma proteção robusta contra uma ampla gama de ameaças cibernéticas, garantindo a continuidade dos serviços públicos e a confiança da população nos serviços digitais oferecidos pelo governo. O Estado estará mais preparado para enfrentar os desafios futuros, adaptando-se continuamente às novas ameaças.

## 2. Aumento da Capacidade e Redundância da Conectividade

Com a ampliação da banda contratada e a introdução de redundância nos acessos por múltiplas tecnologias (banda larga, satélites de baixa ou média órbita e 5G), a nova solução pretende assegurar que os serviços de TIC do Estado sejam mais resilientes e possam suportar uma maior demanda de usuários simultaneamente, sem comprometer o desempenho.

### Resultados Esperados:

- **Melhoria na qualidade e estabilidade das conexões de rede:** Garantia de que os serviços governamentais sejam acessíveis e operacionais mesmo em situações de alta demanda.
- **Redução do tempo de inatividade:** Implementação de conexões redundantes por múltiplas tecnologias que assegurem a continuidade dos serviços, mesmo em casos de falha na rede principal, para isto deve-se contratar uma rede backup, preferencialmente diferente da tecnologia banda larga.
- **Expansão da infraestrutura de TIC:** Suporte a novas iniciativas e maior número de usuários, permitindo um crescimento sustentável das operações digitais do governo.

### 3. Eficiência Operacional e Automação de Processos

A contratação de novos serviços de TIC, incluindo ferramentas de monitoramento, automação de resposta a incidentes e gerenciamento integrado, visa não apenas aumentar a segurança, mas também tornar as operações de TIC mais eficientes e menos dependentes de intervenções manuais.

#### Resultados Esperados:

- **Redução do tempo médio necessário para a resolução de problemas:** Automatização de tarefas e monitoramento contínuo, resultando em uma operação mais ágil e eficaz.
- **Aumento da produtividade das equipes de TIC:** Foco das equipes em atividades de maior valor agregado, enquanto tarefas rotineiras são automatizadas.
- **Melhoria na capacidade de gestão e controle:** Informações em tempo real sobre o estado da rede e das soluções de segurança, permitindo uma tomada de decisão mais informada e ágil.

### 4. Sustentabilidade e Crescimento Sustentável das Operações de TIC

A solução proposta tem como objetivo garantir que as operações de TIC do governo sejam sustentáveis a longo prazo, tanto em termos de segurança quanto de escalabilidade.

#### Resultados Esperados:

- **Capacidade de crescimento sustentável da infraestrutura de TIC:** Adaptação às novas demandas e desafios tecnológicos sem comprometer a segurança ou a eficiência.
- **Adoção de melhores práticas de segurança da informação:** Promoção da conscientização sobre segurança digital, integrando a segurança cibernética em todos os níveis operacionais.

## 14. POSSÍVEIS IMPACTOS AMBIENTAIS

A CONTRATADA responsável pelo serviço da Nova Rede Corporativa deverá adotar práticas de TI Verde para promover a sustentabilidade ambiental e o uso eficiente dos recursos, pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e a prevenir o desperdício de insumos e material consumidos, bem como o consumo excessivo de energia, a fim de atender às diretrizes de responsabilidade ambiental previstas em lei:

- **Resoluções do Conselho Nacional do Meio Ambiente (CONAMA):** Resolução CONAMA nº 416/2009: Dispõe sobre a responsabilidade compartilhada pelo ciclo de vida dos produtos, envolvendo fabricantes, importadores, distribuidores, comerciantes e consumidores.
- **Política Nacional de Resíduos Sólidos (PNRS) - Lei nº 12.305/2010:** Logística Reversa: Define a necessidade de implantação de sistemas de logística reversa para resíduos eletroeletrônicos, visando a devolução dos produtos após o uso pelo consumidor.

- **Norma internacional ISO 50001:** Auxilia as instalações na avaliação e priorização da implementação de novas tecnologias de eficiência energética e na melhoria da eficiência energética, uso e consumo de energia. Também cria transparência e facilita a comunicação sobre a gestão dos recursos energéticos.

Importante que a empresa busque otimizar a eficiência energética nas localidades atendidas pelo projeto e também no Centro Integrado de Inteligência e Segurança Cibernética na ATI, e incorporem a gestão do ciclo de vida dos equipamentos eficiente e sustentável. A adoção de tecnologias certificadas pelo programa Energy Star e o cumprimento da legislação ambiental supracitadas.

## 15. PROVIDÊNCIAS A SEREM ADOTADAS

Para garantir que a execução do contrato referente à nova solução de rede de segurança e conectividade do Estado de Pernambuco ocorra sem obstáculos, é necessário adotar uma série de providências que assegurem a adequação da infraestrutura, a capacitação dos servidores envolvidos e o cumprimento das exigências legais e administrativas. Estas medidas são essenciais para que a transição e a implementação da nova solução ocorram de forma eficiente e segura, evitando problemas que possam comprometer os objetivos do projeto.

### 1. Estruturação Organizacional e de Processos

A implementação da nova solução de segurança e conectividade exige não apenas a adaptação tecnológica, mas também uma reestruturação organizacional e de processos nos órgãos responsáveis, a saber, a Agência Estadual de Tecnologia da Informação de Pernambuco (ATI-PE) e a Secretaria de Administração de Pernambuco (SAD). Essas mudanças visam alinhar as operações e processos internos às novas demandas impostas pela solução, garantindo uma gestão eficiente, segura e que esteja de acordo com as melhores práticas de governança de TIC.

#### Providências:

- **Revisão e Atualização das Políticas de Segurança da Informação:** Os setores do estado responsáveis pela governança de TI estadual deverão revisar e atualizar as políticas de segurança da informação para refletir as novas exigências e capacidades proporcionadas pela solução contratada. Isso inclui a definição de novas diretrizes para o gerenciamento de acessos, proteção de dados e resposta a incidentes de segurança. As políticas revisadas devem ser amplamente divulgadas e implementadas em todos os níveis da organização.
- **Redefinição dos Papéis e Responsabilidades na Gestão de TIC:** A reestruturação organizacional deve incluir a redefinição clara dos papéis e responsabilidades dos servidores e gestores envolvidos na gestão da nova solução de TIC. Os setores do estado responsáveis pela governança de TI estadual precisam assegurar que as equipes tenham uma compreensão precisa de suas funções, especialmente no que tange à operação e monitoramento das novas ferramentas de segurança e conectividade. Isso envolve a designação de responsáveis específicos para áreas críticas, como gestão de incidentes, monitoramento de rede e conformidade regulatória.
- **Integração de Processos de Gestão de Riscos:** Os setores do estado responsáveis pela governança de TI estadual devem implementar um sistema robusto de gestão de riscos que esteja alinhado com as novas soluções de segurança. Isso inclui a identificação proativa de riscos potenciais, a avaliação contínua das ameaças cibernéticas e a implementação de medidas mitigatórias. A gestão de riscos deve ser integrada aos processos operacionais, garantindo que qualquer risco emergente seja rapidamente identificado e tratado.
- **Criação de Comitês Interdepartamentais de TIC e Segurança da Informação:** Para assegurar uma coordenação eficiente entre as diferentes áreas e processos afetados pela nova solução, é essencial a criação de comitês interdepartamentais que envolvam ATI-PE, SAD e outros órgãos relevantes. Esses comitês deve-

rão atuar na formulação de estratégias, na resolução de conflitos operacionais e no acompanhamento contínuo da implementação da solução. Eles também serão responsáveis por alinhar as iniciativas de TIC e segurança da informação às necessidades estratégicas do governo.

- **Desenvolvimento de Procedimentos Operacionais Padrão (POPs) e Protocolos de Resposta a Incidentes:** Os setores do estado responsáveis pela governança de TI estadual deverão desenvolver e implementar Procedimentos Operacionais Padrão (POPs) e protocolos de resposta a incidentes específicos para a nova solução de TIC. Esses procedimentos devem cobrir desde a detecção inicial de ameaças até a resolução completa do incidente, incluindo comunicações internas e externas, mitigação de danos e relatórios pós-incidente. Os POPs devem ser testados regularmente através de simulações para garantir sua eficácia e a prontidão das equipes.

- **Aprimoramento da Gestão Documental e Conformidade:** Os setores do estado responsáveis pela governança de TI estadual devem revisar e aprimorar seus sistemas de gestão documental para assegurar que todas as informações relacionadas à segurança da informação e à operação da rede sejam devidamente registradas, armazenadas e auditadas. Isso inclui o armazenamento seguro de logs, registros de incidentes e documentação de conformidade, garantindo que todas as atividades estejam em conformidade com as normas regulatórias e os requisitos de auditoria.

- **Aprimoramento da Comunicação e Transparência:** Os setores do estado responsáveis pela governança de TI estadual devem estabelecer canais de comunicação claros e transparentes para garantir que todos os servidores e stakeholders envolvidos estejam bem informados sobre os processos, políticas e procedimentos relacionados à nova solução de TIC. A comunicação eficaz é essencial para promover a adesão às novas práticas e para assegurar que todos os envolvidos tenham um entendimento comum dos objetivos e responsabilidades.

## 2. Capacitação de Servidores e Empregados

A complexidade técnica da nova solução de segurança e conectividade exige que os servidores e empregados envolvidos na fiscalização e gestão do contrato estejam devidamente capacitados. Essa capacitação deve abranger tanto as especificidades técnicas das ferramentas e serviços contratados quanto os aspectos administrativos relacionados à gestão contratual.

### Providências:

- Realização de treinamentos específicos sobre as novas tecnologias implementadas, como as ferramentas de segurança cibernética, gerenciamento de acessos e monitoramento de rede.
- Capacitação em gestão de contratos e fiscalização de serviços de TIC, com foco em garantir que os servidores estejam preparados para monitorar a execução do contrato e identificar possíveis desvios ou problemas.
- Workshops sobre melhores práticas em segurança da informação, assegurando que todos os envolvidos estejam cientes das políticas e procedimentos de segurança adotados.

## 3. Adequação do Ambiente Organizacional e Infraestrutura Predial

A implementação da nova solução de segurança e conectividade exige uma adequação tanto do ambiente organizacional quanto da infraestrutura predial para assegurar que as condições necessárias ao funcionamento dos novos sistemas sejam atendidas. A responsabilidade por essas adequações está dividida entre a Contratada, que cuidará dos aspectos técnicos específicos, como a infraestrutura elétrica, rede interna de cabeamento e estrutura de racks, e a Contratante, que cuidará das condições físicas e ambientais dos locais onde os equipamentos serão instalados.

### Providências:

- **Avaliação e Manutenção da Infraestrutura Predial:** A Contratante, por meio dos setores do estado responsáveis pela governança de TI estadual, deve garantir que a infraestrutura predial, incluindo a manutenção de paredes, pisos, tetos e combate a vazamentos, umidade/mofo, esteja em condições adequadas para a instalação dos novos equipamentos. Isso assegura que o ambiente físico não comprometerá o desempenho e a segurança dos sistemas.
- **Climatização Adequada dos Ambientes:** A Contratante é responsável por garantir que os ambientes onde serão instalados os novos equipamentos de TIC possuam sistemas de climatização adequados. A climatização deve ser capaz de manter as condições ambientais necessárias ao funcionamento seguro e eficiente dos servidores e dispositivos de rede, evitando sobrecargas térmicas e garantindo a longevidade dos equipamentos.
- **Segurança Física dos Equipamentos:** Os setores do estado responsáveis pela governança de TI estadual devem implementar e manter medidas de segurança física nos locais onde os equipamentos serão instalados. Isso inclui controle de acesso aos ambientes, monitoramento por câmeras de segurança, e barreiras físicas, para evitar acessos não autorizados e proteger os ativos contra vandalismo e roubo.
- **Proteção e Segurança dos Cabos de Fibra Externos:** Os setores do estado responsáveis pela segurança estadual devem garantir a segurança dos cabos de fibra óptica instalados em áreas externas, prevenindo danos por vandalismo ou intervenções não autorizadas. Isso inclui a implementação de medidas de proteção física e a criação de protocolos para monitoramento contínuo dessas infraestruturas críticas.
- **Monitoramento Contínuo e Resposta a Incidentes:** A Contratante deve estabelecer procedimentos para o monitoramento contínuo da infraestrutura predial e para a resposta rápida a qualquer incidente que possa impactar a operação dos sistemas. Isso envolve a manutenção de equipes de prontidão para resolver problemas relacionados à climatização, segurança física e integridade dos ambientes de instalação.

#### 4. Conformidade Regulatória e Gestão Contratual

A conformidade com as exigências legais e infralegais será responsabilidade da Contratada, que deverá contemplar em sua proposta todas as licenças e autorizações necessárias para a operação dos novos equipamentos e sistemas de segurança. No entanto, é essencial que a Administração (Contratante) assegure a gestão adequada desse processo, monitorando o cumprimento dessas exigências para garantir a legalidade e conformidade da execução contratual.

##### Providências:

- **Monitoramento do Cumprimento das Exigências Regulatórias:** Os setores do estado responsáveis pela segurança estadual devem acompanhar e validar que a Contratada obtenha todas as licenças e autorizações necessárias, garantindo que a operação dos sistemas de TIC esteja em conformidade com as regulamentações vigentes. Isso inclui verificações periódicas e auditorias para assegurar que a documentação esteja atualizada e em conformidade com os requisitos legais.
- **Gestão Contratual e Fiscalização:** ATI-PE e SAD deverão fortalecer suas práticas de gestão contratual e fiscalização para assegurar que todas as cláusulas contratuais relacionadas à conformidade legal sejam rigorosamente cumpridas. Isso inclui a implementação de mecanismos de controle e relatórios regulares para monitorar a conformidade da Contratada ao longo da execução do contrato.
- **Apoio na Obtenção de Autorização de Instalação em Áreas Sensíveis:** Em situações que envolvam a instalação de equipamentos em áreas sensíveis ou de alta segurança, Os setores do estado responsáveis pela segurança estadual devem coordenar com outros órgãos governamentais para garantir que as autorizações necessárias sejam obtidas de maneira eficiente, evitando atrasos na implementação da solução.
- **Treinamento em Normas de Conformidade:** A Contratante deve garantir que as equipes responsáveis pela gestão e fiscalização do contrato estejam bem informadas e treinadas sobre as normas de confor-

midade aplicáveis, assegurando que qualquer desvio ou irregularidade seja identificado e corrigido rapidamente.

- **Documentação e Auditoria de Conformidade:** Os setores do estado responsáveis pela segurança estadual devem implementar processos robustos de documentação e auditoria para garantir que todas as exigências legais e contratuais sejam atendidas, assegurando a rastreabilidade e a transparência durante todo o ciclo de vida do contrato.

## 5. Reforço da Equipe de Fiscalização e Gestão Contratual

Dada a necessidade de uma gestão rigorosa e especializada para a execução do contrato da nova solução de segurança e conectividade, a Administração deve considerar o reforço de sua equipe de fiscalização e gestão contratual. Isso inclui a contratação de novos profissionais capacitados para lidar com as especificidades técnicas e administrativas do contrato, garantindo que todas as etapas sejam realizadas de maneira eficiente e conforme os requisitos contratuais e legais.

### Providências:

- **Contratação de Profissionais Especializados:** A Administração, por meio dos setores do estado responsáveis pela governança de TI estadual, deve realizar a contratação de profissionais especializados, incluindo fiscais técnicos e administrativos, que sejam capacitados para acompanhar de perto a execução do contrato. Esses profissionais devem ter experiência em gestão de contratos de TIC e em áreas específicas como cibersegurança, infraestrutura de rede e gestão financeira.
- **Formação de uma Equipe Multidisciplinar:** É recomendada a formação de uma equipe multidisciplinar que inclua profissionais com conhecimentos em tecnologia da informação, finanças, e administração pública. Essa equipe será responsável por monitorar a execução técnica, validar o cumprimento das cláusulas contratuais, processar pagamentos, aplicar glosas de faturamento quando necessário, e garantir que os fornecedores cumpram todos os requisitos estipulados no contrato.
- **Capacitação Contínua da Equipe de Fiscalização:** Além da contratação de novos profissionais, é essencial garantir que a equipe de fiscalização receba treinamento contínuo em áreas relevantes, como gestão de contratos de TIC, análise de conformidade regulatória, e técnicas de auditoria. Esse treinamento deve ser atualizado regularmente para acompanhar as mudanças tecnológicas e regulatórias que possam impactar o contrato.
- **Implementação de Ferramentas de Gestão e Monitoramento:** A equipe de fiscalização e gestão contratual deve ser apoiada por ferramentas de software que facilitem o acompanhamento do contrato em tempo real, incluindo plataformas de monitoramento de performance, gestão financeira, e controle de conformidade. Essas ferramentas ajudarão a equipe a identificar rapidamente qualquer desvio do contrato e a tomar medidas corretivas imediatas.
- **Estruturação de Processos de Revisão e Auditoria:** A criação de processos formais de revisão e auditoria dentro da equipe de fiscalização é essencial para garantir que todas as atividades relacionadas ao contrato sejam conduzidas de acordo com as melhores práticas. Isso inclui a revisão periódica de relatórios de progresso, a auditoria dos serviços entregues pelos fornecedores, e a validação de todas as faturas antes do processamento de pagamentos.

## 16. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A solução selecionada foi o **Cenário 01**, isto é, a Solução de Rede Corporativa com Segurança e banda larga. Modelo de contratação composto por links banda larga, solução de segurança centralizada com equipamento de última milha, solução de rede sem fio, solução de detecção e resposta à dispositivos finais, monitoramento das operações de segurança, gestão de qualidade e uso dos serviços, processos, pessoas e tecnologias de segurança providos por uma única empresa ou consórcio. Além destes, haverão também itens de serviço complementares, compostos por links multitecnologias redundantes e conectividade de Datacenter em lotes distintos. Destaca-se como a opção mais viável para atender às necessidades do Governo de Pernambuco. Esta escolha é fundamentada na sua agilidade no processo, maior capacidade de gestão e facilidade de implementação. Ao optar pela consolidação da prestação dos serviços, elimina-se a necessidade de aguardar outros processos para sua implementação. Uma vez concluído o processo, o serviço pode ser imediatamente utilizado em sua totalidade, garantindo continuidade e integridade ao longo do processo. Além disso, é importante ressaltar que este modelo de contratação já é uma prática consolidada e bem-sucedida no estado de Pernambuco.

## 17. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Estima-se um valor da contratação de R\$ 2.665.117.088,83 (dois bilhões, seiscentos e sessenta e cinco milhões, cento e dezessete mil, oitenta e oito reais e oitenta e três centavos) para o período de 60 meses do contrato.

CENÁRIO 1 DIVISÃO LOTES x SERVIÇOS	ESTIMATIVA DE TCO AO LONGO DOS ANOS						
	SERVIÇOS	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	VALOR TOTAL DO CONTRATO 5 ANOS
1º LOTE	Segurança + Conectividade	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 444.430.065,74	R\$ 2.222.150.328,72
	Comunicação de Voz	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 64.140.485,56	R\$ 320.702.427,79
	Acesso Satélite	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 8.339.623,20	R\$ 41.698.116,00
2º LOTE	Conectividade entre Datacenters	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 8.390.337,73	R\$ 41.951.688,66
3º LOTE	Avaliação e Mitigação de Riscos Cibernéticos	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 7.722.905,53	R\$ 38.614.527,66
TOTAL	-	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 533.023.417,77	R\$ 2.665.117.088,83

## 18. POSICIONAMENTO CONCLUSIVO

Após uma análise detalhada das necessidades do Governo do Estado de Pernambuco e das soluções disponíveis no mercado, foi selecionada o **Cenário 01** como a opção mais viável para atender às demandas de infraestrutura de TI. A solução escolhida, composta por links de banda larga, uma solução de segurança centralizada com equipamentos de última milha, rede sem fio, detecção e resposta a ameaças em dispositivos finais, monitoramento das operações de segurança, gestão de qualidade, e serviços complementares como links multitecnológicos redundantes e conectividade de Datacenter em lotes distintos, demonstra grande adequação técnica, operacional e orçamentária. A solução proposta atende plenamente às necessidades técnicas e operacionais do Governo de Pernambuco. Ela oferece uma infraestrutura robusta, capaz de garantir segurança cibernética, alta disponibilidade e resiliência, que são essenciais para as operações governamentais. A centralização dos serviços em uma única empresa ou consórcio simplifica a gestão e a coordenação das atividades, reduzindo a complexidade e melhorando a eficiência operacional. Além disso, a capacidade de monitoramento e resposta a incidentes em tempo real reforça a proteção dos ativos críticos do governo, assegurando a integridade e a continuidade dos serviços prestados.

A análise de custo-benefício da solução demonstra que os benefícios potenciais justificam plenamente os custos estimados. Ao consolidar os serviços de segurança e conectividade em poucos contratos, o Governo de Pernambuco consegue obter economias de escala, reduzir despesas operacionais e otimizar a alocação de recursos financeiros. A previsibilidade dos custos e a possibilidade de escalabilidade do serviço, conforme o crescimento do parque computacional, garantem uma gestão orçamentária eficiente e sustentável a longo prazo. A necessidade de uma infraestrutura de TI segura, eficiente e escalável para o Governo de Pernambuco é claramente definida e justificada. A solução escolhida é a mais adequada para atender a essa necessidade, proporcionando uma base tecnológica sólida que suportará o crescimento e a modernização dos serviços públicos no estado. A solução está em plena coerência com as prioridades estratégicas do Governo de Pernambuco, que incluem a modernização da infraestrutura de TI, a garantia de segurança cibernética, e a melhoria contínua dos serviços públicos. A escolha desta solução reflete o compromisso do governo com a inovação e a eficiência, alinhando-se perfeitamente com os objetivos operacionais e estratégicos do estado. A implementação da solução selecionada terá impactos positivos tanto internamente, com a melhoria da eficiência operacional e a segurança dos dados, quanto externamente, com a garantia de serviços públicos mais confiáveis e seguros para a população. A centralização dos serviços e a alta capacidade de gestão permitirão ao Governo de Pernambuco responder de forma mais ágil e eficaz às demandas dos cidadãos e às necessidades emergentes.

Diante da análise abrangente das dimensões técnicas, operacionais, orçamentárias e estratégicas, concluímos que a contratação do **Cenário 01** é a melhor opção. Esta solução atende a todos os critérios necessários para garantir a eficácia, efetividade e eficiência das operações governamentais, e a sua implementação deve prosseguir conforme planejado. Esta decisão é fundamental para assegurar que o Governo de Pernambuco continue a oferecer serviços públicos de alta qualidade, protegendo os dados e as operações críticas do estado, e promovendo a inovação tecnológica necessária para o desenvolvimento sustentável da região.

## 19. RESPONSÁVEIS

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
<hr/> <p>Ítalo Fernando Vasconcelos Sivini Filho</p> <p>Matrícula: 144566/02</p> <p>Superintendente de Conectividade e Infraestrutura de TI</p> <p><b>Contato:</b> (81) 98494-5755</p>	<hr/> <p>Joseilson Albuquerque de França</p> <p>Matrícula: 125286/03</p> <p>Gerente de Telemática do Estado</p> <p><b>Contato:</b> (81) 3183-7775</p>

E-mail: italo.sivini@ati.pe.gov.br

Recife, data da assinatura digital

E-mail: joseilson.franca@sad.ati.pe.gov.br

Recife, data da assinatura digital

## 20. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições do Decreto Estadual nº 53.384, de 22 de agosto de 2022 e da Portaria ATI nº 44 de 30 de dezembro de 2024.

### AUTORIDADE MÁXIMA DA ÁREA DE TIC

**FREDERICO DE VASCONCELOS PEREIRA**

Matrícula: 18187714/02

**Diretor Presidente - Agência Estadual de Tecnologia da Informação**

Recife, data da assinatura digital

### ANEXO B - MODELO DE PROPOSTA

(em papel timbrado do proponente)

(A proposta de preços poderá conter Detalhamentos e Planilhas Estimativas de Custos e Formação de Preços, conforme o caso concreto)

À

SECRETARIA

PROCESSO Nº

PREGÃO ELETRÔNICO Nº/

Prezados Senhores,

Apresentamos e submetemos à apreciação de V.Sas, nossa Proposta de Preços, para o objeto da presente Licitação, de acordo com as exigências estabelecidas no Edital e seus anexos e de acordo com a planilha abaixo detalhada:

LOTE 01										
Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
ADENDO III - SEGURANÇA DE REDE LOCAL										
1	598669-9	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1	UNIDADE	1759	48				
2	598670-2	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2	UNIDADE	1299	48				
3	598672-9	27014	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	193	48				
4	598675-3	27014	Solução para gerenciamento de acessos à rede local - NAC	UNIDADE	24427	48				
ADENDO IV - SERVIÇO DE REDE SEM FIO										
5	598692-3	27014	Serviço de Rede Sem Fio Interno com Segurança	UNIDADE	12892	48				
6	598693-1	27014	Serviço de Rede Sem Fio Externo com Segurança	UNIDADE	500	48				
7	598694-0	27014	Serviço de Rede Sem Fio Temporário com Segurança	UNIDADE	10	6				
8	602034-8	27014	Serviço de fornecimento e implantação de Switch	UNIDADE	716	48				
ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL										
9	598281-2	26174	Link de Acesso Permanente (LAP - Tipo 1)	UNIDADE	2968	48				
10	598282-0	26174	Link de Acesso Permanente (LAP - Tipo 2)	UNIDADE	2212	48				
11	598755-5	26174	Link Multitecnologia Especial (LME) - Tipo 1	UNIDADE	250	48				
12	598757-1	26174	Link Multitecnologia Especial (LME) - Tipo 2	UNIDADE	20	48				
13	598758-0	26174	Link Multitecnologia Especial (LME) - Tipo 3	UNIDADE	20	48				
14	598761-0	26174	Link Acesso Temporário (LAT) - Tipo 1	UNIDADE	30	6				

15	598762-8	26174	Link Acesso Temporário (LAT) - Tipo 2	UNIDADE	20	6				
16	598763-6	26174	Link Acesso Temporário (LAT) - Tipo 3	UNIDADE	20	6				
<b>ADENDO VI - SEGURANÇA DE DATACENTER</b>										
17	598673-7	27014	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER	UNIDADE	6	48				
18	598674-5	27014	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço	UNIDADE	3	48				
19	598677-0	27014	Solução de segurança de confiança zero - ZTNA	UNIDADE	1.221	48				
20	598678-8	27014	Solução de proteção, detecção e resposta para servidores - EDR	UNIDADE	4.200	48				
21	598679-6	27014	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR	UNIDADE	3	48				
22	598680-0	27014	Solução para gerenciamento de acessos à rede datacenter - NAC	UNIDADE	1.221	48				
23	598681-8	27014	Solução de segurança de identidade privilegiada - PAM	UNIDADE	1.221	48				
24	598682-6	27014	Solução de filtro de mensagens indesejadas - ANTISPAM	UNIDADE	129.058	48				
25	598683-4	27014	Solução de Filtro de Aplicações WEB - WAF	UNIDADE	3	48				
<b>ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO</b>										
26	598642-7	27014	Solução de gerenciamento e monitoramento de ativos - ITAM	UNIDADE	1	48				
27	598685-0	27014	Solução de gerenciamento de identidade de acesso - IAM	UNIDADE	629.058	48				
28	598686-9	27014	Solução de monitoramento e análise de eventos de segurança - SIEM	UNIDADE	477.186	48				
29	598687-7	27014	Solução de automação de resposta a incidentes de segurança - SOAR	UNIDADE	1	48				
30	598643-5	27014	Solução para guarda de LOGs	UNIDADE	1	48				
31	598644-3	27014	Serviço de disponibilização de ambiente de testes	UNIDADE	1	48				
32	598645-1	27014	Solução de gerenciamento de serviços de TI - ITSM	UNIDADE	1	48				

33	598688-5	26980	Serviço de resposta à incidentes de cibersegurança sob demanda	HORA	318	48				
34	598646-0	26980	Serviço de análise de segurança de primeiro nível	UNIDADE	1	48				
35	598647-8	26980	Serviço de análise de segurança especializada	UNIDADE	1	48				
36	598648-6	26980	Serviço de acompanhamento de reparos	UNIDADE	1	48				
37	598649-4	26980	Serviço de atenção especializada ao cliente	UNIDADE	1	48				
38	598650-8	26980	Service Desk	UNIDADE	1	48				
39	598651-6	26980	Serviço de operação da rede	UNIDADE	1	48				
40	598653-2	26980	Serviço de análise de qualidade	UNIDADE	1	48				
41	598654-0	26980	Serviço de Coordenação do CIISC	UNIDADE	1	48				
42	598655-9	26980	Núcleo de Redes e Segurança Setorial	UNIDADE	5	48				
43	602102-6	26980	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCSs)	UNIDADE	22	48				
44	598656-7	26980	Serviço de Evolução da Maturidade em Segurança da Informação	UNIDADE	1	48				
<b>ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)</b>										
45	598691-5	1988	Serviço de Comunicação Unificada - SCU (Conta de usuário)	UNIDADE	500	48				
<b>ADENDO XIII - SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE</b>										
46	598696-6	1988	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)	UNIDADE	8199	48				
47	598697-4	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	UNIDADE	8000	48				
48	598698-2	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	UNIDADE	202	48				
49	598699-0	1988	Serviço de Ponto de Voz Fixo com Aparelho de Voz DECT IP (PVF-DECT IP)	UNIDADE	354	48				
50	598700-8	1988	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)	UNIDADE	3298	48				
51	598701-6	1988	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)	UNIDADE	500	48				
52	598703-2	1988	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)	UNIDADE	203	48				

53	598704-0	1988	Serviço PVF-Fone-de-Cabeça	UNIDADE	1223	48				
54	463377-6	1988	Serviço Fixo Inter Estadual	MINUTO	364	48				
55	467295-0	1988	Serviço Fixo Intra Estadual	MINUTO	15.303	48				
56	467296-8	1988	Serviço Fixo Local	MINUTO	84.960	48				
57	467297-6	1988	Serviço Móvel Intra Estadual	MINUTO	137.450	48				
58	467300-0	1988	Serviço Móvel Local	MINUTO	575.533	48				
59	467302-6	1988	Serviço Móvel VC2	MINUTO	23.051	48				
60	467303-4	1988	Serviço Móvel VC3	MINUTO	802	48				
61	467304-2	1988	Serviço Longa Inter Regional Fixo	MINUTO	475	48				
62	598664-8	1988	Serviço Adicional de Acesso SIP (SIP TRUNK)	UNIDADE	21	48				

**ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER**

63	598657-5	1988	Serviço de Contact Center com Recurso de Voz	UNIDADE	250	48				
64	598658-3	1988	Serviço de Contact Center com recurso de Whatsapp	UNIDADE	400	48				
65	598659-1	1988	Serviço de Contact Center com recurso de Redes Sociais	UNIDADE	50	48				
67	598661-3	1988	Serviço de Comunicação por vídeo ou vídeo-chamada	UNIDADE	60	48				
68	598662-1	1988	Serviço de Automatizações e Integrações - Consultoria Inicial	UNIDADE	5	48				
69	598663-0	1988	Serviço de Automatizações e Integrações - Implantação	UNIDADE	100	48				

**ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO DOS SERVIÇOS**

70	598640-0	27120	Suporte de Manutenção (12h x 7d)	UNIDADE	600	48				
71	598641-9	27120	Suporte de Manutenção (24h x 7d)	UNIDADE	500	48				
									<b>TOTAL LOTE 01</b>	

**LOTE 02**

Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
<b>ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATA CENTER</b>										
72	598287-1	26506	Link de Fibra Lan To Lan (L2L)	UNIDADE	4	48				
73	598288-0	26506	Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	12				
74	598289-8	26506	Link para Data Center de 4GB com	UNIDADE	2	12				

			AntiDDoS - Link Internet Trânsito (LIT)							
75	598290-1	26506	Link para Data Center de 6GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	12				
76	598291-0	26506	Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	06				
77	598292-8	26506	Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)	UNIDADE	2	06				
									TOTAL LOTE 02	

LOTE 03										
Seq.	E-FISCO	CATSER	DESCRIÇÃO	UNIDADE	QUANTIDADE	PREVISÃO DE USO EM MESES	VALOR UNITÁRIO	VALOR MENSAL	VALOR UNITÁRIO TOTAL	TOTAL CONTRATO
ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS										
78	598665-6	27324	Serviço de gestão de vulnerabilidades	UNIDADE	4.200	48				
79	598666-4	27324	Serviço de análise forense	HORA	141	48				
80	598667-2	27324	Serviço de análise de segurança ofensiva (Red Team)	UNIDADE	1	48				
81	598668-0	27324	Serviço de testes de intrusão (Pentest)	UNIDADE	10	48				
									TOTAL LOTE 03	

### ANEXO C – SITES GOVERNAMENTAIS COM LINKS INSTALADOS

1. Este Anexo representa a base atual de Pontos Conectados Seguros (PCS) com links instalados, não contemplando eventuais expansões que possam ocorrer ao longo da execução contratual.
2. A tabela contempla localidades com diferentes níveis de complexidade de atendimento, incluindo áreas urbanas, zonas rurais, regiões de difícil acesso, escolas indígenas, comunidades quilombolas e demais unidades distribuídas no território do Estado de Pernambuco, devendo a CONTRATADA estar apta a prover atendimento adequado a essas particularidades, conforme requisitos estabelecidos neste Termo de Referência.
3. As informações constantes neste Anexo, inclusive quanto à indicação do tipo de LAP (LAP 1 ou LAP 2) para cada PCS, possuem caráter meramente estimativo e referencial, tendo sido elaboradas com base nos levantamentos realizados no Estudo Técnico Preliminar (ETP).
4. A indicação do tipo de LAP neste Anexo não configura obrigação de contratação na mesma modalidade, tampouco representa definição definitiva de velocidade ou capacidade a serem implementadas em cada localidade.

5. A definição efetiva do tipo de acesso e de suas características técnicas ocorrerá exclusivamente por meio da emissão da respectiva Ordem de Serviço (OS), observadas as necessidades administrativas e a disponibilidade orçamentária do CONTRATANTE PRINCIPAL ou do CONTRATANTE ADERENTE.

6. A Administração poderá, a seu critério, antes ou durante a execução contratual, sem que tais ajustes configurem alteração indevida do objeto ou gerem direito adquirido à CONTRATADA:

6.1. Alterar o tipo de LAP originalmente estimado, redimensionando velocidades ou capacidades;

6.2. Incluir novos PCSs;

6.3. Excluir PCSs previstos neste Anexo;

6.4. Alterar endereços dos PCSs;

6.5. Promover remanejamentos entre localidades.

7. A CONTRATADA deverá manter capacidade técnica e operacional compatível com as demandas efetivamente formalizadas por meio de Ordem de Serviço, independentemente das estimativas inicialmente indicadas neste Anexo.

Órgão	Nome do Site	Endereço	Bairro	Município	TIPO de LAP	Latitude	Longitude
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - JUPI	Av. Trancredo Neves, mercado Público, S/N	Centro	Jupi	LAP 1	-8,712646	-36,415859
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - São Caetano	Av. Rodolfo Torres, 135	Centro	São Caetano	LAP 1	-8,320545	-36,134777
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Belem de São Francisco	Av. Coronel Caribé, 987	Centro	Belém de São Francisco	LAP 1	-8,750549	-38,959119
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Sanharó	Av. Jurandir De Brito, S/N	Centro	Sanharó	LAP 1	-8,364012	-36,567681

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Sede Recife	Av Caxanga, N.º 2200	Cordeiro	Recife	LAP 1	-8,046711	-34,926931
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Venturosa	Rua FRANCISCO PEREIRA CARVALHO BARROS, S/N	Centro	Venturosa	LAP 1	-8,04756	-34,876961
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Angelim	Rua Nossa Senhora de Lourdes - 2	Centro	Angelim	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Petrolândia	Av. Dos Três Poderes, 59	Centro	Petrolândia	LAP 1	-8,97934	-38,21834
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - São João	Rua Dr. Elpidio Branco, S/N	Centro	São João	LAP 1	-8,875221	-36,366189
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Jataúba	Travessa Dois de Março, S/N	Centro	Jataúba	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Altinho	Rua João Barbosa, 40	Boa Vista	Altinho	LAP 1	-8,483756	-36,05713
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Poção	Rua JOAO CORREIA, 10	Centro	Poção	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Serra Talhada	Av. Afonso Magalhães, S/N	Nossa Sra. Da Conceição	Serra Talhada	LAP 1	-7,985098	-38,290339
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Barreira de Xexéu	Rodovia Br 101, Km 138, S/N	Centro	Xexéu	LAP 1	-8,04574453	-34,92473634
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Mirandiba	Av. José da Silva Taraqua, 92	Centro	Mirandiba	LAP 1	-8,119633	-38,729291
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Itaíba	Rua Nova, nº 50, - CENTRO, Itaíba - PE, 56550-000	Centro	Itaíba	LAP 1	-8,946838	-37,423183
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Afrânio	Rua José Aureliano Rodrigues, 193	Centro	Afrânio	LAP 1	-8,516834	-41,005329
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Paratama	Rua São Luiz, 58	Centro	Paratama	LAP 1	-8,922139	-36,661111
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Sertânia	Rua Manoel Borba, S/N	Centro	Sertânia	LAP 1	-8,069811	-37,260559

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Quipapá	Avenida Rio Branco, 519	Centro	Quipapá	LAP 1	-7,922765	-34,834056
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Bom Conselho	R. Agamenon Magalhães, 274	Centro	Bom Conselho	LAP 1	-9,165229	-36,686375
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - São Bento do Una	Av. Manoel Cândido, 728	Centro	São Bento do Una	LAP 1	-8,523153	-36,446745
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - São José do Belmonte	Rua José Pereira de Barros, 68	Centro	São José do Belmonte	LAP 1	-7,865771	-38,762423
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - IPUBI	Av. Getúlio Vargas, 316	Centro	Ipupi	LAP 1	-7,654887	-40,147531
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Alagoinha	Rua Tenente Dorgival Galindo, 13	Centro	Alagoinha	LAP 1	-8,465451	-36,774987
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Bonito	Rua Joaquim Nabuco, 1092	Centro	Bonito	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Floresta	Rua Major José R Moraes, 196	Centro	Floresta	LAP 1	-8,602252	-38,57502
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Limoeiro	Praça Domingos Rodrigues, 179	Centro	Limoeiro	LAP 1	-7,873363	-35,443697
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Afogados Ingazeira	Rua Padre Luiz Gonzaga Campos De Góis, S/N	São Braz	Afogados da Ingazeira	LAP 1	-7,757206	-37,631238
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Caruaru	Av. Dom Bosco, 4	Maurício de Nassau	Caruaru	LAP 1	-8,280122	-35,968794
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Serrita	Rua Coronel Romão Sampaio, 250	Centro	Serrita	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Parnamirim	Rua Gumercindo Cabral, 105	Centro	Parnamirim	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Bezerros	Rua Frei Caneca, S/N	Centro	Bezerros	LAP 1	-8,227303	-35,753384
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Belo Jardim	Av. Sebastião Rodrigues da Costa - s/n	São Pedro	Belo Jardim	LAP 1	-8,322608	-36,415343

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Terezinha	Rua Abílio Alves de Miranda, 32	Centro	Terezinha	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Ouricuri	Rua Doutor Baltazar C Farias, 6	Centro	Ouricuri	LAP 1	-7,886954	-40,083951
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Escada	Rua JOÃO MANOEL PONTUAL, 118	Centro	Escada	LAP 1	-8,363974	-35,234475
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Carpina	Rua Vidal de Negreiros, S/N	Centro	Carpina	LAP 1	-7,840876	-35,255387
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Santa Maria da Boa Vista	Av. Sete De Setembro, S/N	Centro	Santa Maria da Boa Vista	LAP 1	-8,805663	-39,822072
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Timbaúba	Rua, Tenente João Gomes, 119	Centro	Timbaúba	LAP 1	-7,513693	-35,318072
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Gravatá	Rua Lourenço Correia Melo, 285	Centro	Gravatá	LAP 1	-8,203628	-35,571973
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Garanhuns	Av. Caruaru, 228	Heliópolis	Garanhuns	LAP 1	-8,884513	-36,488843
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Vitória Santo Antão	Rodovia Henrique De Holanda, Br 232, Km 51, S/N	Cajá	Vitória de Santo Antão	LAP 1	-8,11307	-35,286972
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Custódia	Praça Padre Leão, 67	Centro	Custódia	LAP 1	-8,085971	-37,640311

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Exú	Rua Coronel Manoel Aires, S/N	Centro	Exu	LAP 1	-7,512094	-39,719924
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Terra Nova	Rua João Mendes de Sá, S/N	Centro	Terra Nova	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Palmares	Travessa José Américo Miranda - S/N	Centro	Palmares	LAP 1	-8,680326	-35,583103
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Cabrobó	Rua 13 de maio, 96	Centro	Cabrobó	LAP 1	-8,515635	-39,310596
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Goiana	Rua do Coqueiro Morto, S/N	Capuava	Goiana	LAP 1	-7,558314	-35,000369

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Dormentes	Av. Maria Reis de Macêdo, 91	Leonísio Lima	Dormentes	LAP 1	-8,446618	-40,766634
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Águas Belas	Rua Leão Coroado, 53	Centro	Águas Belas	LAP 1	-9,115091	-37,116456
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Petrolina	Av. Das Nações, S/N	Centro	Petrolina	LAP 1	-9,390835	-40,508391
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Tabira	Av. Raimundo Ferreira Pires, 320	João Cordeiro	Tabira	LAP 1	-7,59653396	37,54104295
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - São José do Egito	Av. Adalberto Veras, S/N	Planalto	São José do Egito	LAP 1	-7,461431	-37,271304
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Canhotinho	Rua José Cordeiro de Miranda, 257	Centro	Canhotinho	LAP 1	-8,881913	-36,196438
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Agrestina	Rua Coronel João Guilherme, 8	Centro	Agrestina	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Pesqueira	Av. Joaquim Nabuco, 867	Pitanga	Pesqueira	LAP 1	-8,36138	-36,708682
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Taquaritinga Norte	Rua Padre Berenguer, 69	Centro	Taquaritinga do Norte	LAP 1	-7,903003	-36,041357
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Caetés	Av. Luiz Pereira Junior, S/N	Centro	Caetés	LAP 1	-8,04756	-34,876961
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Cachoeirinha	Rua Siqueira Campos, 52	Centro	Cachoeirinha	LAP 1	-8,488467	-36,236503
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Salgueiro	Rua Presidente Getúlio Vargas, 220	Nossa Senhora Aparecida	Salgueiro	LAP 1	-8,04756	-34,876961
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Palmerina	Av. Desembargador João Paes de Carvalho, S/N	Centro	Palmeirina	LAP 1	-9,003832	-36,326433
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Saloá	Rua JOSE BEZERRA DE LIMA, S/N	Centro	Saloá	LAP 1		
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Lajedo	Rua Rui Barbosa - 26, centro - Lajedo	Centro	Lajedo	LAP 1	-8,663189	-36,322904

AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Bodocó	Av. Presidente Castelo Branco, S/N	Centro	Bodocó	LAP 1	-7,781705	-39,941149
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Buíque	Rua Manoel Barbosa, 40	Centro	Buíque	LAP 1	-8,62317518	-37,15409111
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Arcoverde	Av. Oswaldo CruzP, S/N	Sucupira	Arcoverde	LAP 1	-8,429457	-37,060439
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Lagoa Grande	Rua Estudantes, S/N	Centro	Lagoa Grande	LAP 1	-8,80454859	-39,82196932
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Araripina	Rua Manoel Ferreira Sampaio, 300	Centro	Araripina	LAP 1	-7,577104	-40,506138
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - IGUARACI	Av. José Bezerra Camara, S/N	Centro	Iguaraci	LAP 1	-7,836865	-37,515276
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Manari	Rua Antônio Jorge, 75	Centro	Manari	LAP 1	-8,963397	-37,62537
AGÊNCIA DE DEFESA E FISCALIZAÇÃO AGROPECUÁRIA DE PERNAMBUCO	ADAGRO - Surubim	Rua Severino Clemente de Arruda, 340	Centro	Surubim	LAP 1	-7,839427	-35,761838
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE - Mercado Eufrásio Barbosa	Av. Doutor Joaquim Nabuco, S/N	Varadouro	Olinda	LAP 1	-8,019803	-34,853735
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE - Bezerras	Av. Major Aprígio Da Fonseca, 1100	São Sebastião	Bezerras	LAP 1	-8,24392363	-35,75257778
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE - Petrolina	Adm. Do Distrito Industrial Paulo Coelho, S/N	Centro	Petrolina	LAP 1	-9,396515	-40,532578
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE	Av. Conselheiro Rosa e Silva, 347	Graças	Recife	LAP 1	-8,048479	-34,897028
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE - Recife - Armazém 11	Av. Alfredo Lisboa, S/N	Recife Velho	Recife	LAP 1	-8,06229	-34,87065
AGÊNCIA DE DESENVOLVIMENTO ECONÔMICO DE PERNAMBUCO	ADEPE - E-commerce	Rua Dom Pedro Henrique, 242	Boa Vista	Recife	LAP 1	-8,053198	-34,889271
AGÊNCIA DE FOMENTO DO ESTADO DE PERNAMBUCO S.A.	AGEFEPE - Sede	Rua do Apolo - 81	Recife	Recife	LAP 1	-8,061803	-34,873258

AGÊNCIA DE REGULAÇÃO DOS SERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DE PERNAMBUCO	ARPE - Sede	Av. Cons. Rosa E Silva, 975	Aflitos	Recife	LAP 2	-8,042831	-34,897976
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - Posto Avançado Tamandaré	Av. Jose Bezerra Melo, 1099	Loteamento 11 - Centro	Tamandaré	LAP 1		
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - SETOR TRANSPORTE	Rua Jorge Gomes de Sá, S/N	Santana	Recife	LAP 1	-8,041053	-34,917489
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - Posto Caetes	Rodovia Pe-18, S/N, Km 2 E 1/2	Caetés 1	Abreu e Lima	LAP 1	-7,905479	-34,90495
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - LABORATÓRIO	Praça Faria Neves - s/n	Dois Irmãos	Recife	LAP 1	-8,01583	-34,943609
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - SEDE	Rua Oliveira Góes - 395	Poço da Panela	Recife	LAP 2	-8,03985	-34,920823
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - SEDE	Rua Oliveira Góes - 395	Poço da Panela	Recife	LAP 2	-8,03985	-34,920823
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	Anexo CPRH	Rua Professor Edgar Altino	Poço da Panela	Recife	LAP 1	-8,037025	-34,921686
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - APA de Santa Cruz	Rua SENADOR NILO COELHO, 57	Quatro Cantos	Ilha de Itamaracá	LAP 1	-7,73874	-34,824759
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - PETROLINA	Av. Tancredo Neves, S/N	Centro	Petrolina	LAP 1	-8,03963683	-34,92065234
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	IBAMA - MATA DO PASSARINHO	Estrada do passarinho, S/N	Passarinho	Olinda	LAP 1	-7,992766	-34,906709
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - ARARIPINA	RUA ANTONIO ALEXANDRE ALVES, 113	SANTA IZABEL	Araripina	LAP 1	-7,58308289	-40,50062507
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - NAZARÉ DA MATA	Praça Calábria Veiga	Centro	Nazaré da Mata	LAP 1		
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - CARUARU	Avenida José Marques Pontes, 469	Indianópolis	Caruaru	LAP 1	-8,285608	-35,967036
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - Gurjau	Rua Capela, S/N	Gurjáú	Cabo de Santo Agostinho	LAP 1	-7,880442	-34,832776
AGÊNCIA ESTADUAL DE MEIO AMBIENTE	CPRH - GARANHUNS	RUA JOAQUIM PÁRORA, S/N	ELIÓPOLES	Garanhuns	LAP 1		
Agência Estadual de Meio Ambiente e Recursos Hídricos	CPRH - SERRA TALHADA	Avenida Afonso Magalhães - s/n, Centro de Serra Talhada, SERRA TALHADA - PE		Serra Talhada	LAP 1	-7,985366	-38,290517
Agência Estadual de Meio Ambiente e Recursos Hídricos	CPRH - CETAS	Rodovia PE 16, KM 08, Estrada da Mumbeca	Aldéia	Recife	LAP 1	-7,94621378	-34,97985617
AGÊNCIA ESTADUAL DE PLANEJAMENTO E PESQUISAS DE PERNAMBUCO	Condepe - Fidem - Sede - Jauvaro	Av. Conde da Boa Vista - 1450, Boa Vista, 8º e 9º andar - Boa Vista - Recife-PE	Boa Vista	Recife	LAP 1	-8,056169	-34,89345
AGÊNCIA ESTADUAL DE PLANEJAMENTO E PESQUISAS DE PERNAMBUCO	Condepe - Fidem - Sede - Jauvaro	Av. Conde da Boa Vista - 1450, Boa Vista, 8º e 9º andar - Boa Vista - Recife-PE	Boa Vista	Recife	LAP 1	-8,056169	-34,89345
AGÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO	LIGA GD - Novo Endereço	Rua Cais do Apolo	Recife Velho	Recife	LAP 2	-8,062744	-34,872516

AGÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO	CeSU - Central de Serviços Única	Rua DO BOM JESUS, 156	Recife Antigo	Recife	LAP 1	-8,04756	-34,876961
AGÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO	Agência Estadual de Tecnologia da Informação	Av. Rio Capibaribe, 147	São José	Recife	LAP 2	-8,04756	-34,876961
AGÊNCIA PERNAMBUCANA DE ÁGUAS E CLIMA	APAC - Chã Grande	Água Fria	Zona Rural	Chã Grande	LAP 1	-8,190571	-35,458015
AGÊNCIA PERNAMBUCANA DE ÁGUAS E CLIMA	Agência Pernambucana de Águas e Clima - APAC - Recife	Av.Cruz Cabugá, 1111	Santo Amaro	Recife	LAP 2	-8,04469029	-34,87532663
AGÊNCIA PERNAMBUCANA DE ÁGUAS E CLIMA	Agência Pernambucana de Águas e Clima - APAC - Recife	Av.Cruz Cabugá, 1111	Santo Amaro	Recife	LAP 2	-8,04756	-34,876961
ASSEMBLÉIA LEGISLATIVA DO ESTADO DE PERNAMBUCO	Assembleia Legislativa de Pernambuco - ALEPE	Rua Uniao, 439	Boa Vista	Recife	LAP 1	-8,0581997	-34,88019188
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Almoxarifado Noronha	Rua Vila 30, S/N	Centro	Fernando de Noronha	LAP 1		
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Palácio São Miguel	Vila Dos Remedios, S/N	Vila dos remédios	Fernando de Noronha	LAP 1	-3,8411893	-32,41085936
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Residencia Funcional Administrador	Br 363, S/N	Centro	Fernando de Noronha	LAP 1	-3,863789	-32,428244
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Residencia Funcional Diretoria (casa de pedra)	Rua Floresta Nova, S/N	Casa de Pedra	Fernando de Noronha	LAP 1	-3,84806	-32,410698
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Núcleo de Vigilância Animal	Rua DOM JUQUINHA, S/N	Vila do Trinta	Fernando de Noronha	LAP 1	-3,846101	-32,4084
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Casa Estudante Defn	Rua Arnobio Marques, 320	Santo Amaro	Recife	LAP 1	-8,046298	-34,888042
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Fernando Noronha - Aeroporto	Vila Trinta, S/N	Vila do Sueste	Fernando de Noronha	LAP 1	-3,85627002	-32,42782051
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Sede Distrito Memorial Noronhense	Complexo Turístico do Cachorro, S/N	Memorial Noron	Fernando de Noronha	LAP 1		

AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	ESCOLA DE REFERENCIA EM ENSINO MEDIO ARQUIPELAGO DE FERNANDO DE NORONHA	Floresta Nova, S/N	Rocas	Fernando de Noronha	LAP 1	-3,84704214	- 32,41410786
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Porto Sto Antonio Noronha	Porto Sto Antonio , S/N	Centro	Fernando de Noronha	LAP 1	-3,834297	-32,400425
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Posto de Saúde Familiar - Fernando de Noronha	BR 363, S/N	Floresta Nova	Fernando de Noronha	LAP 1	-3,84750038	- 32,41426672
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Creche Bem Me Quer	Rua Don Juquinha Primeiro, S/N	Vila dos remédios	Fernando de Noronha	LAP 1	-3,84603	-32,429138
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Fernando Noronha - Tv Golfinho	Rua Floresta Nova, S/N	Alameda das Acácias	Fernando de Noronha	LAP 1	-3,847939	-32,413368
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Conselho Tutelar Noronha	Vila Floresta Nova, Br 363, S/N	Vila Boldro	Fernando de Noronha	LAP 1	-3,84806	-32,410698
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Hospital São Lucas	Floresta Nova, S/N	Rocas	Fernando de Noronha	LAP 1	-3,84806	-32,410698
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Hotel de Trânsito	Vila da Basinha S/N- Hotel de Transito - PE	Centro	Fernando de Noronha	LAP 1	-3,842581	-32,410638
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Conselho Distrital Noronha	Rua Nice Cordeiro, 137	Vila dos remédios	Fernando de Noronha	LAP 1	-3,84767682	- 32,41522203
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Sede Distrito Oficina	BR 363 Rodovia Miguel Arraes de Alencar, S/N	Vila dos Remédios	Fernando de Noronha	LAP 1	-3,849111	-32,417495
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	HANG LOOSE	Vila do DPV - s/n	Vila do DPV	Fernando de Noronha	LAP 1	-3,849878	-32,438786
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Sede Usina Residuos Solidos	Vila da Barzinha, S/N	Centro	Fernando de Noronha	LAP 1		

AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Biblioteca Pública	Rua Alameda Armonia, 534	Centro	Fernando de Noronha	LAP 1	-3,847037	-32,411543
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Escritorio Fernando de Noronha - Recife	Av. Rio Capibaribe, 147, 6º andar	São José	Recife	LAP 2	-8,066551	-34,884418
AUTARQUIA TERRITORIAL DISTRITO ESTADUAL DE FERNANDO DE NORONHA	Escritorio Fernando de Noronha - Recife	Av. Rio Capibaribe, 147, 6º andar	São José	Recife	LAP 2	-8,06643751	-34,88474773
CENTRO INTEGRADO SAÚDE AMAURY DE MEDEIROS	Centro de Saúde Amaury Medeiros- CISAM - Maternidade	Rua: Visconde De Mamanguape - S/N	Encruzilhada	Recife	LAP 1	-8,037678	-34,887591
COMPANHIA EDITORA DE PERNAMBUCO	CEPE - Companhia Editora de Pernambuco	Rua Coelho Leite, 530	Santo Amaro	Recife	LAP 1	-8,049808	-34,879918
COMPANHIA EDITORA DE PERNAMBUCO	Livraria CEPE - Mercado Eufrásio Barbosa	Av. Doutor Joaquim Nabuco, S/N	Varadouro	Olinda	LAP 1	-7,97611	-34,86363
COMPANHIA EDITORA DE PERNAMBUCO	CEPE - CGGD	BR101	complexo CONIMULTIMODAL	Cabo de Santo Agostinho	LAP 1	-7,601236	-34,97989
COMPANHIA ESTADUAL DE HABITAÇÃO E OBRAS	Companhia Estadual de Habitação e Obras - CEHAB	Rua Odorico Mendes, 700	Campo Grande	Recife	LAP 2	-8,04756	-34,876961
COMPANHIA ESTADUAL DE HABITAÇÃO E OBRAS	Companhia Estadual de Habitação e Obras - CEHAB	Rua Odorico Mendes, 700	Campo Grande	Recife	LAP 2	-8,03848029	-34,87976392
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Sede	Av. Cruz Cabugá, 1387	Santo Amaro	Recife	LAP 1	-8,043492	-34,874702
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Eal Sairé	Travessa Doutor Mario Ramos, S/N	Centro	Sairé	LAP 1	-8,327547	-35,709348
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Eal Tratamento Esgoto - Vitoria Santo Antao	Av. Henrique de Holanda, S/N	Caja	Vitória de Santo Antão	LAP 1	-8,117565	-35,302307
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Elo Brejo da Madre de Deus	Rua Joaquim Nabuco, 81	Centro	Brejo da Madre de Deus	LAP 1	-8,147963	-36,371254
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Eal Ipubi	Rua Princesa Izabel, S/N	Centro	Ipubi	LAP 1	-7,652818	-40,149104
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Cas - Correntes	Praça da Conceição, 80	Centro	Correntes	LAP 1	-9,130661	-36,327356
COMPANHIA PERNAMBUCANA DE SANEAMENTO	COMPESA - Loja de Atendimento - Vila De Jatoba	Av. CARUARU, 50	Centro	Jatobá	LAP 1	-9,174172	-38,266073
COMPANHIA PERNAMBUCANA DE SANEAMENTO	Compesa - Eal - Serrita	Av. Coronel Chico Romão, 565	Centro	Serrita	LAP 1	-7,946274	-39,298281
COMPLEXO INDUSTRIAL PORTUÁRIO GOVERNADOR ERALDO GUEIROS - SUAPE	Suape / Administração Sede	Complexo Industrial Portuário Suape, Rodovia PE-60,Km10 - ED.EDUARDO CAMPOS - 6º	Suape	Ipojuca	LAP 2	-8,363457	-35,00882

COMPLEXO INDUSTRIAL PORTUÁRIO GOVERNADOR ERALDO GUEIROS - SUAPE	Suaape / Torre de Controle	Rodovia Pe-60, S/N, Suaape	Zona Industrial de Suaape	Ipojuca	LAP 1		
COMPLEXO INDUSTRIAL PORTUÁRIO GOVERNADOR ERALDO GUEIROS - SUAPE	Suaape / Administração Porto	Rodovia Pe-60, S/N		Ipojuca	LAP 1	-8,28346	-35,028555
CONSELHO ESTADUAL DE DEFESA DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE	Conselho Estadual Defesa dos Direitos Criança e do Adolescente - CEDCA - Sede	Rua Barão de São Borja, 526	Boa Vista	Recife	LAP 1	-8,060418	-34,890391
CONSÓRCIO DE TRANSPORTES DA REGIÃO METROPOLITANA DO RECIFE LTDA	Transporte da Região Metropolitana do Recife	Rua do Brum - 275	Recife Antigo	Recife	LAP 1	-8,007508	-34,902601
CONSÓRCIO DE TRANSPORTES DA REGIÃO METROPOLITANA DO RECIFE LTDA	Grande Recife Consórcio Transporte - Armazém 13	Av. Alfredo Lisboa, s/n	Bairro do Recife	Recife	LAP 1	-8,060814	-34,870314
CONSÓRCIO DE TRANSPORTES DA REGIÃO METROPOLITANA DO RECIFE LTDA	Grande Recife Consórcio Transporte - Armazém 13	Av. Alfredo Lisboa, s/n	Bairro do Recife	Recife	LAP 2	-8,060815	-34,870316
CONSÓRCIO DE TRANSPORTES DA REGIÃO METROPOLITANA DO RECIFE LTDA	Grande Recife Consórcio Transporte - Armazém 13	Av. Alfredo Lisboa, s/n	Bairro do Recife	Recife	LAP 2	-8,072225	-34,879253
COORDENADORIA ESTADUAL DE PROTEÇÃO E DEFESA DO CONSUMIDOR	Procon - Aeroporto	Praça Ministro Salgado Filho, S/N	Imbiribeira	Recife	LAP 1		
COORDENADORIA ESTADUAL DE PROTEÇÃO E DEFESA DO CONSUMIDOR	PROCON - Sede	Rua Floriano Peixoto, 141	Santo Antonio	Recife	LAP 1	-8,065814	-34,88229
COORDENADORIA ESTADUAL DE PROTEÇÃO E DEFESA DO CONSUMIDOR	COORDENADORIA GERAL DE PROTEÇÃO E DEFESA DO CONSUMIDOR	RUA DJALMA FARIAS, 250	TORREÃO	Recife	LAP 1	-8,040259	-34,884077
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4º SB / 2º GB - Belo Jardim	Rua Jose Romero C Pereira, S/N	Floresta	Belo Jardim	LAP 1	-8,343329	-36,41567
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2ºSB / 3ºGB - Afogados da Ingazeira	PE-320, S/N	Padre Pedro Pereira	Afogados da Ingazeira	LAP 1	-7,73301303	-37,64266202
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 7º GB - Carpina	Av. Conselheiro João Alfredo, nº 391	Santa Cruz	Carpina	LAP 1	-7,8471	-35,246219
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º SB / 4º GB - Santa Maria da Boa Vista	Rua Dióscoro de Sá Gonzaga	Centro	Santa Maria da Boa Vista	LAP 1	-8,80569345	-39,82309038

CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3º GB - Serra Talhada	Av. Vicente Inácio de Oliveira, S/N	Alto do Bom Jesus	Serra Talhada	LAP 1	-7,981335	-38,304978
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3º GB - Serra Talhada	Av. Vicente Inácio de Oliveira, S/N	Alto do Bom Jesus	Serra Talhada	LAP 1	-7,981335	-38,304978
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - SBFN - Gseção de Bombeiros de Fernando de Noronha	Vila Do Dpv-Sci, S/N	Centro	Fernando de Noronha	LAP 1	-3,845188	-32,428319
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - DTIC	Av. João de Barro, Nº399	Centro	Recife	LAP 1	-8,051194	-34,890324
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3ºSB / 7ºGB - Macaparana	Rua Severino Costa, S/N	Centro	Macaparana	LAP 1	-7,55377	-35,447575
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - ABMG - Link Secundário	Rod Br 232 S/N	Curado	Jaboatão dos Guararapes	LAP 1	-8,066732	-34,942133
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3ºSB / 3ºGB - São José do Egito	Av. 25 de agosto, S/N	Planalto	São José do Egito	LAP 1	-7,468483	-37,274647
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º SB / 7º GB - Goiana	PE-75 - 200	Alvorada	Goiana	LAP 1	-7,566504	-35,011299
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3º SAPH / GBAPH - São Lourenço	Rua Pedro Correia, N.º 499	Centro	São Lourenço da Mata	LAP 1	-7,994793	-35,036758
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 6º SB / 2º GB - Toritama	RAIMUNDO JOSE DA SILVA	DEUS É FIEL	Toritama	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - CAT ST - 3º SATEC - PA Afogados da Ingazeira	Rua José de Sá Maranhão, Afogados da Ingazeira - PE		Afogados da Ingazeira	LAP 1	-7,747562	-37,645421
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - CMan - Porto	Rua Carlos Salazar Sn	Recife	Recife	LAP 1	-8,049536	-34,870218
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 6º GB - Garanhuns	Rua Pedro Rocha, 131	Heliópolis	Garanhuns	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 6º GB - Garanhuns	Rua Pedro Rocha, 131	Heliópolis	Garanhuns	LAP 1	-8,88357	-36,486475
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	CI (Centro de Inteligência)	Avenida Visconde de Suassuna	Boa Vista	Recife	LAP 1	-8,052774	-34,885599
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 5º GB - Salgueiro	Rua João Veras de Siqueira, 2020	Nossa Senhora das Graças	Salgueiro	LAP 1	-8,079976	-39,130051
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - GBS - Grupamento de Bombeiros de Salvamento	Av. Dr. Rinaldo Pinho Alves S/Nº	Dist. Industrial	Abreu e Lima	LAP 1	-7,934715	-34,888988
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2ºSB / 6ºGB - Bom Conselho	Capitão Lizimaco, SN	Centro	Bom Conselho	LAP 1	-9,169878	-36,680479
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - QCG SEDE - Boa Vista	Av. João De Barros, 399	Boa Vista	Recife	LAP 2	-8,051374	-34,891143
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º SAPH / GBAPH - Igarassu	Br 101 Norte Nº 26	Centro	Igarassu	LAP 1	-7,88574	-34,904338

CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - CAT ST - 4ª SATEC - Arcoverde	Rua Augusto Cavalcanti, S/N	Centro	Arcoverde	LAP 1	-8,418986	-37,059064
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4ª SB / 5ª GB - Ouricuri	Rua Bela Vista, S/N	Nossa Sra. de Fátima	Ouricuri	LAP 1	-7,88259797	-40,8132964
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 9ª GB Arcoverde	BR 232, Km 254	São Cristóvão	Arcoverde	LAP 1	-8,424026	-37,040051
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3ª SB / GBI - Suape	Engenho Massangana, S/N	Engenho Massangana	Ipojuca	LAP 1	-8,357744	-35,017674
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - Diretoria de Assistência Social (DAS)	Avenida João de Barros, 380	Boa Vista	Recife	LAP 1	-8,051432	-34,889809
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - SATEC CAT SERTÃO - Serra Talhada	Vicente Inácio de Oliveira, Km 411	Alto do Bom Jesus	Serra Talhada	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 5ª SB / 2ª GB - Santa Cruz do Capibaribe	Pe-160, Km 12, S/N	Bela Vista	Santa Cruz do Capibaribe	LAP 1	-7,95110505	-36,22503702
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4ª SB / 3ª GB - Petrolândia	Av. Deputado Nilvener Cruz Lima, S/N	Centro	Petrolândia	LAP 1	-8,987183	-38,221931
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - DINTER 1 - Caruaru	Rua Quintino Bocaiuva, 400	Maurício de Nassau	Caruaru	LAP 1	-8,27336	-35,975044
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - CAT ST - 6ª SATEC - Petrolândia	Praça dos três poderes. 41	Centro	Petrolândia	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - GBAPH - Olinda	Av. Presidente Kennedy, N.º 145	Varadouro	Olinda	LAP 1	-8,020091	-34,856747
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 1ª GB - Vitória de Santo Antão	Rod Pe 45, S/N	Centro	Vitória de Santo Antão	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 1ª GB - Vitória de Santo Antão	Rod Pe 45, S/N	Centro	Vitória de Santo Antão	LAP 1	-8,125156	-35,283694
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4ª GB - Petrolina	Av. Senador Nilo Coelho, 155	Gercino Coelho	Petrolina	LAP 1	-9,390806	-40,510365
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4ª GB - Petrolina	Av. Senador Nilo Coelho, 155	Gercino Coelho	Petrolina	LAP 1	-9,390806	-40,510365
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - GBI - Grupamento de Bombeiros de Incêndio	Rua Arão Lins De Andrade, Nº 1043	Piedade	Jaboatão dos Guararapes	LAP 1	-8,163855	-34,922654
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - GBMar - Jaboatão	Av Beira Mar 606	Piedade	Recife	LAP 1	-8,156424	-34,909891
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - CAT ZM - 2ª SATEC - Goiana	Rua Duque de Caxias, S/N	Centro	Goiana	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2ªSB / 9ªGB - Pesqueira	BR 232, KM 208	Prado	Pesqueira	LAP 1		
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2ª SB - 1ª GB - Palmares	Av. Ministro Marcos Freire, S/N	Santa Rosa	Palmares	LAP 1	-8,685579	-35,586021

CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3ºSB / 9ºGB - Custódia	Rua Francisco Rodrigues de Resende	Centro	Custódia	LAP 1	-8,085276	-37,648277
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º SB / 2º GB - Bezerras	Av. Francisca Lemos, S/N	São Pedro	Bezerras	LAP 1	-8,237995	-35,748875
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3º SB / 1º GB - Gravatá	Rua 15 de Novembro, SN	Santo Antônio	Gravatá	LAP 1	-8,197283	-35,55993
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 4ºSB / 7ºGB - Surubim	AV. SENADOR PAULO PESSOA GUERRA	CABACEIRA	Surubim	LAP 1	-7,84471132	-35,75563002
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 3ºSB / 5ºGB - Araripina	Travessa Florentino Alves Batista - 253	Centro	Araripina	LAP 1	-7,57656	-40,497632
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º GB - Caruaru	Rua Cel. Fernandes Pontes Filho, S/N	Pinheirópolis	Caruaru	LAP 1	-8,295735	-35,989639
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - 2º GB - Caruaru	Rua Cel. Fernandes Pontes Filho, S/N	Pinheirópolis	Caruaru	LAP 1	-8,295735	-35,989639
CORPO DE BOMBEIROS MILITAR DE PERNAMBUCO	Bombeiros - ABMG - Academia Bombeiro Militar dos Guararapes	Br 232, S/N - Km 9,5	Curado	Recife	LAP 2	-8,078418	-34,985184
CORREGEDORIA DA SECRETARIA DE DEFESA SOCIAL	Corregedoria / Anexo	Avenida Conde Da Boa Vista, 428	Boa Vista	Recife	LAP 2	-8,060171	-34,884973
DEFENSORIA PÚBLICA DO ESTADO DE PERNAMBUCO	Defensoria Pública de Pernambuco - Marquês	Rua Marquês do Amorim, 127	Boa Vista	Recife	LAP 1	-8,061743	-34,890016
DEFENSORIA PÚBLICA DO ESTADO DE PERNAMBUCO	Defensoria - Sede Administrativa	Av. Manoel Borba, 640	BOA VISTA	Recife	LAP 1	-8,059588	-34,889975
DEFENSORIA PÚBLICA DO ESTADO DE PERNAMBUCO	Defensoria Pública de Pernambuco - José de Alencar	Avenida Conde da Boa Vista, Edf. Emp. José Maria - 1450	Boa Vista	Recife	LAP 1	-8,056169	-34,89345
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 5 Dod - Sertania	Av. Agamenon Magalhães, 415	Centro	Sertânia	LAP 1	-8,070271	-37,266055
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	Der 2 Dod Carpina	Av. Estacio Coimbra, S/N	São José	Carpina	LAP 1	-7,845567	-35,253715
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 7º Dro - Garanhuns	Av. Irga, 210	Severino Moraes Filho	Garanhuns	LAP 1	-8,874738	-36,467783
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - Sede	Av. Cruz Cabugá, 1033	Santo Amaro	Recife	LAP 1	-8,045666	-34,87647
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - Sede	Av. Cruz Cabugá, 1033	Santo Amaro	Recife	LAP 1		

DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - Bprv - Posto 06 Gaibú	Pe 60 Km 5		Cabo de Santo Agostinho	LAP 1	-8,438609	-35,082827
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 3º Dro - Caruaru	Praça Coronel Porto, 174	Nossa Sra. das Dores	Caruaru	LAP 1	-8,28767555	-35,97606873
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 8º Dro - Petrolina	Av. Clementino Coelho, S/N	Centro	Petrolina	LAP 1		
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	Policial Rodoviária Estadual - Muro Alto	Rodovia Pe09 - S/N	Porto de Galinhas	Ipojuca	LAP 1	-8,476443	-34,999283
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - Parque Rodoviário	Av Mascarenha de Moraes 4232	Imbiribeira	Recife	LAP 1	-8,096344	-34,909605
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 6º Dro - Salgueiro	Av. Presidente Getúlio Vargas, 500	Nossa Sra. Aparecida	Salgueiro	LAP 1	-8,07268007	-39,12990191
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - 4º Dod Ribeirão	Av. Mario Domingues, 518	Centro	Ribeirão	LAP 1	-8,379705	-35,450933
DEPARTAMENTO DE ESTRADAS DE RODAGEM DO ESTADO DE PERNAMBUCO	DER - BPRV POSTO 02 - CATENDE	Rodovia PE-120, Km 1, S/N	Niterói	Catende	LAP 1	-8,636528	-35,766981
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Posto Prefeitura Custódia	Av. Inocencio Lima, 826	Centro	Custódia	LAP 1	-8,087854	-37,647986
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Paudalho	Av. Miguel Arraes - s/n	Centro	Paudalho	LAP 1	-7,897941	-35,176352
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Inajá	Travessa Cícero Torres, S/N	Centro	Inajá	LAP 1	-8,901645	-37,825018
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Ipojuca	RODOVIA PE-60 KM 18, S/N	Centro	Ipojuca	LAP 1	-8,28346	-35,028555
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran Posto Prefeitura - Parnamirim	Rua Carlos Viana, S/N	Bomba	Parnamirim	LAP 1	-8,091661	-39,572032

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Posto de Atendimento Casa Forte (Cetran)	Rua Dr. José Maria - 1163	Tamarineira	Recife	LAP 1	-8,034867	-34,901762
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Shopping Guararapes	Rua S Sebastiao, 1	Piedade	Jaboatão dos Guararapes	LAP 1	-8,168336	-34,91921
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Posto Prefeitura - Lagoa de Itaenga	Praça Da Bandeira, 134	Centro	Lagoa do Itaenga	LAP 1	-7,932555	-35,291057
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Bonito	Av. Dr.Alberto De Oliveira, 170	Centro	Bonito	LAP 1		
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - São José do Egito	Rua 25 de Agosto 421, S/N	Centro	São José do Egito	LAP 1	-7,472158	-37,274376
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Shopping Center Tacaruna	Av. Gov. Agamenon Magalhães, 153	Santo Amaro	Recife	LAP 1	-8,038761	-34,871189
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Vitória de Santo Antão	Rua Henrique De Holanda, 70	Centro	Vitória de Santo Antão	LAP 1	-8,116299	-35,296506
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Cachoeirinha	Rua Dr. Manoel Borba, 201	Centro	Cachoeirinha	LAP 1	-8,489382	-36,234407
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Barreiros	Av. Felisbino Vasconcelo, 43	Centro	Barreiros	LAP 1	-8,812299	-35,202895
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Sede	Estrada Do Barbalho, 889	Iputinga	Recife	LAP 1	-8,030762	-34,939537
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Sede	Estrada Do Barbalho, 889	Iputinga	Recife	LAP 2	-8,031185	-34,940015
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Sede	Estrada Do Barbalho, 889	Iputinga	Recife	LAP 2	-8,031185	-34,940015
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - São Caetano	Rua Salustiano F De Lima, S/N	Centro	São Caetano	LAP 1		
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Pesqueira	BR-232, km 210, nº 04	Vila Anápolis	Pesqueira	LAP 1	-8,162778	-34,916179
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Cabo	Rodovia PE 60, 237	Santo Inácio	Cabo de Santo Agostinho	LAP 1	-8,413663	-35,073291

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Canhotinho	Rua Barão De Rio Branco, 286	Centro	Canhotinho	LAP 1	-8,88147	-36,19084
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Macaparana	Av. Jose Leitao de Melo, 230	Centro	Macaparana	LAP 1	-7,554303	-35,446331
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Araripina - Mig	Av. Governador Muniz Falcão, S/N	Zonarural	Araripina	LAP 1	-7,584046	-40,502083
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Cabrobó	Rua Alexandre Francisco De Sá, 1008	Centro	Cabrobó	LAP 1	-8,510015	-39,313455
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Caruaru	Br 104, Km 04, S/N	Centro	Caruaru	LAP 1	-8,229668	-35,979333
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Petrolina	Av. Monsenhor Angelo Sampaio, S/N	Areia Branca	Petrolina	LAP 1	-9,382063	-40,488673
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran Lagoa do Carro	Antigo: Rua Dr José Mariano, 87	Centro	Lagoa do Carro	LAP 1	-7,843636	-35,310801
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Sanharó - Posto Prefeitura	Av. 18 de Copacabana, 768	Centro	Sanharó	LAP 1	-8,361511	-36,562978
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Abreu e Lima	Rua - A, S/N	Centro	Abreu e Lima	LAP 1	-7,90739642	-34,90059985
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Altinho	Av. Manuel Borba, 98	Centro	Altinho	LAP 1	-8,489176	-36,059206
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Toritama	Rua 13 de Maio, S/N	Centro	Toritama	LAP 1	-7,5583	-35,005186
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran Shopping Camara	Rua Manoel Honorato da Costa, Vila da Fábrica.	Camaragibe	Camaragibe	LAP 1	-7,988889	-34,9725
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Belo Jardim - Mig	Rodovia Br232 - Km 181, S/N	Floresta	Belo Jardim	LAP 1	-8,33303	-36,418981
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Catende	Rua Coronel Mendo Sampaio, 35	Centro	Catende	LAP 1	-8,670725	-35,720596
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Jaboatão Guararapes - Mig	Rua Desembargador Henrique Capitulino, S/N	Centro	Jaboatão dos Guararapes	LAP 1	-8,112584	-35,015107

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran Shopping Costa Dourada	Rodovia Pe-60, 3200	Garapu	Cabo de Santo Agostinho	LAP 1	-8,305774	-35,022165
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran-Deposito Br 101	Av. da Recuperação, 95	Iputinga	Recife	LAP 1	-8,022294	-34,943147
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Posto do Detran - Fernando de Noronha	Centro de Convivência, s/n	Vila do Trinta	Fernando de Noronha	LAP 1	-3,8467	-32,406412
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	SHOPPING PAULISTA NORTH WAY	RODOVIA PE 15, MEGA LOJA 07, S/N	Centro	Paulista	LAP 1	-7,982633	-34,856573
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran Shopping Igarassu	Av. Mario Melo, PE - 35 - KM 1 - CE - s/n	Centro	Igarassu	LAP 1	-7,822705	-34,908268
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Gravata	Av. Gov. Agamenon Magalhães, 220	Prado	Gravatá	LAP 1	-8,200317	-35,563717
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Shopping Difusora - Caruaru	Av. Agamenom Magalhães 444	Maurício de Nassau	Caruaru	LAP 1	-8,277779	-35,971877
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Garanhuns	Av. Irga S/N	Heliópolis	Garanhuns	LAP 1	-8,883924	-36,481016
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Posto de Atendimento - Lagoa do Ouro	Rua Do Progresso, 62	Centro	Lagoa do Ouro	LAP 1	-9,125002	-36,460343
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran Posto Prefeitura Lagoa Grande	Rua Dom Pedro II, 30	Centro	Lagoa Grande	LAP 1	-8,664222	-36,31982
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Shopping Plaza	Rua Dr Joao Santos Filho, 255	Santo amaro	Recife	LAP 1	-8,036893	-34,912604
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Tacaibó	Travessa Major João Gomes, S/N	Tacaibó	Tacaibó	LAP 1	-8,321062	-36,290674
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Itaiba	Praça Francisco Martins, 50	Centro	Itaiba	LAP 1	-8,962029	-37,254407
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Departamento de Controle de Taxi e Coletivos - Dovt	Rua Professor Joaquim Cavalcanti, 859	Iputinga	Recife	LAP 1	-8,030775	-34,943188
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Paulista - Mig	Rua Primavera, S/N		Paulista	LAP 1	-7,923448	-34,831767

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Agrestina - Posto Prefeitura	Rua HERMOGENES VIEIRA DA CUNHA, 15	Centro	Agrestina	LAP 1	-8,4532934	-35,94536547
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Triunfo	Rua Olavo Gomes De Oliveira, S/N	Centro	Triunfo	LAP 1	-7,834386	-38,106282
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Sertânia	Av. Agamenon Magalhães, 222	Centro	Sertânia	LAP 1	-8,072632	-37,266229
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Posto Shopping Caruaru	Av. Adjair Da Silva Case, 800	Indianópolis	Caruaru	LAP 1	-8,283088	-35,970395
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Afrânio	Rua Coronel Clementino Coelho, 203	Centro	Afrânio	LAP 1	-8,515126	-41,005409
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Cupira	Av. Etelvino Lins, S/N	Centro	Cupira	LAP 1	-8,613182	-35,951205
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Bom Jardim	Av. Presidente Castelo Branco, 89	Centro	Bom Jardim	LAP 1	-7,790821	-35,59549
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Floresta	Av. PAULO GUERRA, 141	Centro	Floresta	LAP 1	-8,601542	-38,572406
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran Dormentes Posto Prefeitura	Rua José Coelho de Macedo Nº 281 - Dormentes		Dormentes	LAP 1	-8,450192	-40,767305
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - São Lourenço da Mata	Av. Doutor Francisco Correia, 1880	Centro	São Lourenço da Mata	LAP 1	-7,991042	-35,047829
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Goiana	Rua André Vidal De Negreiros, 57	Centro	Goiana	LAP 1	-7,559357	-35,007995
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Lajedo	Rodovia PE 170, S/N	Centro	Lajedo	LAP 1		
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Tuparetama	Av. Central, S/N	Centro	Tuparetama	LAP 1	-7,602372	-37,309432
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Taquaritinga do Norte	Av. Manoel Everaldo Tietre, S/N	Centro	Taquaritinga do Norte	LAP 1	-7,902235	-36,045248
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Posto Prefeitura - Tacaratú	Rua Sete De Setembro, S/N	Centro	Tacaratú	LAP 1	-9,103294	-38,148154

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Rio Formoso	Rua Pedro Albuquerque, S/N	Centro	Rio Formoso	LAP 1	-8,659768	-35,152655
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Correntes	Rua Coronel Francisco Santos - 126	Centro	Correntes	LAP 1	-9,1283	-36,328111
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Afogados da Ingazeira	Pe 320-Km 01, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,508829	-37,32465
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Aliança	Rua Domingos Braga, 192	Centro	Aliança	LAP 1	-7,601452	-35,230165
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Chã de Alegria	Rua Barbosa Lima, S/N	Centro	Chã de Alegria	LAP 1	-7,995955	-35,212431
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Palmares - Mig	Rua Ministro Marcos Freire, S/N	Centro	Palmares	LAP 1	-8,685579	-35,586021
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Ibimirim - Mig	Av. Castro Alves, 437	Centro	Ibimirim	LAP 1	-8,537149	-37,690155
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Salgueiro - Mig	Rua Manoel Santiago S/N	Augusto Sampaio	Salgueiro	LAP 1	-8,06911858	-39,13780923
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran Expresso Cidadão Boa Vista	Av. Conde da Boa Vista, S/N	Centro	Recife	LAP 1	-8,059614	-34,887046
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Posto Peixinhos	Rua Carmelita Soares Muniz de Araujo, 225	Casa Calada	Olinda	LAP 1	-7,993478	-34,840287
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Exú	Rodovia Br Asa Branca, S/N	Centro	Exu	LAP 1	-7,523539	-39,720598
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Ouricuri - Mig	Rua José Tomás De Aquino, 29	Centro	Ouricuri	LAP 1	-7,880932	-40,079331
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Itambé	Rua São Francisco, 210	Centro	Itambé	LAP 1	-7,407256	-35,11286
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Vicência	Av. Estefânia Carneiro da Cunha, 463	Centro	Vicência	LAP 1	-7,658802	-35,330288
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Nazaré	Rua Cel. Manoel Inácio, 44	Centro	Nazaré da Mata	LAP 1	-7,741286	-35,22556

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Condado	Av. 15 De Novembro, 346	Centro	Condado	LAP 1	-7,587521	-35,101979
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Expresso Cidadão - Petrolina	Av. Monsenhor Ângelo Sampaio - Shop River, 100	Centro	Petrolina	LAP 1	-9,39407	-40,492787
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - São José do Belmonte	Av. Euclides De Carvalho, 73	São José Belmonte	São José do Belmonte	LAP 1	-7,863161	-38,763508
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Ciretran - Aguas Belas	Av. CORONEL ALFREDO DUARTE, 278	São Sebastião	Águas Belas	LAP 1	-9,118132	-37,113223
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Carpina - Mig	Rua Santos Dumont, S/N	Senzala	Carpina	LAP 1	-7,849851	-35,251047
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Bezerros	Av. Major Aprigio da Fonseca, 35	São Sebastião	Bezerros	LAP 1	-8,238339	-35,742488
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Brejo Madre Deus - Mig	Av. Cleto Campelo, 299	Centro	Brejo da Madre de Deus	LAP 1	-8,147285	-36,370783
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Santa Cruz do Capibaribe	Av. Teofanes F. Torres, 20	Malaquias Cardoso	Santa Cruz do Capibaribe	LAP 1	-7,95567	-36,19688
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Santa Maria da Boa Vista - Mig	Rua Dr. Araujo Jorge, S/N	Centro	Santa Maria da Boa Vista	LAP 1	-8,808398	-39,823736
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Surubim	Rua K, S/N	Santo Antônio	Surubim	LAP 1	-7,845474	-35,74987
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Shopping Center Recife	Rua Padre Carapuceiro, 777	Boa Viagem	Recife	LAP 1	-8,118946	-34,904827
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Belém São Francisco	Rua Padre Norberto, 1261	Centro	Belém de São Francisco	LAP 1	-8,48749727	-39,3227586
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Orobó Posto Prefeitura	Rua Dom Sebastião Ieme - 94 - 94	Bela Vista	Orobó	LAP 1	-7,743502	-35,597597
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Petrolândia	Av. Dos Três Poderes, 46	Centro	Petrolândia	LAP 1	-8,979423	-38,218382
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Escada	Av. Visconde De Utinga, S/N	Centro	Escada	LAP 1	-8,364401	-35,231358

DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Moreno	Av. Dantas Barreto, 1795a	Centro	Moreno	LAP 1	-8,11864	-35,100161
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Olinda	Av. Presidente Kenedy 3333	Peixinhos	Olinda	LAP 1	-8,00651	-34,883336
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Bom Conselho	Rua Mário Melo - s/n	Centro	Bom Conselho	LAP 1	-9,1709444	-36,6889135
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Ribeirão	Praça Abelardo Sena, 231	Centro	Ribeirão	LAP 1	-8,513608	-35,374801
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - São Bento do Una	Praça Cônego João Rodrigues, 164	Centro	São Bento do Una	LAP 1	-8,520432	-36,445627
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran - Vitória Park Shopping	Av. HENRIQUE DE HOLANDA, 3000	Redenção	Vitória de Santo Antão	LAP 1	-8,114766	-35,273603
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran Posto Prefeitura Tabira	Rodovia Roberto Vianey Pires Liberal, 1100	Riacho do Gado	Tabira	LAP 1	-7,616466	-37,544858
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Detran Calçado Posto da Prefeitura	Travessa Vereador José Miguel, Centro, S/N	Centro	Calçado	LAP 1		
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Limoeiro	Rua Da Alegria, 638	Centro	Limoeiro	LAP 1	-9,38497	-40,547792
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Serra Talhada	Rua Custódia C. Lorena E Sá, 726	Centro	Serra Talhada	LAP 1	-7,98858	-38,278722
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Arcoverde	Av. Gumecindo Cavalcante, S/N	São Cristóvão	Arcoverde	LAP 1	-8,412382	-37,068985
DEPARTAMENTO ESTADUAL DE TRÂNSITO DE PERNAMBUCO	Ciretran - Timbaúba	Rua Coronel Claudino, S/N	Centro	Timbaúba	LAP 1		
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Estádio Governador Carlos Wilson Campos - Arena Pernambuco	Av. Deus é fiel, s/n	Penedo	São Lourenço da Mata	LAP 1	-7,99452	-35,042162
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Empetur - Memorial Arco Verde - Olinda	Av: Olinda S/N	Santa Tereza	Olinda	LAP 1	-8,04756	-34,876961
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Museu Cais do Sertão	AVENIDA ALFREDO LISBOA	Recife Antigo	Recife	LAP 2	-8,061457	-34,870694
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Empetur - Posto Terminal Rodoviário	Rodovia Br 408, S/N, Km 10,8	Curado Iv	Jaboatão dos Guararapes	LAP 1	-8,069927	-34,997862
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Empetur - Posto Informacao Turistica - Boa Viagem	R. Floriano Peixoto, S/N	São José	Recife	LAP 1	-8,132153	-34,900203

EMPRESA DE TURISMO DE PERNAMBUCO S/A	Empetur - Secretaria de Desenv. Econômico - Olinda	Av. Complexo Rodoviário Salgadinho S/N		Recife	LAP 2	-8,031075	-34,871358
EMPRESA DE TURISMO DE PERNAMBUCO S/A	Empetur - Posto Informacao Turistica - Aeroporto	Praça Menino Salgado Filho, S/N	Imbiribeira	Recife	LAP 1	-8,152423	-34,911708
EMPRESA PERNAMBUCANA DE TRANSPORTE COLETIVO INTERMUNICIPAL	EPTI - Sede	Av. Caxangá, 2200	Cordeiro	Recife	LAP 2	-8,05780827	-34,95215987
EMPRESA PERNAMBUCANA DE TRANSPORTE COLETIVO INTERMUNICIPAL	EPTI - Sede	Av. Caxangá, 2200	Cordeiro	Recife	LAP 2	-8,05780827	-34,95215987
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Custódia	Av. Inocencio Lima, 1072	Rodoviária	Custódia	LAP 1	-8,085969	-37,651192
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Petrolina	Av. Sete de Setembro, 223	Ouro Preto	Petrolina	LAP 1	-9,384407	-40,519175
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Caruaru Sede	Rua Dalton Santos - 319	São Francisco	Caruaru	LAP 2	-8,267312	-35,974514
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Morro do Peludo Olinda	Praca Do Mirante Ouro Preto, S/N	Ouro Preto	Olinda	LAP 1	-7,995028	-34,861413
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Recife	Av. Conde Da Boa Vista, 1424	Boa Vista	Recife	LAP 2	-8,056242	-34,893322
EMPRESA PERNAMBUCO DE COMUNICAÇÃO S/A	EPC - Salgueiro	Rua Joao Veras Siqueira, S/N	Nossa Senhora Aparecida	Salgueiro	LAP 1	-8,080986	-39,128909
ESCOLA POLITÉCNICA DE PERNAMBUCO	Poli - Escola Politécnica de Pernambuco	Rua Benfica, 455	Madalena	Recife	LAP 1	-8,060165	-34,903599
ESCOLA SUPERIOR DE EDUCAÇÃO FÍSICA	Escola Superior de Educação Física - ESEF	Rua Arnóbio Marques, 310	Santo Amaro	Recife	LAP 1	-8,047734	-34,887576
FACULDADE DE CIÊNCIAS DA ADMINISTRAÇÃO DE PERNAMBUCO	FCAP - Sede	Rua Pq Sport Clube Do Recife, 252	Madalena	Recife	LAP 1	-8,060947	-34,903341
FACULDADE DE CIÊNCIAS MÉDICAS	Faculdade de Ciências Médicas	Rua Arnóbio Marques, 310	Santo Amaro	Recife	LAP 1	-8,046407	-34,888042
FACULDADE DE ENFERMAGEM NOSSA SENHORA DAS GRAÇAS	Faculdade de Enfermagem Nossa Senhora Das Graças - FENSG	Rua Arnóbio Marques, 310	Santo Amaro	Recife	LAP 1	-8,047604	-34,887969
FACULDADE DE FORMAÇÃO DE PROFESSORES DE GARANHUNS	Facites - Faculdade de Ciências e Tecnologia de Salgueiro	Av. Coronel Veremundo Soares, S/N	Planalto	Salgueiro	LAP 1		
FACULDADE DE FORMAÇÃO DE PROFESSORES DE GARANHUNS	UPE - Facitec - Faculdade de Ciência e Tecnologia de Caruaru	Cru (Pe) Tv Jose Martins 1 Nossa Sra Das Dores	Nossa Sra. das Dores	Caruaru	LAP 1	-8,284493	-35,969886
FACULDADE DE FORMAÇÃO DE PROFESSORES DE GARANHUNS	UPE - Campus Arcoverde	Rua Cícero Monteiro de Melo, S/N	São José	Arcoverde	LAP 1	-8,88347408	-36,49630621

FACULDADE DE FORMAÇÃO DE PROFESSORES DE GARANHUNS	Faceteg - Faculdade de Ciências Educação e Tecnologia de Garanhuns	Rua Capitão Pedro Rodrigues, 105	Centro	Garanhuns	LAP 1	-8,883667	-36,496193
FACULDADE DE FORMAÇÃO DE PROFESSORES DE PETROLINA	UPE - Faculdade Formação Professores - Petrolina	Br-203 Km-2, S/N	Campus Universitário	Petrolina	LAP 1	-9,39946	-40,502356
FACULDADE DE ODONTOLOGIA DE PERNAMBUCO	Faculdade de Odontologia de Pernambuco	Avenida Norte 80	Santo Amaro	Recife	LAP 1		
FUNDAÇÃO DE AMPARO A CIÊNCIA E TECNOLOGIA DO ESTADO DE PERNAMBUCO	Fundação de Amparo à Ciência e a Tecnologia - FACEPE	Rua Benfica, 150	Madalena	Recife	LAP 1	-8,06039	-34,901272
FUNDAÇÃO DE APOSENTADORIAS E PENSÕES DOS SERVIDORES DO ESTADO DE PERNAMBUCO	FUNAPE SEDE	Avenida Conde da Boa Vista - 1450	Boa Vista	Recife	LAP 1		
FUNDAÇÃO DE APOSENTADORIAS E PENSÕES DOS SERVIDORES DO ESTADO DE PERNAMBUCO	FUNAPE SEDE	Avenida Conde da Boa Vista - 1450	Boa Vista	Recife	LAP 1	-8,056169	-34,89345
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE CABO DE SANTO AGOSTINHO	Estrada Pirapama, S/N	Centro	Cabo de Santo Agostinho	LAP 1	-8,296563	-35,068179
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE MURIBECA	Eixo da Integração PE 17 - Km 36	Muribeca	Jaboatão dos Guararapes	LAP 1	-8,138016	-34,980959
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM GARANHUNS	Rua LUIS BURGOS, 1507	Boa Vista	Garanhuns	LAP 1	-8,90843	-36,499399
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE CARUARU	Fazenda Alagoinha Estrada Carroçável, S/N	Sítio Lagoa dos Porcos	Caruaru	LAP 1	-8,283928	-35,969737
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM CARUARU	Rua Natalício Soares Do Santos, 47	Indianópolis	Caruaru	LAP 1	-8,29354	-35,959559
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM SANTA LUZIA	Rua Tomaz Gonzaga, 385 Torre -Recife/PE	Torre	Recife	LAP 1	-8,04883	-34,918818
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE JABOATAO DOS GUARARAPES	Rua Pititinga, S/N	Vista Alegre	Jaboatão dos Guararapes	LAP 1	-8,110056	-35,026858
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM PETROLINA	Av. DAS NAÇÕES, 190	Centro	Petrolina	LAP 1	-9,38957474	-40,50859265
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM HARMONIA	Rua Capitão Araújo de Miranda, 103, S/N	Iputinga	Recife	LAP 1	-8,044905	-34,932899
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - UNIAI RECIFE	R. João Fernandes Vieira, Nº 405	Boa Vista	Recife	LAP 1	-8,053445	-34,891932
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM AREIAS	RUA ANTONIO VIDAL, NÚMERO 55	AREIAS	Recife	LAP 1	-8,091081	-34,930023

FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - ALMOXARIFADO JABOATÃO	Estrada da Batalha 1495 - GALPÃO B	Prazeres	Jaboatão dos Guararapes	LAP 1	-8,14986706	-34,91860636
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	CASE PIRAPAMA	KM 02 Estrada de Pirapama	Pirapama	Cabo de Santo Agostinho	LAP 1	-8,296563	-35,068179
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - Parque Profissionalizante	RUA Coronel Alfredo Duarte	Afogados	Recife	LAP 1	-8,070585	-34,911107
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE TIMBAÚBA	Loteamento César Augusto, S/N	Centro	Timbaúba	LAP 1	-7,50244674	-35,31278815
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CENIP RECIFE	Av. Abdias de Carvalho, S/N	Torrões	Recife	LAP 1	-8,064273	-34,936772
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - SEDE ADMINISTRATIVA	AV. CONSELHEIRO ROSA E SILVA, 773	Aflitos	Recife	LAP 2	-8,044549	-34,897373
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE_CENIP ARCOVERDE	Av. Dom Pedro II, S/N	Santa Luzia	Arcoverde	LAP 1	-8,417727	-37,051819
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE PETROLINA	Rua Pedronio Souza, 514	Jardim Massangano	Petrolina	LAP 1	-9,39271689	-40,52175618
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CENIP CARUARU	SITIO LAGOA DOS PORCOS	COAB 2	Caruaru	LAP 1	-8,26552173	-36,1081613
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CENIP PETROLINA	Rua Do Curral Queimado, 290	Jardim Maravilha	Petrolina	LAP 1	-9,38729507	-40,5202407
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASEM IPUTINGA	Avenida Mário Álvares Pereira Lira, 1313	Iputinga	Recife	LAP 1	-8,04712	-34,934236
FUNDAÇÃO DE ATENDIMENTO SOCIOEDUCATIVO	FUNASE - CASE GARANHUNS	Rua Luis Burgo, 1507	Boa Vista	Garanhuns	LAP 1	-8,90843	-36,499399
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Arcoverde	Av. Joaquim Nabuco, S/N	Centro	Arcoverde	LAP 1	-8,41751	-37,056292
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Derby	Av. Joaquim Nabuco, Nº 171	Graças	Recife	LAP 2	-8,052726	-34,897955
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Petrolina	Rua Pacifico Da Luz, 739	Centro	Petrolina	LAP 1	-9,3947	-40,500661
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Derby - Link Wi-Fi	Rua Joaquim Nabuco, 171	Graças	Recife	LAP 1	-8,625788	-35,524933
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Derby - Link Backup	Av. Joaquim Nabuco, Nº 171	Graças	Recife	LAP 2	-8,052726	-34,897955

FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Garanhuns	Av. Gonçalves Maia, S/N	Heliópolis	Garanhuns	LAP 1	-8,885759	-36,48122
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Sede	Rua Rio Capibaribe, 147	São José	Recife	LAP 1	-8,06639437	-34,88404642
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Sede	Rua Rio Capibaribe, 147	São José	Recife	LAP 1	-8,06639437	-34,88404642
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Limoeiro	Av. Santa Terezinha, 174	José Fernandes Salsa	Limoeiro	LAP 1	-7,881448	-35,457721
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Serra Talhada	Rua Dep Afranio Ribeiro De Godoy, 1003	Nossa Sra. da Penha	Serra Talhada	LAP 1	-7,990495	-38,29718
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Ouricuri	Rua Ulisses Guimarães, S/N	Centro	Ouricuri	LAP 1	-7,881701	-40,085353
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Madalena	RUA GASPAR PERES, 273	IPUTINGA	Recife	LAP 1	-8,042216	-34,940599
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Caruaru	Rua Dr. Osvaldo Cruz, S/N	Maurício de Nassau	Caruaru	LAP 1	-8,28026	-35,970847
FUNDAÇÃO DE HEMATOLOGIA E HEMOTERAPIA DO ESTADO DE PERNAMBUCO	Hemope - Salgueiro	Rua Joaquim Gondim, 65	Santo Antônio	Salgueiro	LAP 1	-8,075043	-39,12097
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu do Estado de Pernambuco	Av. Rui Barbosa N: 960	Graças	Recife	LAP 1	-8,044929	-34,902086
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu de Arte Contemporânea	Rua Treze De Maio, 153	Varadouro	Olinda	LAP 1	-8,016229	-34,853448
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu de Arte Sacra	Rua Bispo Coutinho, 726	Carmo	Olinda	LAP 1	-8,013358	-34,850317

FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	CEDOC/Vice - Governadoria	Rua da Aurora - 469	Boa Vista	Recife	LAP 1		
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Theatro Cinema Guarany	Manoel Pereira Lima, CENTRO, Triunfo	Triunfo	Recife	LAP 2		
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	CASA DA CULTURA DE PERNAMBUCO (ECONOMIA CRIATIVA SALA JOARES)	Avenida Oliveira Lima, 813	Boa Vista	Recife	LAP 1	-8,057531	-34,887523
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Casa da Cultura de Pernambuco	Rua Floriano Peixoto, S/N		Recife	LAP 1	-8,067965	-34,883385
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Casa da Cultura de Pernambuco - Miste	Rua Floriano Peixoto, S/N	Centro	Recife	LAP 1	-8,04756	-34,876961
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Sede - Secretaria de Cultura	Rua Da Aurora, 469	Boa Vista	Recife	LAP 2	-8,05954116	-34,88042563
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Sede - Secretaria de Cultura	Rua Da Aurora, 469	Boa Vista	Recife	LAP 2	-8,05954116	-34,88042563
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Teatro Guarani - Triunfo	Praça Carolino Campos, S/N	Centro	Triunfo	LAP 2	-7,837021	-38,10384
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Espaço Cultural Casa de Câmara e Cadeia	Rua Maestro Tomás de A. Maciel, 60	Nossa Senhora do Bom Conselho	Brejo da Madre de Deus	LAP 1	-8,149136	-36,369393
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu Regional de Olinda	Rua Do Amparo, 128	Amparo	Olinda	LAP 1	-8,013401	-34,852927
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu da Imagem e Som (Atualmente Cinema São Luiz)	Rua Aurora, 175	Boa Vista	Recife	LAP 2	-8,062254	-34,881934
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu da Imagem e Som (Atualmente Cinema São Luiz)	Rua Aurora, 175	Boa Vista	Recife	LAP 2	-8,062254	-34,881934

FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Espaço Pasargada	Rua da União, Nº 263	Boa Vista	Recife	LAP 1	-8,04756	-34,876961
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Torre Malakoff	Praça Artur Oscar, S/N	Recife Antigo	Recife	LAP 1	-8,060827	-34,870809
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Sobre Loja do Edf. São Cristovão - Funcultura	Rua da Aurora, 295	Boa Vista	Recife	LAP 2	-8,060971	-34,88138
FUNDAÇÃO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO DE PERNAMBUCO	Fundarpe - Museu do Trem	Rua Floriano Peixoto , s/n	São José	Recife	LAP 1	-8,04756	-34,876961
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Nazaré da Mata	Rua Professor Amaro Maltez, 201	Sítio Novo	Nazaré da Mata	LAP 1	-7,747774	-35,223419
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Tabira	Rua Euclócio Luiz Monteiro, 50	Jureminha	Tabira	LAP 1	-7,590736	-37,539832
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Reitoria	Av Gov Agamenon Magalhaes S/N	Santo Amaro	Recife	LAP 1	-8,040761	-34,880629
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Floresta	Av. Dep Audomar Ferraz, 65	São José	Floresta	LAP 1	-8,600399	-38,572026
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Garanhuns	Rua Capitão Pedro Rodrigues, 105	Centro	Garanhuns	LAP 1	-8,88036	-36,501617
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Ouricuri	Estrada Vicinal Do Azude Tamburil, S/N		Ouricuri	LAP 1	-7,883333	-40,166667
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Petrolina	Rodovia Br 203 Km 02, S/N	Vila Eduardo	Petrolina	LAP 1	-9,392083	-40,502842
FUNDAÇÃO UNIVERSIDADE DE PERNAMBUCO	UPE - Vídeo Conferência - Surubim	Rua do Açude, 3000	Centro	Surubim	LAP 1	-7,83403654	-35,76312093
HOSPITAL UNIVERSITÁRIO OSWALDO CRUZ	UPE - Hospital Oswaldo Cruz	Rua Arnóbio Marques, 130	Santo Amaro	Recife	LAP 1	-8,046242	-34,888251
INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - Cumaru	Rua Elmenia Gonçalves Oliveira, S/N	Centro	Cumaru	LAP 1	-8,009271	-35,700791
INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - Alagoinha	Rua Tenente Dogival Dalindo, 13	Centro	Alagoinha	LAP 1	-8,46544386	-36,775036
INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - São Caetano	Rua Olimpio Oliveira Ramos, 110	Centro	São Caetano	LAP 1	-8,328463	-36,139882
INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - Nazare da Mata	Rua Don Ricardo Villela, 1056	Centro	Nazaré da Mata	LAP 1	-7,741878	-35,226143
INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - Santa Cruz do Capibaribe	Rua José Francisco Barbosa, 107	Centro	Santa Cruz do Capibaribe	LAP 1	-7,953157	-36,203722

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tabira	Praça Gonçalo Gomes, S/N	Centro	Tabira	LAP 1	-7,592507	-37,540358
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jatauba	Rua Manoel Batista Lima, 81	Centro	Jataúba	LAP 1	-7,989031	-36,496115
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritorio Municipal Ipojuca	Rua Vereador Antônio Bonifácio, 155	Centro	Ipojuca	LAP 1	-8,39787637	-35,6126741
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Salgadinho	Rua Antonio Gomes de Moura, 33	Centro	Salgadinho	LAP 1	-7,940931	-35,633407
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Chã de Alegria	Rua Manoel Bernardo da Silva, 444	Vila do Campo	Chã de Alegria	LAP 1	-7,997888	-35,213308
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jaqueira	Rua Dionísio Pereira da Costa, 157	Centro	Jaqueira	LAP 1	-8,731258	-35,79623
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tuparetama	Rua Siqueira Campos, 151	Centro	Tuparetama	LAP 1	-7,601347	-37,309454
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Limoeiro	Praça São Domingues, 174	Centro	Limoeiro	LAP 1	-7,87688894	-35,44474432
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Brejão	Rua José Inácio dos Santos - 17011	Centro	Brejão	LAP 1	-9,01571355	-36,53598206
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Palmeirina	Av. Desembargador Joao Paes de Carvalho, 220	Centro	Palmeirina	LAP 1	-9,003853	-36,326295
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritorio Municipal Mirandiba	Av. José da Silva Torres Aracua, 92	Centro	Mirandiba	LAP 1	-8,119633	-38,729291
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Palmares	Sítio Flor Dos Montes, S/N	Santa Rosa	Palmares	LAP 1	-8,67884	-35,583879
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Lajedo Gerencia Regional	Rua Pacheco de Medeiros, 60	Socorro	Lajedo	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Camocim de Sao Felix	Av. JOÃO BEZERRA, 298	Centro	Camocim de São Félix	LAP 1	-8,366528	-35,758751
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Verdejante	Rua Osmundo Bezerra, 330	Centro	Verdejante	LAP 1	-8,073411	-39,121987
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Estacao Experimental Sertania	Fazenda Cachoeira, 1	Zona Rural	Sertânia	LAP 1	-8,06285	-37,217994
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Sairé	Av. CORONEL JOSÉ PESSOA, 210	Centro	Sairé	LAP 1	-8,329465	-35,708251
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Catende	Rua 11 de Setembro, 138	Centro	Catende	LAP 1	-8,666931	-35,721091
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Xexeu	Rua da Alegria, 152	Centro	Xexéu	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Vicencia	Rua Manuel Borba, 81	Centro	Vicência	LAP 1		

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Pedra	Rua Gerônimo de Siqueira, 21	Centro	Pedra	LAP 1	-8,500185	-36,948094
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Lagoa do Ouro	Rua Do Progresso, 235	Centro	Lagoa do Ouro	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Calumbi	Rua Eliseu de Melo Neto, 10	Centro	Calumbi	LAP 1	-7,93878	-38,153422
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ouricuri	Av. Manoel Irineu de Araujo, 1165	Centro	Ouricuri	LAP 1	-7,875054	-40,095499
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Estação Experimental - Itapirema	Br 101 Norte Km 53, S/N		Goiana	LAP 1	-7,569556	-35,026251
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tacaimbó	Rua MAJOR JOAO GOMES, 92	Rua Velha	Tacaimbó	LAP 1	-8,320177	-36,290532
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Dormentes	Av. Maria Reis, 79	Centro	Dormentes	LAP 1	-8,445703	-40,766388
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Parnamirim	Rua Coronel Jambo, 27	Centro	Parnamirim	LAP 1	-8,088857	-39,577608
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Vertentes do Lério	Praça Nossa Senhora das Victorias, 31	Centro	Vertente do Lério	LAP 1	-7,774199	-35,850534
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Maria da Boa Vista	Rua 7 de Setembro, S/N	Centro	Santa Maria da Boa Vista	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA Riacho Das Almas	Rua ANTONIO LIMEIRA, 159	Centro	Riacho das Almas	LAP 1	-8,135818	-35,854574
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritório de Extensão - Itambé	Rua Pedro Araújo, 121	Centro	Itambé	LAP 1	-7,404697	-35,118006
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Correntes	Rua Floriano Peixoto, S/N	Centro	Correntes	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Macaparana	Rua Brasílio Ribeiro de Souza, 135	Centro	Macaparana	LAP 1	-7,551048	-35,447783
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - SURUBIM	Rua JOSE MALAQUIAS GUERRA, 138	Cabaceiras	Surubim	LAP 1	-7,844796	-35,757095
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Cruz	Av. 3 de Maio, 140	Centro	Santa Cruz	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Angelim	Rua Nossa Senhora de Nazaré, 115	Centro	Angelim	LAP 1	-8,888758	-36,282553
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerência Regional - Garanhuns	Av. Caruaru, 228	Heliópolis	Garanhuns	LAP 1	-8,884519	-36,488849
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jurema	Av. Joao Cordeiro de Souza, 45	Centro	Jurema	LAP 1	-8,719215	-36,136464
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gravatá	Rua Cleto Campelo, 109	Centro	Gravatá	LAP 1	-8,20428	-35,569176

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gameleira	Assentamento Paussangue, 01	Centro	Gameleira	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tupanatinga	Rua 31 de Março, 25	Centro	Tupanatinga	LAP 1	-8,753298	-37,340674
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Carnaíba	Rua Maestro Israel Gomes, S/N	Centro	Carnaíba	LAP 1	-7,805134	-37,794174
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Malhada de Pedra	Sítio Malhada de Pedra, S/N	Distrito Caruaru	Caruaru	LAP 1	-8,248141	-35,915941
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Panelas	Av. Petrolino Santa Cruz, 42	Centro	Panelas	LAP 1	-8,663822	-36,008338
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Iati	Av. Sete de Setembro, S/N	Centro	Iati	LAP 1	-9,043916	-36,846697
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Glória de Goita	Rua Lídia Câmara, 52	Centro	Glória do Goitá	LAP 1	-7,999296	-35,28891
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Estação Experimental São Bento Una	Estação Experimental de São Bento, S/N	Centro	São Bento do Una	LAP 1	-8,52682592	-36,45902923
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Venturosa	Rua Laurentino de Souza - 5	Centro	Venturosa	LAP 1	-8,574155	-36,880371
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Bonito	Rua Mizael Galindo, 42	Centro	Bonito	LAP 1	-8,04756	-34,876961
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Paudalho	Av. Padre Emídio, S/N	Centro	Paudalho	LAP 1	-7,899227	-35,175883
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ferreiros	Rua Julio Veloso, S/N	Centro	Ferreiros	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Rio Formoso	Rodovia Pe 60 - Km 57, 215	Centro	Rio Formoso	LAP 1	-8,665553	-35,158023
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Itamaraca	Travessa Padre Tenório - Nº 64	Pillar	Ilha de Itamaracá	LAP 1	-7,742834	-34,824352
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Goiana	Av. Nunes Machado, 460	Centro	Goiana	LAP 1	-7,558522	-34,996276
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Bodocó	Av. São Francisco, S/N	Centro	Bodocó	LAP 1	-7,781748	-39,941613
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Sertânia	Rua Manoel Borba, S/N	Centro	Sertânia	LAP 1	-8,069811	-37,260559
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Itacuruba	Rua Cicero Delgado dos Santos, 9	Centro	Itacuruba	LAP 1	-8,728159	-38,685034
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Pombos	Rua Alto Do Frade, 29	Loteamento Rancho Novo	Pombos	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Orocó	Av. Agamenom Magalhães, 538	Centro	Orocó	LAP 1	-8,619218	-39,60105

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Cruz da Baixa Verde	Rua Santa Luiza, 854	Centro	Santa Cruz da Baixa Verde	LAP 1	-7,82007171	-38,15315558
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Vitória Santo Antão	Rua Doutor Democrito Cavalcante, 1200	Livramento	Vitória de Santo Antão	LAP 1	-8,129244	-35,304846
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerencia Regional - Arcoverde	Rua Padre Roma, 343	Zonarural	Arcoverde	LAP 1	-8,420558	-37,048105
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Águas Belas	Av. CORONEL CONSTANTINO, 75	Centro	Águas Belas	LAP 1	-9,109422	-37,127274
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Buíque	Av. Dona Amelia Cavalcanti, 121	Centro	Buíque	LAP 1	-8,620974	-37,157217
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jupi	Rua Gersina Pereira da Silva, 221	Centro	Jupi	LAP 1	-8,71008	-36,415004
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Trindade	Rua 29 de janeiro, 233	Centro	Trindade	LAP 1	-7,762944	-40,265168
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Buenos Aires	Rua Projetada, 08	Centro	Buenos Aires	LAP 1	-7,723204	-35,326667
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Igarassu	Rua João Alves Beringer, 40		Igarassu	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Iguaracy	Rua João Alves Dos Passos, 38	Centro	Iguaracy	LAP 1	-7,83418	-37,515054
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São José do Egito	Rua João Pessoa, 69	Centro	São José do Egito	LAP 1	-7,478658	-37,274788
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Belo Jardim	Rua Cleto Campelo, 86	Centro	Belo Jardim	LAP 1	-8,336899	-36,42514
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Cabrobó	Praça Prefeito João Freire De Carvalho, 76	Centro	Cabrobó	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritório Local Triunfo	Av. Jose Veríssimo dos Santos, 365	Centro	Triunfo	LAP 1	-7,835886	-38,10635
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Condado	Rua Severino Gomes, 72	Centro	Condado	LAP 1	-7,590888	-35,098518
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Cupira	Rua Padre Felix, 71	Centro	Cupira	LAP 1	-8,611549	-35,950651
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Granito	Rua Sossego, S/N	Centro	Granito	LAP 1	-7,715557	-39,616488
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Bezerros	Rua Matriz, 133	Rosário	Bezerros	LAP 1	-8,23573	-35,753743
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Sanharó	Rua Major Satiro, 172	Centro	Sanharó	LAP 1	-8,36377	-36,56181
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Orobó	Rua Sizenando Maximiano de Aguiar, 44	Centro	Orobó	LAP 1	-7,747845	-35,604546

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ingazeira	Rua Albino Feitosa, S/N	Centro	Ingazeira	LAP 1	-7,67638906	-37,45917269
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Saloá	Av. Bezerra de Lima, SN	Centro	Salóá	LAP 1	-8,97032905	-36,69199955
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São Bento do Una	Entrada para Capoeira km 03, S/N		São Bento do Una	LAP 1	-8,524945	-36,449325
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Brejinho	Rua Joao Venancio de Souza, 57	Centro	Brejinho	LAP 1	-7,348053	-37,285919
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Lagoa do Carro	Rua Antônio Francisco Silva, 403	Centro	Lagoa do Carro	LAP 1	-7,842772	-35,310673
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Filomena	Rua Virgílio de Coelho, S/N	Centro	Santa Filomena	LAP 1	-8,161	-40,61377
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Bom Conselho	Rua 15 de Novembro, 172	Centro	Bom Conselho	LAP 1	-9,166786	-36,67978
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Terra Nova	Rua Antonio Freire de As, 45	Centro	Terra Nova	LAP 1	-8,229343	-39,377043
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritório Municipal Lajedo	Rua. Nossa Senhora Perpétuo Socorro, 96	Centro	Lajedo	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São João	Rua Jucelino C de Araújo, 99	Parque Alvorada	São João	LAP 1	-7,677203	-37,459109
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Aliança	Rua Domingos Braga, 196	Centro	Aliança	LAP 1	-7,601369	-35,230148
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Capoeiras	Praça JOÃO DO REGO, 12	Centro	Capoeiras	LAP 1	-8,737928	-36,626073
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Sede	Av. Gen San Martin, 1371	San Martin	Recife	LAP 1	-8,063117	-34,926454
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Quixaba	Rua Padre Marciel, 363	Centro	Quixabá	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ipubi	Av. Getulio Vargas, 316	Centro	Ipubi	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tacaratu	Av. Conego Frederico, S/N	Centro	Tacaratu	LAP 1	-9,106253	-38,150251
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Terezinha	Rua Bernardo Nunes, 162	Centro	Santa Terezinha	LAP 1	-7,377024	-37,48038
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Itapetim	Rua Padre José Guereí, S/N	Centro	Itapetim	LAP 1	-7,379282	-37,18464
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Poção	Av. Conrado de Andrade, 169	Centro	Poção	LAP 1	-8,18754	-36,702568

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Bom Jardim	Rua Israel Fonseca, 128	Centro	Bom Jardim	LAP 1	-7,796375	-35,590657
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São Benedito do Sul	Rua Antônio Lúcio Severino - 5	Centro	São Benedito do Sul	LAP 1	-8,807359	-35,933492
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Manari	Rua Antonio Jorge, 75	Centro	Manari	LAP 1	-8,963389	-37,625364
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jucati	Rua Pertulino Alves, 8	Centro	Jucati	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Passira	Rua Severino Fontes, 7	Centro	Passira	LAP 1	-7,980367	-35,580421
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Inaja	Rua Padre Agostinho, 57	Centro	Inajá	LAP 1	-8,900975	-37,824551
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Cabo	R. Severino Bezerra Marques, S/N	Centro	Cabo de Santo Agostinho	LAP 1	-8,28423	-35,034668
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Carpina - Centro de Treinamento	Av. Padre Rocha, 1369	São José	Carpina	LAP 1	-7,835952	-35,254064
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Feira Nova	Rua Julio Ferreira Chaves, S/N	Centro	Feira Nova	LAP 1	-7,951032	-35,388121
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerencia Regional - Araripina	Rua Manoel Ferreira Sampaio, 300	Centro	Araripina	LAP 1	-7,577104	-40,506138
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritorio Municipal de Agrestina	Rua 04 De Outubro, 8	Centro	Agrestina	LAP 1	-8,45766067	-35,94788953
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritório Afogados da Ingazeira	Av. Manoel Borba, 08	Centro	Afogados da Ingazeira	LAP 1	-7,746117	-37,639802
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ibirajuba	Rua Josefa Alves de Couto, 06	Centro	Ibirajuba	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Vitória Santo Antao	Av. Henrique de Holanda, S/N	Centro	Vitória de Santo Antão	LAP 1	-8,11307	-35,286972
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Betania	Rua Alfredo José Dos Santos, 95	Centro	Betânia	LAP 1		

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Belém de São Francisco	Av. Coronel Caribé, 987	Centro	Belém de São Francisco	LAP 1	-8,750549	-38,959119
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Moreilandia	Av. Coronel Romão Sampaio, S/N	Centro	Moreilandia	LAP 1	-7,620659	-39,555064
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Carnaubeira Penha	Rua José Manculino Pereira, 295	Centro	Carnaubeira da Penha	LAP 1	-8,31861145	-38,74269307
INSTITUTO AGRONÔMICO DE PERNAMBUCO	Estação Experimental de Arcoverde-Ipa	Br-232, S/N	Santa Luzia	Arcoverde	LAP 1	-8,419608	-37,047041
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ribeirão	Rua Dr. Luiz Gusmão, S/N	Centro	Ribeirão	LAP 1	-8,515208	-35,376242
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Toritama	Rua Galdino Afonso, 53	Centro	Toritama	LAP 1	-8,008003	-36,053529
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Camutanga	Av. Dr. Simplicio Tavares, 56	Centro	Camutanga	LAP 1	-7,40721	-35,274672
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Frei Miguelinho	Rua- Manoel Pereira de Souza Filho, S/N	Centro	Frei Miguelinho	LAP 1	-7,93939734	-35,91120479
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Terezinha	Rua Abílio Alvez de Miranda, 40	Centro	Terezinha	LAP 1	-9,057144	-36,624796
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Santa Maria do Cambuca	Travessa Agripino de Almeida, 210	Centro	Santa Maria do Cambucá	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escritório Municipal - Floresta	Rua Major José Rodrigues De Moraes, 196.	Centro	Floresta	LAP 1	-8,602346	-38,575124
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Altinho	Rua Coronel João Guilherme, 135	Centro	Altinho	LAP 1	-8,487702	-36,059594
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ibimirim - 1	Av. Alexandre Emerêncio, 40	Centro	Ibimirim	LAP 1	-8,5228203	-37,68790757
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Casinhas	Rua Maria Cecília L Miranda, S/N	Centro	Casinhas	LAP 1	-7,836992	-34,90383
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Timbaúba	Rua Tenente João Gomes, 119	Centro	Timbaúba	LAP 1	-7,513693	-35,318072
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São Lourenço da Mata	Rua Doutor Pedro Correia de Araújo, S/N	Centro	São Lourenço da Mata	LAP 1	-7,996477	-35,040193
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São Vicente Férrer	Rua Joao Araujo, 40	Centro	São Vicente Férrer	LAP 1	-7,590386	-35,489583
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Petrolândia	Av. 3 Poderes, 59	Centro	Petrolândia	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Est Experimental Brejão	Sítio Vista Alegre, S/N	Zona Rural	Brejão	LAP 1	-9,009118	-36,563155
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Serra Talhada - Estação Experimental	Estação Experimental de Serra Talhada, S/N	Zona rural	Serra Talhada	LAP 1	-7,982044	-38,289749

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jaboatão Dos Guararapes	Rua Barão de Moreno	Vila Rica	Jaboatão dos Guararapes	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Vertentes	Rua Ivan Figueiroa, 209	Centro	Vertentes	LAP 1	-7,9058	-35,983601
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Itaíba	Rua Nova - 5	Centro	Itaíba	LAP 1	-8,946954	-37,421707
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Machados	Rua José Bernardo de Oliveira, 228	Centro	Machados	LAP 1	-7,68283	-35,514195
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Serrita	Rua Dr. Avelar, 88	Centro	Serrita	LAP 1	-7,948306	-39,296859
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Jatoba	Av. Olinda, S/N	Centro	Jatobá	LAP 1	-9,181693	-38,265628
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Estação Experimental - Itambé	Rodovia Pe-75, S/N	Centro	Itambé	LAP 1	-7,396427	-35,182217
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Moreno	Av. Conde da Boa Vista, 84	Moreno Centro	Moreno	LAP 1	-8,117771	-35,101907
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - São José do Belmonte	Rua José Alves de Carvalho, 28	Centro	São José do Belmonte	LAP 1	-7,863191	-38,756538
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Lagoa Grande	Rua Estudante, S/N	Centro	Lagoa Grande	LAP 1	-8,994943	-40,277095
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Amaraji	Rua Praça da Bandeira, 96	Centro	Amaraji	LAP 1	-8,376467	-35,452315
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Centro de Produção e Comercialização de Petrolina	Av. Luiz de Sousa, S/N	Distrito Industrial	Petrolina	LAP 1	-9,39792	-40,535131
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Escada	Rua Joao Manoel Pontual, 38	Centro	Escada	LAP 1	-8,364014	-35,233157
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Brejo da Madre de Deus	Rua Joaquim Nabuco, 3	Centro	Brejo da Madre de Deus	LAP 1	-8,149488	-36,370286
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Ibimirim - 2	Rua Alexandre Emereciano, 40	Centro	Ibimirim	LAP 1	-8,53436363	37,69522168
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerência Regional de Salgueiro	Av. Getúlio Vargas, 220	Nossa Sra. Aparecida	Salgueiro	LAP 1	-8,073615	-39,129631
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerencia Regional Caruaru	Av. Dom Bosco, 20	Heliópolis	Caruaru	LAP 1	-8,279602	-35,96871
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Exu	Rua Coronel Manuel Aires, 444	Centro	Exu	LAP 1	-7,512755	-39,718874
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Taquaritinga do Norte	Rua Dr. José Rebello de Castro, 114	Centro	Taquaritinga do Norte	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Solidão	Rua Luiz Carolino Siqueira, S/N	Centro	Solidão	LAP 1		

INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Cha Grande	Rua JOAO PRUDENTE SANTANA, S/N	Centro	Chã Grande	LAP 1		
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Paratama	Rua São Luis, 58	Centro	Paratama	LAP 1	-8,921146	-36,656945
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Cedro	Rua Jose Inacio Leite, 154	Centro	Cedro	LAP 1	-7,99207028	-38,29404125
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Lagoa de Itaenga	Rua José Izidoro, 22	Centro	Lagoa do Itaenga	LAP 1	-7,931705	-35,29331
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerência Regional Petrolina	Av. Das Nações, S/N	Centro	Petrolina	LAP 1	-9,390835	-40,508391
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Tamandaré	Loteamento Cohab 2, 24	Centro	Tamandaré	LAP 1	-8,757866	-35,105071
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Estacao Experimental Pesqueira	Avenida Évio Araújo, 436	Centro	Pesqueira	LAP 1	-8,354483	-36,689991
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Custodia	Praça Padre Leão, 67	Centro	Custódia	LAP 1	-8,088481	-37,642588
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Sao Joaquim do Monte	Av. Presidente Kennedy, 25	Centro	São Joaquim do Monte	LAP 1	-8,432293	-35,807317
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Afranio	Praça Sebastião Coelho, 40	Centro	Afrânio	LAP 1	-8,516311	-41,003915
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Joao Alfredo	Av. BR RIO BRANCO, S/N	Centro	João Alfredo	LAP 1	-7,861941	-35,588041
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Barra de Guabiraba	Rua Francisco Batista da Silva, 80	Centro	Barra de Guabiraba	LAP 1	-8,421008	-35,664515
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Carpina	Rua Vidal de Negreiros, S/N	Centro	Carpina	LAP 1	-7,835952	-35,254064
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Gerência Afogados da Ingazeira	Rua Padre Luis de Goes, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,75731679	-37,633207
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Serra Talhada	Av. Afonso Magalhaes, S/N	Centro	Serra Talhada	LAP 1	-7,985395	-38,290433
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Agua Preta	Travessa Siqueira Campos, 3117	Centro	Água Preta	LAP 1	-8,7056845	-35,52084007
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Abreu e Lima	Rua Joaquim Nabuco, N 183 - Timbó	Abreu e Lima	Recife	LAP 1	-7,910303	-34,903958
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Primavera	Rua Nova Aurora, 40	João Murilo	Primavera	LAP 1	-8,33738377	-35,35240287
INSTITUTO AGRONÔMICO DE PERNAMBUCO	Estação Experimental de Belem de São Francisco	Ilha Do Estreito (Ipa), S/N	Centro	Belém de São Francisco	LAP 1	-8,567682	-39,246437
INSTITUTO AGRONÔMICO DE PERNAMBUCO	IPA - Caetés	Av. Luis Pereira Junior, 11	Centro	Caetés	LAP 1	-8,772449	-36,621694

INSTITUTO AGRÔNOMICO DE PERNAMBUCO	IPA - Cachoeirinha	Av. 31 de março, 339	Centro	Cachoeirinha	LAP 1	-8,488982	-36,238112
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Ambulatório - Centro de Saúde Bucal	Rua Conde do Irajá, 176	Torre	Recife	LAP 1	-8,045562	-34,905366
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agencia de Goiana	Rua Nova, 160	Centro	Goiana	LAP 1	-7,561213	-35,012229
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Palmares	Rua Bispo Pereira Alves, 800	Centro	Palmares	LAP 1	-8,682627	-35,587113
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Caruaru - 4ª Região	Rua Joao Colin, 275	Indianópolis	Caruaru	LAP 1	-8,291134	-35,949396
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Serra Talhada	Rua Tiburtino Nogueira, S/N	Centro	Serra Talhada	LAP 1	-7,98986229	-38,29543911
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Afogados da Ingazeira	Rua Padre Luiz Campos Góes, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,753	-37,632795
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Surubim	Rua Antônio Medeiros Sobrinho, 4	Centro	Surubim	LAP 1	-7,841468	-35,755702
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agência Salgueiro - 7ª Região	Av. Joaquim Sampaio, 313	Centro	Salgueiro	LAP 1	-8,070019	-39,123335
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Posto de Saúde Mental	Rua Da Harmonia, 626	Casa Amarela	Recife	LAP 1	-8,029072	-34,914759

INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Hospital Dos Servidores do Estado	Av. Cons. Rosa E Silva, S/N	Graças	Recife	LAP 2		
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Hospital Dos Servidores do Estado	Av. Cons. Rosa E Silva, S/N	Graças	Recife	LAP 2	-8,040665	-34,898627
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agência Petrolina - 8ª Região	Av. Fernando Góes - S/N	Centro	Petrolina	LAP 1	-9,397707	-40,49959
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agencia Carpina	Rua Santos Dumont, S/N	Centro	Carpina	LAP 1	-7,849612	-35,251029
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agencia de Arcoverde	Av. Joaquim Nabuco, 251	Centro	Arcoverde	LAP 1	-8,417514	-37,056363
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agência de Garanhuns	Av. Caruaru, S/N	Heliópolis	Garanhuns	LAP 1	-8,881068	-36,486382
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Sede ( Ipsep )	Rua Henrique Dias, S/N	Derby	Recife	LAP 2	-8,05877337	34,89927537
INSTITUTO DE ATENÇÃO À SAÚDE E BEM-ESTAR DOS SERVIDORES DO ESTADO DE PERNAMBUCO	IRH - Agencia Ouricuri	Av. Fernando Bezerra, S/N	Centro	Ouricuri	LAP 1	-7,888213	-40,086934
INSTITUTO DE CIÊNCIAS BIOLÓGICAS	Instituto de Ciências Biológicas - Sede	Rua Arnóbio Marques, 310	Santo Amaro	Recife	LAP 1	-8,047604	-34,887969
INSTITUTO DE PESOS E MEDIDAS DO ESTADO DE PERNAMBUCO	Instituto de Pesos e Medidas do Estado de Pernambuco - Porto de Suape	Pe 60 - Avenida Portuária S/N		Ipojuca	LAP 1	-8,404129	-34,967271
INSTITUTO DE PESOS E MEDIDAS DO ESTADO DE PERNAMBUCO	IPEM - Sede Recife - Cidade Universitária	Av. Luiz Freire, 100	Cidade Universitária	Recife	LAP 1	-8,05917	-34,94692
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Sede	Av. General San Martin - 1701	Bongi	Recife	LAP 1	-8,066802	-34,927402

INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Serra Talhada	Av. Afonso Magalhães, S/N	Nossa Senhora da Conceição	Serra Talhada	LAP 1	-7,985395	-38,290433
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Caruaru	Rua Dom Bosco, 20	Maurício de Nassau	Caruaru	LAP 1	-8,279666	-35,96854
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Afogados da Ingazeira	Travessa Pe. Luis de Campos Goes, S/N	Morada Nova	Afogados da Ingazeira	LAP 1	-7,756972	-37,631227
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Ouricuri	Av. Presidente Kenedy, 121	Centro	Ouricuri	LAP 1	-7,88691	-40,08445
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Garanhuns	Av. Caruaru, 228	Centro	Garanhuns	LAP 1	-8,093963	-34,936141
INSTITUTO DE TERRAS E REFORMA AGRÁRIA DO ESTADO DE PERNAMBUCO	Iterpe - Petrolina	Av. Nações, S/N	Centro	Petrolina	LAP 1	-9,39946	-40,502356
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Arcoverde	Av. Coronel Antonio Japiassu, 227	Centro	Arcoverde	LAP 1	-8,420175	-37,050474
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Araripina	Rua Antônio Alexandre Alves, 358	Centro	Araripina	LAP 1	-7,57694572	-40,49683183
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Goiana	Rua MARECHAL DEODORO DA FONSECA, 220	Centro	Goiana	LAP 1	-7,557855	-34,99901
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Sede	Rua Imperial, Nº 1600	São José	Recife	LAP 2	-8,075319	-34,892444
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Palmares	Rua Latécio Montenegro, 70	Centro	Palmares	LAP 1	-8,684567	-35,590402
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Petrolina	Av. Manoel Dos Arroz, S/N	Vila Moco	Petrolina	LAP 1	-9,38385826	-40,50531886
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Santa Cruz do Capibaribe	Rua Julio Aragão, 249	Bairro Novo	Santa Cruz do Capibaribe	LAP 1	-7,956182	-36,206573
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Garanhuns	Av. LIONS CLUB, 305	Aluísio Pinto	Garanhuns	LAP 1	-8,89592	-36,500076
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Salgueiro	Av. Antônio Angelim, 570	Santo Antônio	Salgueiro	LAP 1	-8,072433	-39,124081
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Serra Talhada	Rua Ignacio de Oliveira, 1312	Nossa Sra. da Penha	Serra Talhada	LAP 1	-7,992046	-38,294979
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Petrolândia	Praça DOS TRES PODERES, S/N	Centro	Petrolândia	LAP 1	-8,9815809	-38,21869913
JUNTA COMERCIAL DO ESTADO DE PERNAMBUCO	Jucepe - Caruaru	Rua Armando da Fonte, 15	Maurício de Nassau	Caruaru	LAP 1	-8,28193057	-35,97232732

LABORATÓRIO FARMACÉUTICO DE PERNAMBUCO	LAFEPE - Sede	Largo De Dois Irmãos, 1117	Dois Irmãos	Recife	LAP 1	-8,016058	-34,943387
PERNAMBUCO PARTICIPAÇÕES E INVESTIMENTOS S/A	Perpart - Sede	Rua Doutor João Lacerda, 395	Cordeiro	Recife	LAP 2	-8,04609267	-34,9225417
PERNAMBUCO PARTICIPAÇÕES E INVESTIMENTOS S/A	Perpart - Sede	Rua Doutor João Lacerda, 395	Cordeiro	Recife	LAP 2	-8,046097	-34,922225
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-IMLAPC-CARUARU.LINK-PRINCIPAL	BR 232, KM 130	Indianópolis	Caruaru	LAP 1	-8,305789	-35,964914
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-ICPAS-SALGUEIRO.LINK-PRINCIPAL	Rua Joaquim Sampaio, 321	Centro	Salgueiro	LAP 1	-8,070142	-39,123237
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-ICPAS-PETROLINA.LINK-PRINCIPAL	Av. Cardoso de Sá, S/N	Vila Eduardo	Petrolina	LAP 1	-9,384205	-40,483849
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-NAZARE-MATA.LINK-PRINCIPAL	Rua Leão Coroado	Estação	Nazaré da Mata	LAP 1	-7,75034987	-35,22863186
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-IMLAPC-SEDE.LINK-PRINCIPAL	Av. Marques De Pombal, 455	Centro	Recife	LAP 1	-8,057838	-34,882897
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-AFOGADOS-INGAZEIRA.LINK-PRINCIPAL	Rua Valdevino José Praxedes	Manoela Valadares	Afogados da Ingazeira	LAP 1	-7,754463	-37,630012
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-OURICURI.LINK-PRINCIPAL	Rua Luiz Gonzaga do Nascimento 260	Renascença	Ouricuri	LAP 1	-7,881717	-40,093417
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-IMLAPC-JABOATÃO.LINK-PRINCIPAL	Estrada da Batalha, S/N	Prazeres	Jaboatão dos Guararapes	LAP 1	-8,153934	-34,920667
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-ICPAS-SEDE.LINK-PRINCIPAL	Odorico Mendes, 700	Campo Grande	Recife	LAP 1	-8,038525	-34,879777
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-PALMARES.LINK-PRINCIPAL	Rua Planejada	São Sebastião	Palmares	LAP 1	-8,67884	-35,583879
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-IGFEC-LINK-PRINCIPAL	Rua São Geraldo	Santo Amaro	Recife	LAP 1	-8,05271263	-34,88046499
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-GARANHUNS.LINK-PRINCIPAL	Av. Ministro Marcos Freire, 490	Heliópolis	Garanhuns	LAP 1	-8,890573	-36,482673
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-ICPAS-CARUARU.LINK-PRINCIPAL	Av. Caruaru, S/N	Boa Vista	Caruaru	LAP 1	-8,274225	-35,99378
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-URPOC-ARCOVERDE.LINK-PRINCIPAL	Rua Sebastião de Souza Ferraz	Sucupira	Arcoverde	LAP 1	-8,426284	-37,057039
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-ICPAS-SEDE.ADE	Odorico Mendes	Campo Grande	Recife	LAP 1	-8,038525	-34,879777
POLÍCIA CIENTÍFICA DA SDS	SDS.POLICIA-CIENTIFICA-IMLAPC-PETROLINA.LINK-PRINCIPAL	Av. 7 De Setembro, S/N	Jardim Maravilha	Petrolina	LAP 1	-9,383192	-40,516283
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.188 Circunscrição Belem de Sao Francisco	Av. Coronel Geronimo Pires, 820	Centro	Belém de São Francisco	LAP 1	-8,75374	-38,968117
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.94 Circunscrição - Cupira	Av. Presidente Vargas, S/N	Centro	Cupira	LAP 1	-8,607183	-35,947583
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.180 Circunscrição - Carnaíba	Rua Saturnino Bezerra, 654	Centro	Carnaíba	LAP 1	-7,801105	-37,792354
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.16 Circunscrição - Água Fria	Rua Julio Ramos, 171	Água Fria	Recife	LAP 2	-8,020788	-34,893343
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.95 Circunscrição - Altinho	Rua Siqueira Campos, 41	Centro	Altinho	LAP 1	-8,490066	-36,059946
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.24 Circunscrição- Delegacia - Varadouro - Olinda	Av. Olinda, 160	Varadouro	Olinda	LAP 2	-8,02034	-34,856133
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.64 Circunscrição - Glória do Goita	Rua Siqueira Campos, 40	Centro	Glória do Goitá	LAP 1	-7,999509	-35,288906
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.18 Circunscrição - Macaxeira	Vereador Otacilio De Azevedo, 2880	Brejo da guabiraba	Recife	LAP 2	-7,989104	-34,930812
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.03 Seccional - Boa Viagem + PCPE.07 Circunscrição - Boa Viagem	v. Domingos Ferreira, 4420	Boa Viagem	Recife	LAP 2	-8,127421	-34,901445

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.192 Circunscrição - Itacuruba	Rua Olegário Rezende, S/N	Centro	Itacuruba	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Proteção Ao Consumidor	Rua Gervásio Pires, 863	Boa Vista	Recife	LAP 2	-8,055208	-34,883989
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.114 Circunscrição - Póca	Av. Manoel Vieira De Melo, 223	Centro	Póca	LAP 1	-8,184646	-36,705564
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DHPP.Delegacia de Homicídios e Proteção à Pessoa	RUA DR. JOÃO LACERDA, 395	CORDEIRO	Recife	LAP 2	-8,046097	-34,922225
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.32 Circunscrição - Engenho Maranguape - Janga	Av. Cláudio Gueiros Leite, SN	Janga	Paulista	LAP 2	-7,9061	-34,825917
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.31 Circunscrição - Itapissuma	Av. Frei Serafim, 114	Centro	Itapissuma	LAP 2	-7,77343	-34,897136
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.18 Seccional- Garanhuns	Rua Joaquim Nabuco, 189	Centro	Garanhuns	LAP 2	-8,888482	-36,496404
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.148 Circunscrição - Calçado	Travessa VEREADOR JOAO MIGUEL, 18	Centro	Calçado	LAP 1	-8,741339	-36,337385
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.112 Circunscrição - Tacaimbó	Rua Major João Gomes, 164	Centro	Tacaimbó	LAP 1	-8,320754	-36,290098
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.AIS.04 Seccional - Varzea + PCPE.14 Circunscrição - Varzea	Rua Dona Maria Lacerda, S/N	Varzea	Recife	LAP 2	-8,048016	-34,960784
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.AIS - Prazeres. Delegacia de Polícia Crimes Contra a Mulher	Estrada Da Batalha, Sn, Prazeres	Jaboatão	Jaboatão dos Guararapes	LAP 2	-8,147202	-34,919175
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.173 Circunscrição - Tuparetama	Rua Monsenhor Sebastião Rabelo, 65	Centro	Tuparetama	LAP 1	-7,600904	-37,309715
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.81 Circunscrição - Maraial	Av. Savador Texeira, Nº238	Centro	Maraial	LAP 1	-8,783205	-35,811684
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Complexo policial de Olinda	Rua José Dias Raposo, S/N	Ouro Preto	Olinda	LAP 2	-7,993655	-34,862949
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.04 Circunscrição - Espinheiro	Rua Othon Paraíso - 343	Torreão	Recife	LAP 2	-8,038139	-34,883991
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.48 Circunscrição - Aliança	Av. Genésio Gomes de Moraes, 840	Centro	Aliança	LAP 1	-7,60815	-35,231048
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.01 Seccional - Santo Amaro	Rua Frei Cassimiro, S/N	Santo Amaro	Recife	LAP 2	-8,045776	-34,881556
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.107 Circunscrição - Brejo Madre Deus	Rua José Bonifácio, 34	Centro	Brejo da Madre de Deus	LAP 1	-8,149927	-36,36906
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.88 Circunscrição - Caruaru	Rua CRISTOVAO COLOMBO, 99	Nossa Sra. das Dores	Caruaru	LAP 2	-8,285247	-35,974131
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.77 Circunscrição - Quipapá	Av. Tito Galvão, 78	Centro	Quipapá	LAP 1	-8,827891	-36,012887
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.80 Circunscrição - Joaquim Nabuco	Rua Manoel Jose da Costa Filho, 30	Centro	Joaquim Nabuco	LAP 1	-8,625788	-35,524933
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.136 Circunscrição - Bom Conselho	Rua José Amaral, 33	Centro	Bom Conselho	LAP 1	-9,163065	-36,678468
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.153 Circunscrição - Angelim	Rua Martiniano da Costa, 53	Centro	Angelim	LAP 1	-8,888627	-36,282414
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.35 Circunscrição - Aracoiaba	Rua JOSE LUIZ DE SILVA, 895	Centro	Araçoiaba	LAP 1	-7,787892	-35,092382
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.123 Circunscrição - São Vicente Ferrer	Praça Pedro Pereira Guedes, 70	Centro	São Vicente Ferrer	LAP 1	-7,591062	-35,487055
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPP.Departamento de Proteção à Pessoa	Rua Tabira, 160, ACADEPOL	Boa Vista	Recife	LAP 2	-8,047277	-34,922786
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.152 Circunscrição - Palmeirina	Rua General Osório, 6	Centro	Palmeirina	LAP 1	-9,002524	-36,323077
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.04 Delegacia da Mulher - Caruaru	Av. Portugal - 155	Universitário	Caruaru	LAP 2	-8,266744	-35,964455

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.57 Circunscrição - Tracunhaem	Rua Antonio Felipe Dos Santos, 110	Centro	Tracunhaem	LAP 1	-7,804725	-35,238926
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Divisão de Patrimônio	Avenida Olinda, Nº 517		Olinda	LAP 2	-8,032688	-34,866807
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.10 Seccional - Cabo de Santo Agostinho	Rua Nova Nº 233	Santo Inácio	Cabo de Santo Agostinho	LAP 2	-8,280736	-35,022187
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Administracao Geral.Recife	Rua da Aurora, Nº487		Recife	LAP 2	-8,059644	-34,880256
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.70 Circunscrição - Palmares	Av. José Americo de Miranda, S/N	Centro	Palmares	LAP 2	-8,681608	-35,584725
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.135 Circunscrição - Garanhuns	Rua Joaquim Tavora, 259	Heliópolis	Garanhuns	LAP 2	-8,885345	-36,487676
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.97 Circunscrição - São Joaquim do Monte	Rua José Cândido da Silva, 5	Centro	São Joaquim do Monte	LAP 1	-8,430864	-35,810937
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Repressão Crimes Contra a Propriedade Imaterial	Av. Liberdade, 364	Tejupió	Recife	LAP 2	-8,08652	-34,952687
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.191 Circunscrição - Caruaru	Rua Juvenal Lopes, 37	Centro	Caruaru	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPCA- Estrada da Batalha - Prazeres	Estrada da Batalha - S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,153934	-34,920667
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.160 Circunscrição - Itaíba	Rua da paz - s/n	Centro	Itaíba	LAP 1	-8,947621	-37,422364
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.AIS.06 Seccional Prazeres	Estrada Da Batalha S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,155819	-34,922648
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.125 Circunscrição - Machados	Rua José Antonio Cardoso, S/N	Centro	Machados	LAP 1	-7,686429	-35,509686
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.16ª Homicídios - Goiana	Rua do Gilo	Centro	Goiana	LAP 2	-7,562018	-35,000342
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.183 Circunscrição - Santa Cruz da Baixa Verde	Rua José Joaquim de Lima, 143	Centro	Santa Cruz da Baixa Verde	LAP 1	-7,820301	-38,148297
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.01 Circunscrição - Rio Branco	Av. Alfredo Lisboa - 188	Recife Antigo	Recife	LAP 2	-8,064813	-34,871937
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.58 Circunscrição - Buenos Aires	Rua José Emiliano, 39	Centro	Buenos Aires	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.43 Circunscrição e plantao - Porto de Galinhas	Rua Praça Dois, 56	Porto de Galinhas	Ipojuca	LAP 2	-8,507955	-35,001761
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.139 Circunscrição - Canhotinho	Praça CORONEL CLOVIS VIDAL, 974	Centro	Canhotinho	LAP 1	-8,879775	-36,198375
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Prédio Sede da Chefia da Polícia Civil (Gabinete da Polícia)	Rua Aurora, Nº 405	Boa Vista	Recife	LAP 2	-8,04756	-34,876961
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.197 Circunscrição - Cedro	Rua Francisco Siqueira Sampaio, 488	Centro	Cedro	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.37 Circunscrição - Camaragibe	Rua Padre Oseas Cavalcante, S/N	Bairro Novo	Camaragibe	LAP 2	-8,017907	-34,981108
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.185 Circunscrição - Quixaba	Rua Marçal Salvador, 544	Centro	Quixabá	LAP 1	-7,719067	-37,847475
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.2ª Divisão de Homicídios - Sul	Av. Barreto de Menezes, 637	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,157871	-34,932744
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.156 Circunscrição + Plantao - Arcoverde	Rua Henrique Dias, 200	Centro	Arcoverde	LAP 2	-8,417794	-37,060965
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.74 Circunscrição - Catende	Rua 15 de Novembro, 71	Centro	Catende	LAP 2	-8,668847	-35,720452
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.181 Circunscrição - Triunfo	Rua Galdino Diniz, 355, S/N	Centro	Triunfo	LAP 1	-7,834685	-38,107821
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.131 Circunscrição - Vertentes	Rua Dr. Emidio Cavalcanti, 255	Centro	Vertentes	LAP 1	-7,90302	-35,98725
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.08 Delegacia da Mulher - Goiana	Praça Duque de Caxias, 66	Centro	Goiana	LAP 2	-7,562282	-34,999399

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Protecao Ao Idoso	Rua Da Glória, 301	São José	Recife	LAP 2	-8,064277	-34,887223
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.16ª DEAM - Palmares	Rua Capitão Pedro Ivo, 590	Centro	Palmares	LAP 2	-8,683924	-35,587264
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.198 Circunscrição - Verdejantes	Rua Osmundo Bezerra, 62	Centro	Verdejante	LAP 1	-7,930238	-38,968544
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.24 Seccional + 200 Circunscrição - Araripina	Av. Gov. Muniz Falcão S/N	Planalto Araripina	Araripina	LAP 1	-7,586153	-40,49998
POLÍCIA CIVIL DE PERNAMBUCO	12ª DPRN - Petrolina	Rua Cardoso de Sá, S/N	Centro	Petrolina	LAP 2	-9,384205	-40,483849
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.143 Circunscrição - Iati	RUA JOÃO DE BARROS SILVA - 2000	Centro	Iati	LAP 1	-9,042085	-36,844234
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DIRH. Diretoria de Recursos Humanos Recife	Rua Tabira, 208	Boa Vista	Recife	LAP 2	-8,050752	-34,891619
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.155 Circunscrição - Terezinha	Av. Profº Agamenon Magalhães, 9	Centro	Terezinha	LAP 1	-9,056631	-36,625452
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.87 Circunscrição - São Benedito do Sul	Rua da Boa Vista, 12	Centro	São Benedito do Sul	LAP 1	-8,806752	-35,935201
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.118 Circunscrição - Passira	Rua Severino Ferreira - 181	Centro	Passira	LAP 1	-7,98306	-35,580725
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.04 Circunscrição.Posto Policial do Hospital da Restauração	Av. Agamenon Magalhães, S/Nº	Derby	Recife	LAP 2	-8,04756	-34,876961
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.140 Circunscrição - Caetés	Rua Dom Jose Adelino Dantas, S/N	Centro	Caetés	LAP 1	-8,771605	-36,626599
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.26 Circunscrição- Rio Doce	Av. Brasil, S/N	Rio Doce	Olinda	LAP 2	-7,945184	-34,859944
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.133 Circunscrição - Santa Maria do Cambuca	Rua Doutor Miguel Brás, 103	Centro	Santa Maria do Cambucá	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.134 Circunscrição - Garanhuns	Av. DANTAS BARRETO, 150	Centro	Garanhuns	LAP 2	-8,888895	-36,492388
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.19 Circunscrição - Prazeres	Estrada da Batalha, S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,155819	-34,922648
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Roubos e Furtos de Cargas	Rua São Miguel, Nº 268	Afogados	Recife	LAP 2	-8,080146	-34,908804
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.110 Circunscrição - Sanharó	Rua Domingos Zuza, 121	Marajas	Sanharó	LAP 1	-8,35822	-36,564656
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.71 Circunscrição - Ribeirão	Av. Mario Domingues, S/N	Cohab	Ribeirão	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.209 Circunscrição - Granito	Av. José Saraiva Xavier, S/N	Centro	Granito	LAP 1	-7,715367	-39,615819
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.13 Seccional- Palmares	Av. Jose Americo De Miranda, S/N	Santa Rosa	Palmares	LAP 2	-8,679116	-35,580084
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.40 Circunscrição + Plantão - Cabo de Santo Agostinho	Br 101, Km 33	Centro	Cabo de Santo Agostinho	LAP 2	-8,3289	-35,106843
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.14 Seccional - Caruaru	BR 104, Km 67, S/N	Divinópolis	Caruaru	LAP 2	-8,295442	-35,988602
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.65 Circunscrição - Pombos	Loteamento Vila Brasil, 71	Vila Brasil	Pombos	LAP 1	-8,14108	-35,396742
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.5ª DPRN - Goiana	Praça duque de caxias	Centro	Goiana	LAP 2	-7,562282	-34,999399
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.7ª DPRN - Caruaru	Rua Cristovão Colombo, 99	Centro	Caruaru	LAP 2	-8,285247	-35,974131
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.69 Circunscrição - Cha de Alegria	Rua Dr. Bernado Porto, S/N	Centro	Chã de Alegria	LAP 1	-8,003445	-35,212179

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.90 Circunscrição - Posto Policial Hospital Regional do Agreste - Caruaru	Hospital Regional Do Agreste, S/N	Indianópolis	Caruaru	LAP 2	-8,307584	-35,968147
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DEPOMA.Delegacia Polícia do Meio Ambiente	R. Itanhenga, 65 - Tejipio, Recife - PE	Tejipio	Recife	LAP 2	-8,09024	-34,951046
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.158 Circunscrição - Sertania	Rua Ulisses Albuquerque, 55	Centro	Sertania	LAP 1	-8,04756	-34,876961
POLÍCIA CIVIL DE PERNAMBUCO	PCPE. 17ª DEAM - Arcoverde	Rua Augusto Cavalcante, 276	Centro	Arcoverde	LAP 2	-8,418837	-37,060425
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.20 Circunscrição - Jaboatão	Av. Barão De Lucena S/N	Centro	Jaboatão dos Guararapes	LAP 2	-8,112701	-35,018644
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.194 Circunscrição - Parnamirim	Rua Matriz, 20	Centro	Parnamirim	LAP 1	-8,06284	-34,885534
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.08 Circunscrição - Jordão	Rua Rio Brígida, 266	Ibura Baixo	Recife	LAP 2	-8,112815	-34,940821
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.179 Circunscrição - Flores	Rua Pedro Santos Estimas - s/n	Centro	Flores	LAP 1	-7,86411	-37,977017
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.208 Circunscrição - Moreilândia	Rua São José - s/n	Centro	Moreilândia	LAP 1	-7,625838	-39,550807
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.62 Circunscrição + Plantão - Gravatá	Rua Travessa QUINTINO BOCAIUVA, S/N	Centro	Gravatá	LAP 1	-8,198744	-35,569268
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.170 Circunscrição - Itapetim	Rua Paulino Soares, 25	Centro	Itapetim	LAP 1	-7,377596	-37,19263
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DTI-Diretoria Tecnologia da Informação	Rua da Aurora	Boa Vista	Recife	LAP 2	-8,059649	-34,880248
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.147 Circunscrição - Jupi	Rua Antonio Inácio Primo - 122	Centro	Jupi	LAP 1	-8,711115	-36,414539
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.166 Circunscrição - Manari	Rua Costa Silva, S/N	Centro	Manari	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.117 Circunscrição - Bom Jardim	Rua Etelvino Solto Maior, 11	Centro	Bom Jardim	LAP 1	-7,79844503	-35,58516468
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.61 Circunscrição + Plantão - Vitória de Santo Antão	Av. Henrique de Holanda, 1333	Cajá	Vitória de Santo Antão	LAP 1	-8,117314	-35,297328
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Mulher Vitória de Santo Antão	Rua Ismael de Andrade, 152, Matriz	Matriz	Vitória de Santo Antão	LAP 1	-8,688366	-35,593922
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.82 Circunscrição - São José da Coroa Grande	Rua Valdemar Acioli Belo - 100	Centro	São José da Coroa Grande	LAP 1	-8,897366	-35,146423
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.103 Circunscrição - Ibirajuba	Rua Prof. José Apolinário, 20	Centro	Ibirajuba	LAP 1	-8,57946	-36,178089
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.146 Circunscrição - Jurema	Rua Jose Maria Simoes, S/N	Centro	Jurema	LAP 1	-8,718837	-36,136983
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.145 Circunscrição - Saloá	Rua Josefa Vicente Psiquira - 39, Centro, Saloá - PE	Centro	Saloá	LAP 1	-8,975935	-36,69112
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DEPATRI. Administração e Delegacia de Repressão ao Estelionato	Rua São Miguel, 268	Afogados	Recife	LAP 2	-8,080137	-34,908713
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.216 Circunscrição - Afrânio	Rua Praça Sebastiao Coelho, S/N	Centro	Afrânio	LAP 1	-8,516062	-41,003161
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.75 Circunscrição - Água Preta	Praça Tres Poderes, 3027	Catende	Água Preta	LAP 1	-8,703245	-35,527942
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.169 Circunscrição - Tabira	Rua ANTONIO PEREIRA MORIM, 2535	Centro	Tabira	LAP 1	-7,583071	-37,536854
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Delitos de Trânsito	Av. Da Recuperação, 95	Dois Irmãos	Recife	LAP 2	-8,022299	-34,943133
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.9 Delegacia de Homicídios - Olinda	Carlos de Lima Cavalcante, 5013	Janga	Olinda	LAP 2	-7,961373	-34,831293

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.01 Delegacia de Polícia de Prevenção e Repressão Aos Crimes Contra a Mulher - Santo Amaro	Rua André Rebouças - 136	Rosarinho	Recife	LAP 2	-8,049688	-34,882877
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.205 Circunscrição - Trindade	Av. Central Sul, 526	Centro	Trindade	LAP 1	-7,766216	-40,26022
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.171 Circunscrição - Iguaraci	Rua D.R. Ulisses Guimarães, S/N	Centro	Iguaraci	LAP 1	-7,835504	-37,512568
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPTUR.Delegacia de Polícia do Turista	Aeroporto Dos Guararapes - Sala 14, 201	Boa Viagem	Recife	LAP 2	-8,125932	-34,924015
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Grupo de Operações Especiais	Rua Odete Monteiro, S/N	Cordeiro	Recife	LAP 2	-8,044763	-34,922019
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.17ª Homicídios Vitória de Santo Antão	Rua: Henrique de Holanda, 1333	Redenção	Vitória de Santo Antão	LAP 1	-8,117287	-35,297355
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.142 Circunscrição - Capoeiras	Av. 21 de Dezembro, 203	Centro	Capoeiras	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.07 Delegacia da Mulher - Surubim	Rua Santos Dumont, N° 69	Cabaceira	Surubim	LAP 2	-7,843675	-35,757791
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.92 Circunscrição - Bonito	Rua Severino N Coelho, 13	Centro	Bonito	LAP 1	-8,473817	-35,728392
POLÍCIA CIVIL DE PERNAMBUCO	PCPE. 15ª DEAM - Olinda	Av. Carlos de Lima Cavalcanti	Casa Caiada, s/n	Olinda	LAP 2	-7,982496	-34,837521
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.159 Circunscrição - Custódia	Rua Luis Epaninondas, S/N	Centro	Custódia	LAP 1	-8,090093	-37,640844
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.23 Seccional - Salgueiro	Rua Joaquim Sampaio, 321	Centro	Salgueiro	LAP 2	-8,070142	-39,123237
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.91 Circunscrição - Bezerros	Av. Francisca De Moraes Lemos, S/N	São Pedro	Bezerros	LAP 1	-8,237751	-35,748486
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Complexo Policial de Paulista - Criança e Adolescente	Rua Do Cajueiro, S/N		Paulista	LAP 2	-7,940577	-34,884657
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.15 Circunscrição - Alto do Pascoal	Av. Anibal Benevolo, S/N	Agua Fria	Recife	LAP 2	-8,009998	-34,898523
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.17 Circunscrição - Vasco da Gama	Rua Vasco da Gama S/N	Vasco da Gama	Recife	LAP 2	-8,012351	-34,920104
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Policia Interestadual e Capturas	Av.Liberdade, 364	Tejipió	Recife	LAP 2	-8,08652	-34,952687
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.41 Circunscrição - Ponte dos Carvalhos	Rua Vicente Yanes Pizon, N°36	Ponte Dos Carvalhos	Cabo de Santo Agostinho	LAP 2	-8,232715	-34,981385
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.195 Circunscrição - Serrita	Rua Antônio Filgueira Sampaio, 35	Centro	Serrita	LAP 1	-7,948483	-39,29431
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.63 Circunscrição - Escada	Rua Mangueira, S/N	Atalaia	Escada	LAP 2	-8,368518	-35,23266
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.33 Circunscrição - Cruz de Rebouças	Av. Luciana Paiva, 100	Cruz De Rebouças	Igarassu	LAP 2	-7,87411	-34,908555
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.UNITOF - Unidade de Transporte e Oficina	Rua Coelho Leite, 570	Santo Amaro	Recife	LAP 2	-8,049067	-34,879781
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.49 Circunscrição - Itambé	Rua Joaquim Nabuco, 32	Centro	Itambé	LAP 1	-7,409853	-35,110171
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.16 Seccional + 115 Circunscrição - Limoeiro	Av. Geronimo Heraclito, 1559	Juá	Limoeiro	LAP 1	-7,86667	-35,435088
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.168 Circunscrição - Sao Jose do Egito	PE 320 - S/N(Vizinho ao Lar do Idoso), CEP 56.70	Centro	São José do Egito	LAP 1	-7,508829	-37,324650
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.151 Circunscrição - Jucati	Avenida Rua Rui Barbosa, 180	Centro	Jucati	LAP 1	-8,705919	-36,487403
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.59 Circunscrição - Ferreiros	Rua Monsenhor Júlio Maria, 95a	Centro	Ferreiros	LAP 1	-7,44803	-35,24386

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.79 Circunscrição - Tamandare	Rua Nova Canpina, 758	Centro	Tamandaré	LAP 1	-8,755314	-35,099041
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.46 Circunscrição - Timbauba	Rua Irmão Albertine, 46	Centro	Timbaúba	LAP 1	-7,51179	-35,319382
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.201 Circunscrição - Ouricuri	Av. Pres. Kennedy, 85	Centro	Ouricuri	LAP 2	-7,887304	-40,084955
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.60 Circunscrição - Camutanga	Rua Ciro Alves, 90	Centro	Camutanga	LAP 1	-7,409081	-35,271991
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.108 Circunscrição - São Caetano	Rua Olindino Santino, S/N	Centro	São Caetano	LAP 1	-8,326661	-36,137465
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.13 Circunscrição - Mustardinha	Estrada Velha Do Bongi, 922	Bongi	Recife	LAP 2	-8,065045	-34,915793
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.03 Delegacia da Mulher - Petrolina	BR 428 km 122, S/N	Centro	Petrolina	LAP 2	-9,150705	-40,359057
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.129 Circunscrição - Toritama	Rua Projetada - s/n	Novo Alvorecer	Toritama	LAP 1	-8,010132	-36,066969
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.27 Circunscrição - Abreu e Lima	Rua Mascarenhas De Moraes, Nº 137	Timbó	Abreu e Lima	LAP 2	-7,91176	-34,902546
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.109 Circunscrição - Cachoeirinha	Rua Luiz Gonzaga, 134	Centro	Cachoeirinha	LAP 1	-8,493605	-36,238272
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.17 Seccional + 128 Circunscrição - Santa Cruz do Capibaribe	Rua José Francisco Barbosa, 321	Centro	Santa Cruz do Capibaribe	LAP 2	-7,953748	-36,205514
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Roubos e Furtos de Veículos	Rua São Miguel, 268	Afogados	Recife	LAP 2	-8,080146	-34,908804
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.182 Circunscrição - Betânia	Rua Enoque Guerra, S/N	Centro	Betânia	LAP 1	-8,274485	-38,031132
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPCRIC -Crimes Cibernéticos	Gervásio Pires	Boa Vista	Recife	LAP 2	-8,057355	-34,885054
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.204 Circunscrição - Ipubi	Rua Guaraci, 71	Centro	Ipubi	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.186 Circunscrição - Petrolândia	Rua Manoel Rodrigues de Almeida - 77	Centro	Petrolândia	LAP 1	-8,979007	-38,217313
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DRACO	Av. Liberdade, 364	Tejipió	Recife	LAP 2	-8,086692	-34,952882
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.120 Circunscrição - João Alfredo	Rua JOSE ERCULANO SOARES, S/N	Centro	João Alfredo	LAP 1	-7,862065	-35,589888
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.83 Circunscrição - Xexeu	Rodovia Governador Covas S/N	Centro	Xexéu	LAP 1	-8,809295	-35,627682
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.73 Circunscrição - Sirinhaém	Rua Sebastião Chaves, 412	Centro	Sirinhaém	LAP 1	-8,591807	-35,116086
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.30 Circunscrição - Itamaraca	Av Joao Pessoa Guerra, 230	Pilar	Ilha de Itamaracá	LAP 2	-7,749629	-34,825117
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.NI PETROLINA	Rua Luiz Gonzaga - 47	Centro	Petrolina	LAP 2	-9,390469	-40,503473
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.150 Circunscrição - Paratama	Rua Francisco de Paulo Melo, 08	Centro	Paratama	LAP 1	-8,918946	-36,658926
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.202 Circunscrição - Exu	Av. Edmundo Dantas, 140	Centro	Exu	LAP 1	-7,51308	-39,721391
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Prevenção e Repressão Ao Narcotráfico	Rua Da União, N 225	Boa Vista	Recife	LAP 2	-8,059931	-34,881269
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.165 Circunscrição - Inajá	Rua José Malaquias Dos Santos, 53	Centro	Inajá	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.172 Circunscrição - Santa Terezinha	Rua Jose Davi de Vasconcelos, 117	Centro	Santa Terezinha	LAP 1	-7,377024	-37,48038
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.15 Seccional + 104 Circunscrição - Belo Jardim	Rua Sebastião Rodrigues Da Costa, S/N	SÃO PEDRO	Belo Jardim	LAP 1	-8,322848	-36,415543

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.56 Circunscrição - Lagoa do Carro	Rua Antonio Francisco da Silva, 47	Centro	Lagoa do Carro	LAP 1	-7,84303	-35,309355
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.154 Circunscrição - Brejão	Rua José Inácio dos Santos, 83	Centro	Brejão	LAP 1	-9,029292	-36,565554
POLÍCIA CIVIL DE PERNAMBUCO	8º DENARC - Granhuns	Rua Barreto Coelho, S/N	Magano	Garanhuns	LAP 2	-8,88076	-36,497565
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Departamento de Polícia da Mulher - Recife	Av. Alfredo Lisboa, 539	Recife Velho	Recife	LAP 2	-8,062208	-34,871145
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.105 Circunscrição - Pesqueira	Av. Maria de Brito, S/N	Centro	Pesqueira	LAP 1	-8,356302	-36,693451
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Delegacia de Roubos e Furtos	Rua São Miguel, 268	Afogados	Recife	LAP 2	-8,080146	-34,908804
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.164 Circunscrição - Venturosa	Av. Jose Alves Bezerra, 198	Centro	Venturosa	LAP 1	-7,945795	-39,293515
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.90 Circunscrição - Caruaru	Rodovia Br-104 km67, S/N	Pinheirópolis	Caruaru	LAP 2	-8,23953	-35,980598
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.2 Seccional - Agua Fria	Rua Júlio Ramos, 171	Água Fria	Recife	LAP 2	-8,038139	-34,883991
POLÍCIA CIVIL DE PERNAMBUCO	PCPE. 11ª DEAM - Salgueiro	Rua antonio figuereado sampaio	Nossa Senhora das graças	Salgueiro	LAP 2	-8,068349	-39,120109
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.141 Circunscrição - Sao Joao	Rua Antonio Vilela,14	Centro	São João	LAP 1	-8,876755	-36,368034
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.100 Circunscrição - Camocim de Sao Felix	Av. Agamenon Magalhães, 21	Centro	Camocim de São Félix	LAP 1	-8,362282	-35,762956
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.89 Circunscrição - Caruaru	Rua bartomeu de anacleto, S/N	Salgado	Caruaru	LAP 2	-8,273801	-35,957754
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.3ª DIV. HOMICÍDIOS CARUARU	BR 104 Km 67, S/N	Agamenon Magalhães	Caruaru	LAP 2	-8,23953	-35,980598
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.113 Circunscrição - Alagoinha	Av. Frei Geronimo, 185	Centro	Alagoinha	LAP 1	-8,46789169	-36,7750169
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.111 Circunscrição - Jatauba	Av. JOSÉ LOPES SIQUEIRA, 510	Centro	Jatáuba	LAP 1	-7,985531	-36,500417
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.55 Circunscrição - Itaquitinga	Rua Joaquim Bezerra Perreira, 30	Centro	Itaquitinga	LAP 1	-7,664765	-35,100867
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.09 Delegacia da Mulher - Garanhuns	Av. Frei Caneca, 460	Heliópolis	Garanhuns	LAP 2	-8,882299	-36,481648
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.199 Circunscrição - Terra Nova	Rua Jose gomes da Costa, 25	Centro	Terra Nova	LAP 1	-8,230378	-39,380539
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.66 Circunscrição - Amaraji	Praça Jorge Coelho Silva, S/N	Centro	Amaraji	LAP 1	-8,377827	-35,450986
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.29 Circunscrição - Igarassu	Av Severino Uchoa Cavalcante 63	Centro	Igarassu	LAP 2	-7,831861	-34,909287
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.207 Circunscrição - Santa Cruz de Malta	Rua 3 de Maio, 140	Centro	Santa Cruz	LAP 1	-8,04756	-34,876961
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.21 Circunscrição - Moreno	Rua Artur Mendonça - 253	Bela Vista	Moreno	LAP 2	-8,119046	-35,092078
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.07 Seccional - Varadouro - Olinda	Av. OLINDA, 517	Varadouro	Olinda	LAP 2	-8,023322	-34,859356
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.44 Circunscrição - Goiana	Rua Senador de Barros de Carvalho, 190	Cidade Nova	Goiana	LAP 2	-7,5591529	-34,9975633
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.212 Circunscrição - Orocó	Rua Quirino O Do Nascimento, 29	Centro	Orocó	LAP 1	-8,618931	-39,600698
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.175 Circunscrição - Solidão	Rua Riacho Verde, S/N	Centro	Solidão	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.67 Circunscrição - Cha Grande	Rua Noberto Cruz, 273	Centro	Chã Grande	LAP 1	-8,245373	-35,461887
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.68 Circunscrição - Primavera	Praça Presidente Castelo Branco, 92	Centro	Primavera	LAP 1	-8,329627	-35,352753

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.12 Seccional- Vitoria de Santo Antao	Av. Henrique De Holanda, 1333	Cajá	Vitória de Santo Antão	LAP 1	-8,117314	-35,297328
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.ACADEPOL.LINK-PRINCIPAL	Tabira, Nº 160	Boa Vista	Recife	LAP 1	-8,050722	-34,891921
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.85 Circunscricao -Jaqueira	Rua Vereador Nova Cosque, 287	Centro	Jaqueira	LAP 1	-8,729605	-35,796616
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.47 Circunscricao - Paudalho	Rua SENADOR PINHEIRO RAMOS, 160	Centro	Paudalho	LAP 2	-7,897923	-35,175892
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.99 Circunscricao - Lagoa Dos Gatos	Rua Professor Manoel Edmundo, S/N	Centro	Lagoa dos Gatos	LAP 1	-8,651964	-35,90459
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.54 Circunscricao - Lagoa de Itaenga	Rua Leopoldina Pinheiro, S/N	Centro	Lagoa do Itaenga	LAP 1	-7,932118	-35,293726
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.102 Circunscricao - Barra de Guabiraba	Rua Prachedes Bezerra Frereira Pontes, 74	Centro	Barra de Guabiraba	LAP 1	-8,420478	-35,660649
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Força Nacional	Marechal Floriano Peixoto		Paulista	LAP 2	-7,939741	-34,880308
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.126 Circunscricao - Vertentes do Lério	Rua Maria Salomé De Souza, S/N	Centro	Vertente do Lério	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.210 Circunscricao - Santa Maria da Boa Vista	Rua Oscar Sampaio, S/N	Centro	Santa Maria da Boa Vista	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.19 Seccional - Arcoverde	Rua Henrique Dias, 200	Centro	Arcoverde	LAP 2	-8,058402	-34,896541
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.162 Circunscricao - Tupanatinga	Rua Sete de Setembro, 50	Centro	Tupanatinga	LAP 1	-8,753775	-37,34218
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DINTEL. Diretoria Inteligencia. Recife	Rua Natercio De Holanda 4	Espinheiro	Recife	LAP 2	-8,041382	-34,894389
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.12 Circunscricao - Jardim Sao paulo - Tejipió	Praça De Jardim São Paulo, 240	Jardim São Paulo	Recife	LAP 2	-8,081652	-34,938978
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.78 Circunscricao - Rio Formoso	Rua Adelmo Lucas de Oliveira S/N	Centro	Rio Formoso	LAP 1	-8,66365	-35,154839
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.124 Circunscricao - Casinhas	Rua Coronel Perianandro, 144	Centro	Casinhas	LAP 1	-7,744719	-35,722734
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.217 Circunscricao - Dormentes	Rua Salustiano, 10	Centro	Dormentes	LAP 1	-8,445703	-40,766388
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.157 Circunscricao - Bulque	Rua Odilon Nopa de Azevedo, 28	Centro	Bulque	LAP 1	-8,622002	-37,156175
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.10 Circunscricao - Ibura	Av. Campina Grande, S/N	(Cohab) Ur-1 - Pe	Recife	LAP 2	-8,119705	-34,948037
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.38 Circunscricao -Sao Lourenco da Mata	Av. Dr. Francisco Correia, Nº 74	Centro	São Lourenço da Mata	LAP 2	-7,997443	-35,036471
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.190 Circunscricao - Jatoba	Av. Das Flores, S/N	Centro	Jatobá	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.138 Circunscricao - Lajedo	Av. Agamenom Magalhães, 381	Centro	Lajedo	LAP 1	-8,662657	-36,320187
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.11 Seccional - Goiana	Praça Duque de Caxias, 661	Vila Jardim Pompeia	Goiana	LAP 2	-7,562481	-34,999741
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.86 Circunscricao - Belem de Maria	Rua Jeter Carlos, 34	Centro	Belém de Maria	LAP 1	-8,62304922	-35,8416911
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.106 Circunscricao- Sao Bento do Una	Rua João Pessoa, 505	Centro	São Bento do Una	LAP 1	-8,528344	-36,439339
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.127 Circunscricao - Salgadinho	Rua Ana Barbosa Amorim, S/N	Centro	Salgadinho	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.09 Circunscrição - Ipsep	Av Jean Emile Favre, S/N	Ipsep	Recife	LAP 2	-8,113588	-34,922169

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.25 Seccional + 211 Circunscrição - Cabrobo	Rua Epaminindas Hipólito de Lima, 1087	Centro	Cabrobó	LAP 1	-8,511009	-39,310854
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.130 Circunscrição - Taquaritinga do Norte	Rau 15 De Janeiro, 115	Centro	Taquaritinga do Norte	LAP 1	-7,89977295	-36,4710173
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.122 Circunscrição - Feira Nova	Rua Santos Dunont, 154	Centro	Feira Nova	LAP 1	-7,949637	-35,384049
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.50 Circunscrição - Nazare da Mata	Rua Dom Ricardo Virela, 951	Centro	Nazaré da Mata	LAP 2	-7,741878	-35,226143
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.03 Circunscrição - Joana Bezerra	Rua Visconde de Suassuna	Boa Vista	Recife	LAP 2	-8,052236	-34,886757
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.215 Circunscrição - Lagoa Grande	Rua Senador Marcos Freire, 60	Centro	Lagoa Grande	LAP 1	-8,996607	-40,270248
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.PP São Domingos	Rua José Francisco Barbosa, 321	Nova Santa Cruz	Santa Cruz do Capibaribe	LAP 2	-7,95360845	-36,2054659
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.206 Circunscrição - Santa Filomena	Praça Matriz, 65	Centro	Santa Filomena	LAP 1	-8,162439	-40,614626
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.22 Seccional + 187 Circunscrição - Floresta	Av. Audomar Ferraz, 193	Centro	Floresta	LAP 1	-8,598948	-38,572505
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Central de Flagrantes	Rua Odorico Mendes, 700	Campo Grande	Recife	LAP 2	-8,038525	-34,87977
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.76 Circunscrição - Gameleira	Rua Luiz Rodolfo, 333	Santo Antônio	Gameleira	LAP 1	-8,58698	-35,386176
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.23 Circunscrição - Cavaleiro	Rua Euclides Matoso, S/N	Cavaleiro	Jaboatão dos Guararapes	LAP 2	-8,09083	-34,970877
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.23ª Homicídios Arcoverde	Rua HENRIQUE DIAS	Centro	Arcoverde	LAP 2	-8,417898	-37,060042
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.193 Circunscrição - Salgueiro	Rua Joaquim Sampaio, 321	Nossa Sra. das Graças	Salgueiro	LAP 2	-8,070142	-39,123237
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.42 Circunscrição - Ipojuca	R. Hilda Da Costa Monteiro, 72	Centro	Ipojuca	LAP 2	-8,39741	-35,059368
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.96 Circunscrição - Agrestina	Rua Prefeito Sebastião Grande, 5	Centro	Agrestina	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.9ª DESEC e 37ª Circ. Camaragibe	Rua Padre Osias Cavalcante S/N	Novo Carmelo	Camaragibe	LAP 2	-8,017907	-34,981108
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.137 Circunscrição - Aguas Belas	Rua Santa Cruz, S/N	Centro	Aguas Belas	LAP 1	-9,11258	-37,1206
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.53 Circunscrição - Condado	Rua José Correia, 7	Centro	Condado	LAP 1	-7,58639662	-35,1084179
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.161 Circunscrição-Ibimirim	Rua Carlos Augusto de Melo, 1080	Centro	Ibimirim	LAP 1	-8,527322	-37,553453
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.119 Circunscrição - Cumaru	Av. Santa Terezinha, 19	Centro	Cumaru	LAP 2	-8,022371	-34,976799
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.21ª Homicídios Staª Cruz Capibaribe	Rua José Francisco Barbosa	Centro	Santa Cruz do Capibaribe	LAP 2	-7,953378	-36,204856
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DECCOT	Rua Imperial - 2077	São José	Recife	LAP 2	-8,04756	-34,876961
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.121 Circunscrição - Orobo	Rua Cel. Antonio de Moura - 11	Manoel de Aprício	Orobó	LAP 1	-7,752315	-35,599625
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.26 DESEC	Rua Padre Fraga - 50	centro	Petrolina	LAP 2	-9,393877	-40,480839
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.NI CARUARU	Rua Capitão de, 674	Indianópolis	Caruaru	LAP 2	-8,293182	-35,959606
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Almoxarifado	Av. Olinda, 517	Santa Tereza	Olinda	LAP 2	-8,023322	-34,859356
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.174 Circunscrição - Brejinho	Rua Joao Nunes, 216	Centro	Brejinho	LAP 1	-7,34987	-37,286249

POLÍCIA CIVIL DE PERNAMBUCO	2ª DP 19ª CIRCUNSCRIÇÃO - MURIBECA	Avenida Doutor Júlio Maranhão, 30		Jaboatão dos Guararapes	LAP 2	-8,177748	-34,948976
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.98 Circunscrição - Riacho Das Almas	Rua Raul Bandeira Santa Teresinha, 13	Centro	Riacho das Almas	LAP 1	-8,135818	-35,854574
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.34 Circunscrição - Maria Farinha	AV. CLAUDIO GUEIROS LEITE, S/N		Paulista	LAP 2	-7,9061	-34,825917
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.05 Circunscrição - Casa Amarela	R. Paula Batista, N.º 616	Casa Amarela	Recife	LAP 2	-8,027815	-34,916859
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.189 Circunscrição - Tacaratu	Rua Capitão José xavier - 285	Centro	Tacaratu	LAP 1	-9,109028	-38,151856
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.02 Circunscrição - Boa Vista	Rua Frei Cassimiro, 261	Santo Amaro	Recife	LAP 2	-8,04701	-34,879954
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.149 Circunscrição - Lagoa do Ouro	Rua Progresso, S/N	Centro	Lagoa do Ouro	LAP 1	-9,125002	-36,460343
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.84 Circunscrição - Cortes	Rua Veloso da Silveira, 30	Centro	Cortês	LAP 1	-8,47242	-35,543025
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.45 Circunscrição - Carpina	Rua Enestor Pupilio, 111	Santo Antônio	Carpina	LAP 2	-7,843537	-35,260835
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.06 Circunscrição - Cordeiro	Rua Antero Mota, Nº 87	Cordeiro	Recife	LAP 2	-8,045886	-34,92754
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPCA. Delegacia Policial de Apuração de Crimes Contra Criança e Adolescente	RUA BENFICA, 1008	MADALENA	Recife	LAP 2	-8,0578	-34,908126
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.196 Circunscrição - Mirandiba	Rua Cornelio Soares, 85	Centro	Mirandiba	LAP 1	-8,119522	-38,730658
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.LABLD	RUA IMPERIAL, 20	SÃO JOSE	Recife	LAP 2	-8,072822	-34,88568
POLÍCIA CIVIL DE PERNAMBUCO	PCPE. 19ª Homicídios Caruaru	BR 104 - Km 67 - Divinópolis		Caruaru	LAP 2	-8,143286	-36,045844
POLÍCIA CIVIL DE PERNAMBUCO	CORE - ADMINISTRAÇÃO	RUA JOSÉ DIAS RAPOSO,	OURO PRETO	Olinda	LAP 2		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.178 Circunscrição - Sao Jose do Belmonte	Rua Rufino Pires da Silva, 19	Centro	São José do Belmonte	LAP 1	-7,864638	-38,759787
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.11 Circunscrição - Afogados	Rua João Carlos Guimarães 136 -	Afogados	Recife	LAP 2	-8,078774	-34,905571
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.93 Circunscrição - Pannels	Praça Coronel João Rufino, 10	Centro	Pannels	LAP 1	-8,663529	-36,005139
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.51 Circunscrição - Vicencia	Rua Prof Mota Albuquerque, S/N	Centro	Vicência	LAP 1	-7,653203	-35,32001
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.22 Circunscrição - Piedade	R. São Sebastiao, S/N		Jaboatão dos Guararapes	LAP 2	-8,182571	-34,926174
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.22 Delegacia de Homicidio	Rua Barreto Coelho, S/N	Santo onofre	Garanhuns	LAP 2	-8,880903	-36,497101
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.52 Circunscrição - Macaparana	Av. João Francisco, 134	Centro	Macaparana	LAP 1	-7,552772	-35,448786
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.163 Circunscrição - Pedra	Rua Capitaio Manoel Leite, 40	Centro	Pedra	LAP 1	-8,499309	-36,943354
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.132 Circunscrição - Frei Miguelinho	Rua Dom Pedro Segundo, 12	Boa vista	Frei Miguelinho	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.116 Circunscrição - Surubim	Av. São Sebastião, 407	Centro	Surubim	LAP 2	-7,845185	-35,760946
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.203 Circunscrição - Bodoco	Rua Lourival Rodrigues, 262	Centro	Bodocó	LAP 1	-7,778701	-39,935653
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.Deposito da 26 DESEC	Av. Jatobá, 20	Jatobá	Petrolina	LAP 2	-9,394901	-40,471225
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DPCA - Delegacia Policial de Proteção à Criança e Ao Adolescente - Plantão	Rua João Fernandes Vieira, 405	Boa Vista	Recife	LAP 2	-8,052986	-34,892395
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.101 Circunscrição - Saire	Rua David Lins De Andrade, S/N	Centro	Sairé	LAP 1	-8,329007	-35,711033

POLÍCIA CIVIL DE PERNAMBUCO	PCPE.184 Circunscrição - Calumbi	Av. Central, S/N	Centro	Calumbi	LAP 1		
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.144 Circunscrição - Correntes	Rua Professora Janoca, 17	Centro	Correntes	LAP 1	-9,128889	-36,326267
POLÍCIA CIVIL DE PERNAMBUCO	18ª Homicídios - Palmares	Américo de Miranda	Santa Rosa	Palmares	LAP 2	-8,67884	-35,583879
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.36 Circunscrição - Fernando de Noronha	Vila Do Trinta, 30	Centro	Fernando de Noronha	LAP 1	-3,842581	-32,410638
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.25 Circunscrição - Peixinhos - Olinda	Av. Nacional, 333	Peixinhos	Olinda	LAP 2	-8,013362	-34,876448
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.14 Delegacia da Mulher - Cabo	BR 101 - s/n	Pontezinha	Cabo de Santo Agostinho	LAP 2	-8,226849	-34,969968
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.72 Circunscrição - Barreiros	Rua Santa terezinha, S/N	Tibiri	Barreiros	LAP 1	-8,814995	-35,198731
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.21 Seccional + 177 Circunscrição - Serra Talhada	Rua Enoque De Carvalho S/N	Várzea	Serra Talhada	LAP 2	-7,994843	-38,289535
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.176 Circunscrição. Ingazeira	Rua Albino Feitosa, 130	Centro	Ingazeira	LAP 1	-7,678335	-37,459313
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.IITB-SEDE.LINK-PRINCIPAL	Rua Da Aurora, Nº 1633	Santo Amaro	Recife	LAP 1	-8,060758	-34,880801
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.IITB-SEDE.LINK-PRINCIPAL	Rua Da Aurora, Nº 1633	Santo Amaro	Recife	LAP 2	-8,060758	-34,880801
POLÍCIA CIVIL DE PERNAMBUCO	PCPE.DINTER 1 + Gerencia de Controle Operacional do Interior 1 - Caruaru			Caruaru	LAP 2	-8,271778	-35,981504
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ªCIPM.PELOTÃO.ITACURUBA	Rua Olegario Resende, S/N	Centro	Itacuruba	LAP 1	-8,72597	-38,687009
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.17ªBPM.NSC.JARDIM PAULISTA	Av. Tancredo Neves, S/N	Jardim Paulista	Paulista	LAP 1	-7,946473	-34,899714
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ªBPM.4ªCIA	Rua Benjamin Constant, S/N	Centro	Flores	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ªBPM	Av. Coronel Veremundo Soares, Km 512, S/N	Nossa Sra. das Graças	Salgueiro	LAP 1	-8,06736	-39,134699
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.17ªBPM	RUA NOVA MANGUEIRA N 05	Centro	Paulista	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.17ªBPM	RUA NOVA MANGUEIRA N 05	Centro	Paulista	LAP 2	-7,942659	-34,885037
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ªBPM.9ªCIA.ARARIPINA	Praça Maria da Silva Modesto, S/N	Centro	Araripina	LAP 1	-7,58340941	40,50095418
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.26ªBPM	Rua Barão de Itapissuma	Centro	Itapissuma	LAP 1	-7,773356	-34,905892
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ªCIPM.PELOTÃO.VERTENTES	Rua Doutor Emídio Cavalcante, 225	Centro	Vertentes	LAP 1	-7,903182	-35,987459
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DAL	Rua Dois irmãos, 1060	Apipucos	Recife	LAP 1	-8,015604	-34,942436
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ªCIPM.PELOTÃO.OROCÓ	Rua Francisco Gorgonho, S/N	Centro	Orocó	LAP 1	-8,61895	-39,6024
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.RPMON.CARUARU	Rua Raul Amaral, 251	Maurício de Nassau	Caruaru	LAP 1	-8,265863	-35,977254
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ªBPM.POSTO.LAGOA DO OURO	Rua Ienivaldo cândido de melo,s/n	Centro	Lagoa do Ouro	LAP 1	-9,123192	-36,459743
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DINTER1	Rua Raul Amaral, 251	Divinópolis	Caruaru	LAP 1	-8,265863	-35,977254
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CPS	Rua Coronel Cornelio Soares, 651	Nossa Sra. da Penha	Serra Talhada	LAP 1	-7,992428	-38,29932
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ªBPM.PELOTÃO.CARNAÍBA	Rua Professora Maria Alvani Da Silva, S/N	Centro	Carnaíba	LAP 1		

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.DESTACAMENTO.LAGOA DO CARRO	Rua NATANAEL JOAQUIM DA PAZ, 48	Centro	Lagoa do Carro	LAP 1	-7,840514	-35,312918
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.2ªCIA.PARNAMIRIM	Av. Aristande Ferreira Lima, S/N	Centro	Parnamirim	LAP 1	-8,090865	-39,576949
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIATUR.RIBEIRA	Rua Bernardo Vieira de Melo, 102 - Sítio Histórico	Varadouro	Olinda	LAP 1	-8,015308	-34,852808
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ªCIPM.NSC.CHÃ GRANDE	Rua MANOEL FAUSTINO DE QUEIROZ, 67	Centro	Chã Grande	LAP 1	-8,238436	-35,463336
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ªCIPM.ITAQUITINGA	Rua Valdomiro Mendes Perreira, S/N	Centro	Itaquitinga	LAP 1	-7,671718	-35,106678
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.24ºBPM.TORITAMA	Rua Dorival José Pereira, 826 (BR 104)	Parque das Pedras	Toritama	LAP 1	-8,006317	-36,064899
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ºBPM.PELOTÃO.TACAIBÓ	Rua Ines Carmelita Araújo, 155	Centro	Tacaibó	LAP 1	-8,314181	-36,293207
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.PELOTÃO.ALTINHO	Av. Vereador João Alves da Silva, 30	Centro	Altinho	LAP 1	-8,490193	-36,056996
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.2ªCIA	Rua Quinze de Novembro, S/N	Centro	Timbaúba	LAP 1	-7,513684	-35,308842
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DASDH	Rua Francisco Barreto S/N	Ipsep	Recife	LAP 1	-8,108647	-34,921738
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.DPM.JAQUEIRA	Av. DORINHA RODRIGUES, 369	Centro	Jaqueira	LAP 1	-8,730789	-35,795357
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.PELOTÃO.CORRENTES	Av. Inaura de Horlando, 166	Centro	Correntes	LAP 1	-9,128817	-36,327042
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DESTACAMENTO.CAETÉS	Rua Alfredo C de Araujo, S/N	Centro	Caetés	LAP 1	-8,777553	-36,62091
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.3ªCIA	Rua Capitão Lisinaco, S/N	Centro	Bom Conselho	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.CADEIA.ALIANÇA	Rua Luis Inácio, S/N	Centro	Aliança	LAP 1	-7,603558	-35,229273
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.VENTUROSA	Rua Augusto Mendes, S/N	Centro	Venturosa	LAP 1	-8,574838	-36,8802
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.1ªCIA	s N:16, Centro	Centro	Carpina	LAP 1	-7,843912	-35,258904
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.3ªCIA	Rua Manoel Fauto Gomes, S/N	Centro	Ibimirim	LAP 1	-8,40051339	-37,5781683
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM	Rua PASTOR JOÃO BALBINO, 47	Centro de Quipapá	Quipapá	LAP 1	-8,826853	-36,011423
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ºBPM.NSC.OURO PRETO	Rua Puma, S/N	Ouro Preto	Olinda	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.MANARI	Rua COSTA E SILVA, 420	Centro	Manari	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ºBPM.1ªCIA.BODOCÓ	RUA LOURIVAL RODRIGUES - 288	Centro	Bodocó	LAP 1	-7,778626	-39,935471
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.DESTACAMENTO.PAUDALHO	Av. SENADOR PINHEIRO RAMOS, 160	Centro	Paudalho	LAP 1	-7,897923	-35,175892
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.RPMON	Av. General San Martin, S/N	San Martin	Recife	LAP 1	-8,066978	-34,927393
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.2ªCIA.MIRANDIBA	Rua Tiburtino De Carvalho, S/N	Centro	Mirandiba	LAP 1	-8,117437	-38,727316

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.AFRÂNIO	Rua Cachoeiras 153	Centro	Afrânio	LAP 1	-8,516425	-41,008231
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.IGUARACY	Rua Maria Santana Siqueira, S/N	Centro	Iguaracy	LAP 1	-7,83823986	-37,51697532
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.JUREMA	Praça Bandeira, S/N	Centro	Jurema	LAP 1	-8,719032	-36,13815
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DESTACAMENTO.IATI	Rua Manoel Florencio de Souza, S/N	Centro	Iati	LAP 1	-9,04109566	-36,84331559
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CPM.PETROLINA	Av. Coronel Otacilio Ferraz, 20	Jatobá	Petrolina	LAP 1	-9,394901	-40,471225
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.25º BPM.NSC.CURADO	Rua 7, S/N	Curado	Jaboatão dos Guararapes	LAP 1	-8,068861	-34,994309
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIPOMA.CASA COMANDO	Br 363, S/N	Floresta Nova	Fernando de Noronha	LAP 1	-3,863789	-32,428244
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.13ºBPM	Rua Odorico Mendes, 700	Campo Grande	Recife	LAP 1	-8,038525	-34,87977
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.PELOTÃO.VERTENTE DO LÉRIO	Av. Capitão Luiz de França, 6	Centro	Vertente do Lério	LAP 1	-7,905233	-35,988268
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ºBPM.PELOTÃO.SÃO CAETANO	Av. Luiz Coimbra, S/N	Centro	São Caetano	LAP 1	-8,328534	-36,137628
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.3ªCIA.SERRITA	Av. Presidente Getulio Vargas, S/N	Brasília	Serrita	LAP 1	-7,944142	-39,294889
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIPOMA	Rua Do Cajá, S/N	Cruz De Rebouças	Igarassu	LAP 1	-7,877619	-34,898277
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.NISC.VICÊNCIA	Rua Professor Mota Albuquerque, S/N	Centro	Vicência	LAP 1	-7,653203	-35,32001
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.3ªCIA	Praça Da Bandeira, S/N	Centro	São José do Egito	LAP 1	-7,4795	-37,276094
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.PELOTÃO.TERRA NOVA	Rua Joaquim De Sá Parente, S/N	Centro	Terra Nova	LAP 1	-8,227562	-39,377241
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.QCG.LINK INTERNET	Praça Do Derby, S/N	Centro	Recife	LAP 1	-8,056758	-34,899534
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ªCIPM.PELOTÃO.INAJÁ	Avenida Tenente Domingos Gomes - 320	Centro	Inajá	LAP 1	-8,904992	-37,826019
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.GARANHUNS.SEDE	Avenida rua barbosa, 1122		Garanhuns	LAP 1	-8,882962	-36,479315
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.2ªCIA	Rua João Vericimo, S/N	Centro	Custódia	LAP 1	-8,086214	-37,644672
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.POSTO.RAJADA	Av. Nilo Coelho, 70	Centro	Petrolina	LAP 1	-8,507878	-39,31052
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.19ºBPM.NSC.UR02	Rua João Felipe Dos Santos, S/N	Ibura	Recife	LAP 1	-8,135138	-34,954904
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.SERTÂNIA	Pe 230, Km 3, S/N	Centro	Sertânia	LAP 1	-8,072906	-37,266019
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ºBPM.SANTA CRUZ DA BAIXA VERDE	Rua Padre Cícero - 102	Centro	Santa Cruz da Baixa Verde	LAP 1	-7,820273	-38,151551
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.21ºBPM.PELOTÃO.POMBOS	Praça João Pessoa, S/N	Centro	Pombos	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ºBPM	Rua Almir Souza Mascarenhas, S/N	Centro	Ouricuri	LAP 1	-7,885987	-40,087466
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ªCIPM.FLORESTA	Rua Major Jose Rodrigues de Moraes, 32	Centro	Floresta	LAP 1	-8,60344498	-38,5733962
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.PELOTÃO.LAGOA DE ITAENGA	Av. São Sebastião, 195	Centro	Lagoa do Itaenga	LAP 1	-7,932225	-35,293253
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DESTACAMENTO.SALOÁ	Av. José Bezerra de Lima, S/N	Centro	Saloá	LAP 1	-8,975935	-36,69112

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.VILA MÉDICA	Rua Cel. Silva Torres, 117	Graças	Recife	LAP 1	-8,053635	-34,903211
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1º CPM 3º BPM - Pedra	Rua Geronimo Siqueira, S/N	Centro	Pedra	LAP 1	-8,575015	-36,874258
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.19ºBPM.3ªCIA	Praça Jordão Baixo, S/N	Jordão Baixo	Recife	LAP 1	-8,137654	-34,94044
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.13ºBPM.1ªCIA	Rua Fonseca de Oliveira, S/N	Campo Grande	Recife	LAP 1	-8,032093	-34,886898
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.ARCOVERDE.LINK INTERNET	Rodovia Br 232, S/N	Coronel Siqueira Campos	Arcoverde	LAP 1	-8,417644	-37,058521
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CSM/INT	Rua Coelho Leite	Santo Amaro	Recife	LAP 1	-8,049862	-34,880413
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.TUPANATINGA	Rua Travessa Padre Cicero, S/N	Centro	Tupanatinga	LAP 1	-8,754178	-37,341917
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DAS.NADEC	Rua Coronel Silva Torres, 72	Capunga	Recife	LAP 1	-8,053268	-34,90291
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ºBPM.3ªCIA.EXU	Rua Coronel Ulisses, 102	Centro	Exu	LAP 1	-7,511906	-39,722664
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ªCIPM	Rua Ver Jose Moraes Irmão, 340	Malaquias	Santa Cruz do Capibaribe	LAP 1	-7,954756	-36,196684
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.RPMON.GARANHUNS	Av. José Leitão, S/N	Boa Vista	Garanhuns	LAP 1	-8,898486	-36,493797
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ªCIPM.CARAIBEIRAS	Rua JOSE ANTONIO DA SILVA, S/N	Centro	Tacaratu	LAP 1	-9,101482	-38,070286
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ºBPM.PELOTÃO.POÇÃO	Av. Manoel Vieira de Melo, S/N	Centro	Poção	LAP 1	-8,18394	-36,706858
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.24ºBPM.3ªCIA	Cidade Fazenda Nova, S/N	Centro	Brejo da Madre de Deus	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ºBPM.2ªCIA.IPUBI	Rua José Batista, S/N	Centro	Ipubi	LAP 1	-7,655525	-40,153306
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BEPI	Rua José Thomas, 800	Centro	Custódia	LAP 1	-8,091826	-37,649758
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DPM.BREJÃO	Travessa Siqueira Campos, 179	Centro	Brejão	LAP 1	-9,026239	-36,565619
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.2ªCIA	Rua MARIO DOMINGUES, S/N	Centro	Ribeirão	LAP 1	-8,521755	-35,376501
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.19ºBPM.2ªCIA	Av. Jose Ferreira Lins, S/N	Imbiribeira	Recife	LAP 1	-8,094625	-34,9134
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ªCIPM	Rua Dr Oscar Sampalo, S/N	Centro	Santa Maria da Boa Vista	LAP 1	-8,799797	-39,821742
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.NAZARÉ DA MATA	Av. Tiradentes S/N	Centro	Nazaré da Mata	LAP 1	-7,748122	-35,230734
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.20ºBPM.DESTACAMENTO.MATRIZ DA LUZ	Rua Doutor Pedro Correia, S/N		São Lourenço da Mata	LAP 1	-7,994793	-35,036758
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DESTACAMENTO.PARANATAMA	Rua Luiz Roldão, S/N	Centro	Paranatama	LAP 1	-8,91796	-36,656394
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ºBPM.SERRA TALHADA	Qd Dois, S/N	Cohab	Serra Talhada	LAP 1	-7,975125	-38,287285
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.22ºBPM.SURUBIM	Rua Euclides José da Silva, S/N	Cabaceira	Surubim	LAP 1	-7,83997179	-35,75618074
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.DESTACAMENTO.CORTÊS	Rua Arthur Siqueira, 108	Centro	Cortês	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CFAP.CURADO.TELECENTRO	Br-232, Km 8, S/N	Curado IV	Jaboatão dos Guararapes	LAP 1	-8,085029	-35,000376
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.SOLIDÃO	Rua Nossa Senhora Aparecida, S/N	Centro	Solidão	LAP 1	-7,600824	-37,648236

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.2ªCIA	Rua João Pessoa, 168	Centro	Lajedo	LAP 1	-8,663667	-36,324571
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.22ºBPM.3ªCIA	Av. Castelo Branco, S/N	Centro	Bom Jardim	LAP 1	-7,790901	-35,595361
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.TUPARETAMA	Rua Bom Jesus, S/N	Centro	Tuparetama	LAP 1	-7,601762	-37,310724
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.18ºBPM.NSC.IPOJUCA	Cristovão José Da Silva, S/N	Centro	Ipojuca	LAP 1	-8,399643	-35,061231
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPRV.POSTO04.ITAMARACA	PE-045 KM09	ILHA DE ITAMARACA	Ilha de Itamaracá	LAP 1	-7,773109	-34,880343
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.19ºBPM.NSC.BOA VIAGEM	Av. Boa Viagem - s/n	Pina	Recife	LAP 1	-8,133065	-34,900235
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.BUÍQUE	Rua Jonas Camelo, S/N	Centro	Buíque	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ºBPM.3ªCIA.MOREILÂNDIA	Rua 15 De Novembro, S/N	Centro	Moreilândia	LAP 1	-7,630283	-39,549738
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.3ªCIA	Praça JOSÉ NICOLAU, 51	Centro	Barreiros	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.3ªCIA	Praça JOSÉ NICOLAU, 51	Centro	Barreiros	LAP 1	-8,815851	-35,195578
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.AFRÂNIO.SEDE	Avenida Cardoso de Sá, S/N	Cidade Universitária	Petrolina	LAP 1	-9,384205	-40,483849
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.26ºBPM.NSC.CRUIZ DE REBOUÇAS	Rodovia Br 101 Norte, S/N		Igarassu	LAP 1	-7,855729	-34,909912
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.20ºBPM.2ªCIA	AVENIDA DOUTOR PEDRO CORREIA DE ARAÚJO	CHÃ DA TAUBA	Camaragibe	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPRP	Rua Dom Bosco, Nº 1002	Boa Vista	Recife	LAP 1	-8,057146	-34,894671
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.ARCOVERDE	Rodovia Br 232, S/N	cel. siqueira campos	Arcoverde	LAP 1	-8,408888	-37,088857
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.26ºBPM.NSC.ITAPISSUMA	Av. João Pessoa, 198	Centro	Itapissuma	LAP 1	-7,773339	-34,893752
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ºBPM.2ªCIA	Av. Euclides De Carvalho, S/N	Centro	São José do Belmonte	LAP 1	-7,874171	-38,753549
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.21ºBPM.2ªCIA	Rua Dr. João Manoel Pontual, 220	Centro	Escada	LAP 1	-8,363867	-35,23474
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ªCIPM.BELÉM DO SÃO FRANCISCO	BR 316, KM 262, S/N	Ipsep	Belém de São Francisco	LAP 1	-8,754694	-38,96301
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CFAP.CURADO	Rodovia Br 232, Km 8, S/N	Curado I	Recife	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ªCIPM	Praça Cel Solonio Soares Melo, S/N	Centro	Cabrobó	LAP 1	-8,510133	-39,311849
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPCHOQUE	Rua Benficia, S/N	Madalena	Recife	LAP 1	-8,058155	-34,905377
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPGD	Praça Da República, S/N	Santo Antônio	Recife	LAP 1	-8,060467	-34,877215
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.24ºBPM.TAQUARITINGA DO NORTE	Rua Tenente Xavier, S/N	Centro	Taquaritinga do Norte	LAP 1	-7,8972	-36,049293
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.3ªCIA	Rua JOÃO GALINDO, 301	Centro	Bonito	LAP 1	-8,46663805	35,73321753
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.21ºBPM.DESTACAMENTO.GLÓRIA DO GOITÁ	Travessa Santos Paes S/N	Centro	Glória do Goitá	LAP 1	-8,000951	-35,291196
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.HOTEL DE TRÂNSITO	Av. Carlos De Lima Cavalceti,	Rio Doce	Olinda	LAP 1	-7,982496	-34,837521
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.DESTACAMENTO.SÃO BENEDITO DO SUL	Rua Dr. José Mariano, S/N	Centro	São Benedito do Sul	LAP 1	-8,806597	-35,931904

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.22ºBPM.JOÃO.ALFREDO	Rua Dr. José Pontual, 6	Raul Soares	João Alfredo	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ºBPM.3ªCIA	Rua Ceará, S/N	Jardim Brasil II	Olinda	LAP 1	-8,007517	-34,869762
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.16ºBPM	Av. Cais De Santa Rita	Santo Antônio	Recife	LAP 1	-8,071556	-34,878176
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºCIPM	Av. Djalma Wanderley, S/N	Centro	Petrolândia	LAP 1	-8,980563	-38,215764
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.DESTACAMENTO.IBIRAJUBA	Av. Tenente Xavier de Araújo	Centro	Ibirajuba	LAP 1	-8,57946	-36,178089
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.QUIXABA	Rua Antonio Salvador de Araújo, 88	Centro	Parnamirim	LAP 1	-7,720285	-37,850528
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ºBPM.3ªCIA	Av. Frei Fernando, S/N	Liberdade	Triunfo	LAP 1	-7,831764	-38,103615
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.6ºBPM.NSC.MURIBECA	Rua Dois Lote 02, S/N	Muribeca	Jaboatão dos Guararapes	LAP 1	-8,158106	-34,956627
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.SANTA TEREZINHA	Rua Silvino Leite, 261	Centro	Santa Terezinha	LAP 1	-7,37762725	-37,47797243
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ºBPM	Br 232 - Km 180 S/N	Floresta	Belo Jardim	LAP 1	-8,309928	-36,027232
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.3ªCIA.GOIANA	Praça Alvorada	Centro	Goiânia	LAP 1	-7,563015	-35,013143
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.6ºCIPM.LIMOEIRO	Av. Jerônimo Heráclito, 1947	Centro	Limoeiro	LAP 1	-7,8655	-35,432981
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.DPM.MARAIAL	Rua Manoel Nunes Viana, 118	Centro	Maraial	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.11ºCIPM.POSTO.JUPI	Rua José Correia Lima, 58	Centro	Jupi	LAP 1	-8,709997	-36,416197
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.20ºBPM.3ªCIA	Av. Pedro Augusto Correia de Araújo, S/N -	Centro - ao lado do Corpo de Bombeiros e Escola Técnica Estadual	São Lourenço da Mata	LAP 1	-7,99376	-35,039247
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.20ºBPM	Rua 01 S/N	Muribara	São Lourenço da Mata	LAP 1	-8,007887	-35,040464
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºCIPM	Rua 4 de Outubro, 460	Centro	Gravatá	LAP 1	-8,206216	-35,583346
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.22ºBPM.CADEIA.SANTA MARIA DO CAMBUCÁ	Rua Dr. Miguel Bras - s/n, Centro, Santa Maria do Cambucá - PE. CEP: 55.765-000	Centro	Santa Maria do Cambucá	LAP 1	-7,83333	-35,880903
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPTRAN	Rua Arsênio Calaça, Nº 600	San Martin	Recife	LAP 1	-8,069281	-34,930773
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIPMOTO	Travessa Gaspar, S/N	São José	Recife	LAP 1	-8,075457	-34,896178
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.3ªCIA.CEDRO	Rua Francisco Sampaio, S/N	Centro	Cedro	LAP 1	-7,72130827	-39,2338698
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºBPM.DESTACAMENTO.CATENDE	Rua Vereador Joáe Orlando Carneval, 4	Centro	Catende	LAP 1	-8,672443	-35,730075
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.DPM.PETROLINA	Av. Cardoso de Sa, S/N	Vila Eduardo	Petrolina	LAP 1	-9,39173479	-40,48011504
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ºBPM.2ªCIA	Av. Boa Vista, 777	Centro	Cachoeirinha	LAP 1	-8,490696	-36,237792
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.3ªCIA.CONDADO	Av. 15 de Novembro, S/N	Centro	Condado	LAP 1	-7,587588	-35,098045
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CREED	Rodovia Pe 18, Km 06	Caetés 01	Paulista	LAP 1	-7,928616	-34,922397

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CPM.RECIFE	Rua Henrique Dias, 609	Derby	Recife	LAP 1	-8,059955	-34,899699
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBIESP	Av. Anízio Moura Leal, 290	Maria Auxiliadora	Petrolina	LAP 1	-9,381184	-40,50623
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIATUR.OLINDA.SEDE	AVENIDA SIGISMUNDO GONÇALVES, 515	VARADOURO	Olinda	LAP 1	-8,018955	-34,849806
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.SEDE.2	Av. Rui Barbosa - 1122	Heliópolis	Garanhuns	LAP 1	-8,882581	-36,478087
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.DESTACAMENTO.ANGELIM	Rua Joaquim Antônio, 48	Centro	Angelim	LAP 1	-8,889334	-36,284256
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ºBPM.PELOTÃO.ITAÍBA	Rua Ulisses Guimarães, S/N	Centro	Itaíba	LAP 1	-8,946321	-37,423065
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.19ºBPM	Av. Doutor Dirceu Veloso Tavares de Brito, S/N	Pina	Recife	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.2ªCIA.PESQUEIRA	Rua Gumercindo Saraiva Duque, S/N	Prado	Pesqueira	LAP 1	-8,35796	-36,68616
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.1ªCIA	Rua Henrique Dias, 51	Centro	Afogados da Ingazeira	LAP 1	-7,751439	-37,639961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ªCIPM.DESTACAMENTO.SANHARÓ	Rua João Alves Leite, 41	Centro	Sanharó	LAP 1	-8,360921	-36,56321
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.GUARDA PATROMONIAL	Rua De São João, 504	São José	Recife	LAP 1	-8,069192	-34,883431
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.INGAZEIRA	Rua Coronel Francisco Miguel Vera, 72	Centro	Ingazeira	LAP 1	-7,75449052	-37,62989835
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.PELOTÃO.ITAPETIM	Rua Olinda, S/N	São José	Itapetim	LAP 1	-7,379253	-37,189334
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ªCIPM.SERINHAÉM	Rua Marques de Olinda, S/N	Centro	Sirinhaém	LAP 1	-8,59517373	-35,11101926
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.25ºBPM.PELOTÃO.CUMARU	Rua Eulampio T. da Silva, 29	Alto do Cruzeiro	Cumaru	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM	Av. Rui Barbosa, 1122	Heliópolis	Garanhuns	LAP 1	-8,882533	-36,478075
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.25ºBPM.2ªCIA	Avenida General Manoel Rabelo - S/N	Sucupira	Jaboatão dos Guararapes	LAP 1	-8,104582	-34,975616
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.6ºBPM.4ªCIA	Rua Arthur Mendonça - 236	Bela Vista	Moreno	LAP 1	-8,119353	-35,104186
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.23ºBPM.2ªCIA	Rua Genesis Marcena Veras, 175	Centro	Tabira	LAP 1	-7,5884	-37,536883
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.SISMEPE	RUA CEL. SILVA TORRES, Nº 33	DERBY	Recife	LAP 1	-8,053453	-34,902479
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.18ºBPM	Rua Marechal Dantas Barreto, 205		Cabo de Santo Agostinho	LAP 1	-8,29007	-35,040946
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.21ºBPM	Rodovia Pe-45, Km 02, S/N	Centro	Vitória de Santo Antão	LAP 1	-8,123743	-35,282119
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ªCIPM	Praça MARIA DA SILVA MODESTO, S/N	Vila Santa isabel	Arapirina	LAP 1	-7,57656	-40,497632
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM	BR 104 - Km 67, S/N		Caruaru	LAP 1	-8,23953	-35,980598
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.QCG	Praça Do Derby, S/N	Derby	Recife	LAP 2	-8,056758	-34,899534
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ºBPM.PELOTÃO.VERDEJANTE	Rua Manoel Alves Ribeiro, S/N	Centro	Verdejante	LAP 1	-7,927285	-38,969644
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.5ªCIA	Rua 11 De Setembro, S/N	Centro	Agrestina	LAP 1	-8,452638	-35,946943

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.17ºBPM.NSC.ABREU E LIMA	Av. Duque de Caxias, S/N	Centro	Abreu e Lima	LAP 1	-7,912291	-34,900115
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ºBIESP	Av. Assunção, 46	Caiuca	Caruaru	LAP 1	-8,286859	-35,989586
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BOPE	Av. central, 3171	Areias	Recife	LAP 1	-8,086329	-34,941785
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CFAP.ANEXO.IMBIRIBEIRA	AVENIDA MARECHAL MASCARENHAS DE MORAIS	Imbiribeira	Recife	LAP 2		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CTT.LINK-PRINCIPAL	Rua Arsênio Calaça, 600	San Martin	Recife	LAP 1	-8,069281	-34,930773
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.SÃO VICENTE FÉRRER	Praça Pereira Guedes, 0, - Centro, São Vicente Férrer	Centro	São Vicente Férrer	LAP 1	-7,591173	-35,48707
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIPCÂES	Av. Hidelbrando De Vasconcelos S/N	Dois Unidos	Recife	LAP 1	-7,996076	-34,909248
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.10ºCIPM.DPM.TAMANDARÉ	Rua Cleto Campelo, 42	Centro	Tamandaré	LAP 1	-8,75756524	-35,10512466
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.18ºBPM.2ªCIA	Rua Prefeito Diomedes Ferreira de Melo, S/N	Ponte Dos Carvalhos	Cabo de Santo Agostinho	LAP 1	-8,24016	-34,981293
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºEMG.NISC.CARUARU	Rua Doutor Jose Rafael Cavalcante, 100	Pinheirópolis	Caruaru	LAP 1	-8,293192	-35,98379
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CEFD	Rua Coronel Silva Torres - s/n	Derby	Recife	LAP 1	-8,053363	-34,903039
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.26ºBPM.3ªCIA	Av. João Pessoa Guerra, S/N	Centro	Ilha de Itamaracá	LAP 1	-7,759793	-34,828458
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DAS.SEDE	Rua Monsenhor Ambrozino Leite, 155	Graças	Recife	LAP 1	-8,05212	-34,900971
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.NSC.PETROLINA	Avenida Cardoso de Sá - s/n	Vila Eduardo	Petrolina	LAP 1	-9,402408	-40,500839
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.18ºBPM.2ªSeção	Onildo Marinho Espindola, S/N	Vila Social	Cabo de Santo Agostinho	LAP 1	-8,04756	-34,876961
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.DESTACAMENTO.CAMUTANGA	Av. GETULIO VARGAS, 460	Centro	Camutanga	LAP 1	-7,408984	-35,273653
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ºBPM.PELOTÃO.BARRA DE GUABIRABA	Av. Eudes Teixeira de Carvalho, 155	Centro	Barra de Guabiraba	LAP 1	-8,417075	-35,663213
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.APMP.LINK-PRINCIPAL	Br 408, Km 76, S/N	Chã de Capoeira	Paudalho	LAP 1	-7,892981	-35,173718
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.DASIS	Rua Betania, S/N	Derby	Recife	LAP 1	-8,055016	-34,902455
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.APMP.LINK-SECUNDÁRIO	Br-408, Km 76, S/N	Chã de Capoeira	Paudalho	LAP 1	-7,892983	-35,173712
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.25ºBPM.SEDE	RUA PADRE CHROMACIO LEÃO, N 14	CENTRO	Jaboatão dos Guararapes	LAP 1	-8,11153	-35,018413
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ºBPM.PELOTÃO.TRACUNHAÉM	Rua Joao Martins Pessoa, S/N	Centro	Tracunhaém	LAP 1	-7,798246	-35,218295
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.5ºBPM.PELOTÃO.DORMENTES	Av. Jose Coelho de Macedo, S/N	Centro	Dormentes	LAP 1	-8,450034	-40,767866
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ºBPM.PELOTÃO.ÁGUAS BELAS	Rua Santa Cruz, S/N	Centro	Águas Belas	LAP 1	-9,11157461	-37,12061733
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.6ºCIPM.SALGADINHO	Rua João Vicente da Silva, S/N	Centro	Salgadinho	LAP 1	-7,94072742	-35,63050315
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.CIPOMA.DESTACAMENTO.FERNANDO DE NORONHA	Praça Centro de Convivencia, S/N	Centro	Fernando de Noronha	LAP 1	-3,8467	-32,406412

POLÍCIA MILITAR DE PERNAMBUCO	PMPE.8ªCIPM.POSTO.ALAGOINHA	Rua Coronel Antônio Pinojosa, S/N	Centro	Alagoinha	LAP 1	-8,466351	-36,774192
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ªCIPM.PELOTÃO.ITAPARICA	Rua Xavantes, S/N	Boa vista	Jatobá	LAP 1	-9,174618	-38,251013
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.1ªBPM	Av Governador Carlos De Lima Cavalcante, 5075	Casa Caiada	Olinda	LAP 1	-7,958661	-34,831015
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.9ªBPM.PELOTÃO.CANHOTINHO	Rua Drº Afonso Pena, 183	Centro	Canhotinho	LAP 1	-8,881996	-36,190416
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.2ªBPM.DESTACAMENTO.FERREIROS	Rua São Vicente de Paula, 25	Centro	Ferreiros	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.3ªCIPM.ITAMBÉ	Rua Juiz Roberto Guimarães, 109	Centro	Itambé	LAP 1	-7,407001	-35,113365
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.14ªBPM. 2ª PEL. Betânia	Praça Pedro Feitosa, S/N	Centro	Betânia	LAP 1		
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ªBPM.COPOM	RODOVIA BR 104 KM67, S/N	Agamenon magalhães	Caruaru	LAP 1	-8,28546228	-35,96697567
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.7ªBPM.1ªCIA.SANTA FILOMENA	Rua João Coelho da Luz, S/N	Centro	Santa Filomena	LAP 1	-8,161009	-40,613769
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.15ªBPM.PELOTÃO.SÃO BENTO DO UNA	Rua Abílio Veloso Braga, 509	Centro	São Bento do Una	LAP 1	-8,525644	-36,442365
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.BPRV	Rua Quinze De Marco, S/N	San Martim	Recife	LAP 1	-8,065267	-34,931411
POLÍCIA MILITAR DE PERNAMBUCO	PMPE.4ªBPM.4ªCIA	Av. Francisca Lemos, S/N	São Pedro	Bezerros	LAP 1	-8,237751	-35,748486
PORTO DO RECIFE S/A	Porto Recife - Sede	Praça Comunidade Luso-Brasileira, Nº 70	Bairro Do Recife	Recife	LAP 2	-8,0541	-34,870899
PROCURADORIA GERAL DE JUSTIÇA	PGJ - Edif. Roberto Lyra	Rua Imperador Dom Pedro II, 473	Santo Antônio	Recife	LAP 1		
PROCURADORIA GERAL DE JUSTIÇA	Promotoria de Justiça de Cortês	Rodovia PE 85, S/N - KM 26, Cortês - PE, 55525000		Recife	LAP 1		
PROCURADORIA GERAL DE JUSTIÇA	Promotoria de Justiça de Jurema	Praça da Bandeira, S/N	Centro	Jurema	LAP 1	-8,718998	-36,137121
PROCURADORIA GERAL DO ESTADO	PGE - Arcoverde	Rua Júlio Tavares de Lima, 185	Sucupira	Arcoverde	LAP 1	-8,425333	-37,057922
PROCURADORIA GERAL DO ESTADO	PGE - Sede	Rua Do Sol, 143	Santo Antônio	Recife	LAP 2	-8,06112689	-34,87983007
PROCURADORIA GERAL DO ESTADO	PGE - Sede	Rua Do Sol, 143	Santo Antônio	Recife	LAP 2	-8,06112689	-34,87983007
PROCURADORIA GERAL DO ESTADO	PGE - Sede	Rua Do Sol, 143	Santo Antônio	Recife	LAP 2	-8,06112689	-34,87983007
PROCURADORIA GERAL DO ESTADO	PGE - Petrolina	Rua Pacifico Da Luz, 276	Centro	Petrolina	LAP 1	-9,399811	-40,50086
PROCURADORIA GERAL DO ESTADO	PGE - Caruaru	Rua OLIVIO FERREIRA DE AZEVEDO, 135	Salgado	Caruaru	LAP 1	-8,259401	-35,967525
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Salgueiro	Rua Maria Nogueira Sampaio, 270	Centro	Salgueiro	LAP 1	-8,070246	-39,122841
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Unidade Gerencial Territorial de Petrolândia	Av. DOS TRES PODERES, 59	Centro	Petrolândia	LAP 1	-8,97934	-38,21834

PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Unidade Técnica Regional de Palmares	Sítio Flor dos Montes, Santa Rosa, S/N	Centro	Palmares	LAP 1	-8,67884	-35,583879
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Caruaru	Rua Raimundo de Morais, 18	Maurício de Nassau	Caruaru	LAP 1	-8,279469	-35,967907
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Unidade Gerencial Territorial de Afogados da Ingazeira	Rua Senador Paulo Guerra, 325	Centro	Afogados da Ingazeira	LAP 1	-7,750215	-37,636624
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Projeto Renascer - Escritório Regional de Petrolina	Av. Das Nações, S/N	Centro	Petrolina	LAP 1	-9,389533	-40,508671
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Arcoverde	Rua Dr. João Pacheco Freire Filho, 160	São Miguel	Arcoverde	LAP 1	-8,426651	-37,065086
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Projeto Renascer - Escritório Regional de Limoeiro	Rua Da Alegria, 670	Centro	Limoeiro	LAP 1	-7,872411	-35,447125
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Projeto Renascer - Sede	Av. Conde da Boa Vista Nº 1410	Boa Vista	Recife	LAP 1	-8,056231	-34,893171
PROGRAMA ESTADUAL DE APOIO AO PEQUENO PRODUTOR RURAL	ProRural - Unidade Gerencial Territorial de Ouricuri	Rua presidente Kennedy, 121	Centro	Ouricuri	LAP 1	-7,8869584	-40,0843517
PRONTO SOCORRO CARDIOLÓGICO DE PERNAMBUCO	PROCAPE - Pronto Socorro Cardiológico de Pernambuco	Rua Palmares, S/N	Santo Amaro	Recife	LAP 2	-8,051244	-34,885374
SECRETARIA DA CASA CIVIL	Gerência Geral de Gestão da Casa Civil	Rua Confederação Do Equador, 111	Graças	Recife	LAP 1	-8,048235	-34,897868
SECRETARIA DA CASA CIVIL	Casa Civil - Brasília	Setor Bancário Norte, Edifício CNC, Quadra 01, Bloco B	Asa Norte	Brasília (DF)	LAP 1		
SECRETARIA DA CASA MILITAR	CAMIL / VICE-GOVERNADORIA	Av. Rio Branco, 104	Recife Antigo	Recife	LAP 1	-8,062653	-34,87238
SECRETARIA DA CASA MILITAR	CAMIL / DSI	Av Cruz Cabuga, 1357	Santo Amaro	Recife	LAP 1	-8,043739	-34,874581
SECRETARIA DA CASA MILITAR	PALÁCIO DO CAMPO DAS PRINCESAS	Praça da República, S/N	Santo Antônio	Recife	LAP 2	-8,060966	-34,877246
SECRETARIA DA CASA MILITAR	PALÁCIO DO CAMPO DAS PRINCESAS	Praça da República, S/N	Santo Antônio	Recife	LAP 2	-8,060966	-34,877246
SECRETARIA DA CASA MILITAR	CAMIL - DAF	Av. Cruz Cabugá, 1357	Santo Amaro	Recife	LAP 2	-8,043739	-34,874581
SECRETARIA DA CONTROLADORIA GERAL DO ESTADO	Sede da Controladoria Geral do Estado	Rua Santo Elias, 535	Espinheiro	Recife	LAP 2		
SECRETARIA DA CONTROLADORIA GERAL DO ESTADO	Sede da Controladoria Geral do Estado	Rua Santo Elias, 535	Espinheiro	Recife	LAP 2		
SECRETARIA DA CRIANÇA E JUVENTUDE	SECRETARIA DA CRIANÇA E JUVENTUDE			Recife	LAP 1	-8,045915	-34,879045

SECRETARIA DA FAZENDA	SEFAZ - Are - Surubim	Av. Agamenom Magalhães, 283	Centro	Surubim	LAP 1	-7,838794	-35,759684
SECRETARIA DA FAZENDA	SEFAZ - Are - Cabo	Rua Historiador Pereira da Costa, S/N	Centro	Cabo de Santo Agostinho	LAP 1	-8,283242	-35,033501
SECRETARIA DA FAZENDA	SEFAZ - Are - Afogados da Ingazeira	Av. Rio Branco, 62	Centro	Afogados da Ingazeira	LAP 1	-7,748618	-37,638208
SECRETARIA DA FAZENDA	Posto Fiscal - São Caetano ( Link II )	Rodovia Br 232, Km 141, S/N	Zona Rural	São Caetano	LAP 1	-8,32120225	-36,8462728
SECRETARIA DA FAZENDA	Posto Fiscal - São Caetano ( Link II )	Rodovia Br 232, Km 141, S/N	Zona Rural	São Caetano	LAP 1	-8,04756	-34,876961
SECRETARIA DA FAZENDA	SEFAZ - 4 Drr - Departamento Secretaria da Fazenda - Petrolina	Av. Cardoso De Sá, 5	Centro	Petrolina	LAP 1	-9,400146	-40,505336
SECRETARIA DA FAZENDA	SEFAZ - 4 Drr - Departamento Secretaria da Fazenda - Petrolina	Av. Cardoso De Sá, 5	Centro	Petrolina	LAP 1	-9,400146	-40,505336
SECRETARIA DA FAZENDA	Are - Belo Jardim	Rua Padre Pedro Pais, 44	Centro	Belo Jardim	LAP 1	-8,33608231	36,42204936
SECRETARIA DA FAZENDA	Are - Santa Cruz do Capibaribe	Rua Raimundo Francelino Aragão, 27	Centro	Santa Cruz do Capibaribe	LAP 1	-7,95736	-36,211239
SECRETARIA DA FAZENDA	SEFAZ - Are - Arcoverde (Antiga 3 Drr)	Av. Coronel Antônio Japiassu, 227	Santa Luzia	Arcoverde	LAP 1	-8,420175	-37,050474
SECRETARIA DA FAZENDA	SEFAZ - San Rafael	Av. Dantas Barreto, 1186	São Jose	Recife	LAP 2		
SECRETARIA DA FAZENDA	SEFAZ - San Rafael	Av. Dantas Barreto, 1186	São Jose	Recife	LAP 2	-8,04756	-34,876961
SECRETARIA DA FAZENDA	SEFAZ Unidade Fiscal Sedex	Av. General San Martins, 1083	Bongi	Recife	LAP 1	-8,065103	-34,92717
SECRETARIA DA FAZENDA	SEFAZ - Posto Fiscal de Goiana	Rod Br 101 Norte, Km 07, S/N	Alvorada	Goiana	LAP 1		
SECRETARIA DA FAZENDA	SEFAZ - Posto Fiscal de Goiana	Rod Br 101 Norte, Km 07, S/N	Alvorada	Goiana	LAP 1	-7,502153	-34,986195
SECRETARIA DA FAZENDA	SEFAZ - DIRETORIA DE INTELIGÊNCIA FISCAL (DIF)	Rua Barão de Água Branca	Imbiribeira	Recife	LAP 2	-8,11167988	34,90641162
SECRETARIA DA FAZENDA	SEFAZ - DIRETORIA DE INTELIGÊNCIA FISCAL (DIF)	Rua Barão de Água Branca	Imbiribeira	Recife	LAP 2	-8,11167988	34,90641162
SECRETARIA DA FAZENDA	SEFAZ - Nuds 2ª Região Fiscal	Rua Treze De Maio, 49	Centro	Caruaru	LAP 1		
SECRETARIA DA FAZENDA	SEFAZ - Nuds 2ª Região Fiscal	Rua Treze De Maio, 49	Centro	Caruaru	LAP 1	-8,286751	-35,973072
SECRETARIA DA FAZENDA	SEFAZ - Are - Garanhuns	Rua Dom José, S/N	Santo Antônio	Garanhuns	LAP 1	-8,892822	-36,494922
SECRETARIA DA FAZENDA	SEFAZ - Sede	Rua Imperador S/N	Centro	Recife	LAP 2		
SECRETARIA DA FAZENDA	SEFAZ - Sede	Rua Imperador S/N	Centro	Recife	LAP 2	-8,063792	-34,876903
SECRETARIA DA FAZENDA	SEFAZ - ENCRUZILHADA	Estrada De Belem, 362	Campo Grande	Recife	LAP 1		
SECRETARIA DA FAZENDA	SEFAZ - ENCRUZILHADA	Estrada De Belem, 362	Campo Grande	Recife	LAP 1	-8,043496	-34,874262
SECRETARIA DA FAZENDA	SEFAZ - Are - Petrolândia	Av. Três Poderes, S/N	Centro	Petrolândia	LAP 1	-8,979985	-38,218283
SECRETARIA DA FAZENDA	Are - Araripina	Rua 11 De Setembro, 92	Centro	Araripina	LAP 1	-7,575116	-40,498244
SECRETARIA DA FAZENDA	Posto Fiscal Xexéu	Br 101 Sul, Km 138, S/N	Centro	Xexéu	LAP 1	-8,806712	-35,628054
SECRETARIA DA FAZENDA	Posto Fiscal Xexéu	Br 101 Sul, Km 138, S/N	Centro	Xexéu	LAP 1	-8,83816991	35,63625374

SECRETARIA DA FAZENDA	SEFAZ - Are - Cabo	Rua Historiador Pereira da Costa, S/N	Centro	Cabo de Santo Agostinho	LAP 1		
SECRETARIA DA FAZENDA	Are - Prazeres	Rua Arão Lins De Andrade, 260	Piedade	Recife	LAP 1	-8,16542	-34,916324
SECRETARIA DA FAZENDA	SEFAZ - Are - Serra Talhada	Rua Cel Cornélio Soares, 363	Nossa Sra. da Penha	Serra Talhada	LAP 1	-7,992025	-38,301775
SECRETARIA DA FAZENDA	Are - Carpina	Rua Estácio De Caimbra, 741	Centro	Carpina	LAP 1	-7,845567	-35,253715
SECRETARIA DA FAZENDA	SEFAZ - Are - Salgueiro	Av. Agamenon Magalhães, 581	Centro	Salgueiro	LAP 1	-8,071166	-39,11979
SECRETARIA DA FAZENDA	Posto Fiscal Suape	Av. Portuária, S/N	Suape	Ipojuca	LAP 1	-8,39296	-34,97127
SECRETARIA DA FAZENDA	SEFAZ - Are - Vitória	Rua : Ambrósio Machado, S/N	Centro	Vitória de Santo Antão	LAP 1	-8,119716	-35,296892
SECRETARIA DA FAZENDA	Are - Centro - Sna	Rua Imperial, 2077	São José	Recife	LAP 2	-8,078186	-34,899917
SECRETARIA DA FAZENDA	Are - Centro - Sna	Rua Imperial, 2077	São José	Recife	LAP 1	-8,07803894	-34,900005
SECRETARIA DA FAZENDA	SEFAZ - Sumap	Avenida Getúlio Vargas, BR 232, KM 12 - 7316	Curado	Recife	LAP 1	-8,073544	-34,963786
SECRETARIA DA FAZENDA	Ceag - Arquivo Geral	Rua São João, 504	São Jose	Recife	LAP 1	-8,06887384	-34,8838647
SECRETARIA DA FAZENDA	SEFAZ - Detran Gpc Ipva	Estrada Do Barbalho, 889	Ipatinga	Recife	LAP 1	-8,04756	-34,876961
SECRETARIA DA FAZENDA	SEFAZ - Detran Gpc Ipva	Estrada Do Barbalho, 889	Ipatinga	Recife	LAP 1		
SECRETARIA DA FAZENDA	SEFAZ - CRUZ CABUGÁ	AVENIDA CRUZ CABUGÁ - 1419	SANTO AMARO	Recife	LAP 1	-8,043481	-34,87425
SECRETARIA DA FAZENDA	SEFAZ - CRUZ CABUGÁ	AVENIDA CRUZ CABUGÁ - 1419	SANTO AMARO	Recife	LAP 1	-8,0432636	-34,8742252
SECRETARIA DA FAZENDA	SEFAZ - Are - Ouricuri	Rua Coronel Anísio Coelho, 105	Centro	Ouricuri	LAP 1	-7,885054	-40,081549
SECRETARIA DA MULHER	Secretaria da Mulher - Salgueiro	Rua Amácio Orácio, 830	Nossa Senhora das Graças	Salgueiro	LAP 1	-8,068563	-39,126634
SECRETARIA DA MULHER	Secretaria da Mulher - Sede	Avenida Rio Branco - 50	Recife Antigo	Recife	LAP 1	-8,062832	-34,872676
SECRETARIA DA MULHER	Secretaria da Mulher - Sede	Avenida Rio Branco - 50	Recife Antigo	Recife	LAP 2		
SECRETARIA DA MULHER	Centro de Aceleração do Desenvolvimento da Mulher Metropolitana - Recife	Rua Carapeba, S/N	Jardim Brasília Teimosa	Recife	LAP 1	-8,084701	-34,88165
SECRETARIA DA MULHER	Secretaria da Mulher - Cabo de Santo Agostinho	Av. Almirante Paulo Moreira, S/N	Cidade Garapu	Cabo de Santo Agostinho	LAP 1	-8,285922	-35,020651
SECRETARIA DA MULHER	Secretaria da Mulher - Petrolina	Rua Cabrobó, S/N	Vila Eduardo	Petrolina	LAP 1	-9,388062	-40,486286
SECRETARIA DA MULHER	Secretaria da Mulher - CEDIM	Rua Alfredo Lisboa, 188	Centro	Recife	LAP 1	-8,04756	-34,876961
SECRETARIA DE ADMINISTRAÇÃO	GGPAE / ARPE	Conselheiro Rosa e Silva	Aflitos	Recife	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO	GGPAE / ARPE	Conselheiro Rosa e Silva	Aflitos	Recife	LAP 1	-8,042869	-34,897729
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Petrolina	Av. Monsenhor Ângelo Sampaio, 100	Centro	Petrolina	LAP 1	-9,393957	-40,492781
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Petrolina	Av. Monsenhor Ângelo Sampaio, 100	Centro	Petrolina	LAP 1	-9,393957	-40,492781
SECRETARIA DE ADMINISTRAÇÃO	CEFOSPE	Rua Tabira S/N	Boa Vista	Recife	LAP 2	-8,050642	-34,891455
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão de Salgueiro	Av. Antônio Angelim, 570	Santo Antônio	Salgueiro	LAP 1	-8,072433	-39,124081

SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão de Salgueiro	Av. Antônio Angelim, 570	Santo Antônio	Salgueiro	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Boa Vista	Av. C. da Boa vista, S/N	Boa Vista	Recife	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Boa Vista	Av. C. da Boa vista, S/N	Boa Vista	Recife	LAP 1	-8,058409	-34,88833
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão Caruaru	Av. Adjar da Silva Casé, 87	Indianópolis	Caruaru	LAP 1	-8,292279	-35,949892
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão Caruaru	Av. Adjar da Silva Casé, 87	Indianópolis	Caruaru	LAP 1	-8,292226	-35,955856
SECRETARIA DE ADMINISTRAÇÃO	SAD / Pina	Rua Antônio de Goes, Nº 194	Pina	Recife	LAP 2		
SECRETARIA DE ADMINISTRAÇÃO	SAD / Pina	Rua Antônio de Goes, Nº 194	Pina	Recife	LAP 2	-8,088955	-34,882914
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão - Carpina	PE-041 KM 02	BAIRRO NOVO	Carpina	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão - Shopping Rio Mar	Av. Republica Do Libanom 251	Pina	Recife	LAP 1	-8,08617465	-34,89412247
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão - Shopping Rio Mar	Av. Republica Do Libanom 251	Pina	Recife	LAP 1	-8,086358	-34,894061
SECRETARIA DE ADMINISTRAÇÃO	SAD / Pina (Rede Sem Fio)	Rua Antônio de Goes, Nº 194	Pina	Recife	LAP 1	-8,088955	-34,882914
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Olinda	Rua do Quartel, S/N	Casa Caiada	Olinda	LAP 1	-7,993478	-34,840287
SECRETARIA DE ADMINISTRAÇÃO	SAD - Expresso Cidadão - Olinda	Rua do Quartel, S/N	Casa Caiada	Olinda	LAP 1	-7,993815	-34,840265
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão Garanhuns	Av. Lions, 305	Centro	Garanhuns	LAP 1	-8,89592	-36,500076
SECRETARIA DE ADMINISTRAÇÃO	Expresso Cidadão Garanhuns	Av. Lions, 305	Centro	Garanhuns	LAP 2	-8,89592	-36,500076
SECRETARIA DE ADMINISTRAÇÃO	SAD - Vitória de Santo Antão	Henrique de Holanda, S/N	Redenção	Vitória de Santo Antão	LAP 1	-8,04756	-34,876961
SECRETARIA DE ADMINISTRAÇÃO	SAD - Vitória de Santo Antão	Henrique de Holanda, S/N	Redenção	Vitória de Santo Antão	LAP 1	-8,11307	-35,286972
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Petrolândia	Av. Barreiras, Quadra 13, S/N	Centro	Petrolândia	LAP 1	-8,97435488	-38,22392902
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Bom Conselho	Rua Carlos Dias, S/N	Centro	Bom Conselho	LAP 1	-9,1725915	-36,68761848
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	CIR ITAQUITINGA	Rua Itaquitinga, Centro	Centro	Itaquitinga	LAP 1	-7,664765	-35,100867
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Cadeia Pública - Ibimirim	Rodovia Br 110, S/N	Centro	Ibimirim	LAP 1	-8,51993654	-37,68149686
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Serra Talhada	Av. Vicente Inácio Oliveira, S/N	Bom Jesus	Serra Talhada	LAP 1	-7,984475	-38,301029
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - PPAB 2 - Presídio Frei Damião de Bozano (PFDB)	Av. Liberdade, S/N	Sancho	Recife	LAP 2	-8,081969	-34,961443
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - PPAB 2 - Presídio Frei Damião de Bozano (PFDB)	Av. Liberdade, S/N	Sancho	Recife	LAP 1	-8,081969	-34,961443

SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Afranio	Rodovia Br-407, Km-112, S/N	Cohab	Afrânio	LAP 1	-8,590089	-40,996647
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	CADEIA PUBLICA DE SANTA CRUZ DO CAPIBARIBE	Rua Cesário Aragão, 226	Santa tereza	Santa Cruz do Capibaribe	LAP 1	-7,950863	-36,213955
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Presídio de Itaquitanga II	Engenho Itapirema do Meio	Itaquitanga	Itaquitanga	LAP 1	-7,710491	-35,035349
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Pedra	Rua Jorge Albuquerque Neiva, S/N	Centro	Pedra	LAP 1	-8,50007	-36,94826
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presidio Rorinildo da Rocha Leão - Palmares - Prri	Av. José Américo De Miranda, S/N	Centro	Palmares	LAP 1	-8,680326	-35,583103
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Escola Penitenciária de Pernambuco - EPPE/Itaquitanga	Rua Itaquitanga, 11	Engenho Itapirema do Meio	Itaquitanga	LAP 1	-7,664765	-35,100867
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Moreilândia	Rua 15 de Novembro, S/N	Centro	Moreilândia	LAP 1	-7,630283	-39,549738
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Presídio de Tacaimbó	BR 232 KM 166, S/N	Fazenda Água Branca	Tacaimbó	LAP 1	-8,316678	-36,291637
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Belem Sao Francisco	Av. Coronel Caribe, S/N	Centro	Belém de São Francisco	LAP 1	-8,75447244	-38,96228247
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Centro de Ressocialização do Agreste - Cra Canhotinho	Fazenda Nascimento, S/N	Centro	Canhotinho	LAP 1	-8,892097	-36,197755
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Penitenciária Juiz Plácido de Souza - Pjps	Av. Espírito Santo, 39	Vassoural	Caruaru	LAP 1	-8,300613	-35,966958
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Vicência	Rua Professora Santinha Lombo, S/N	Centro	Vicência	LAP 1	-7,653785	-35,319249
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Glória do Goitá	Rua Do Matadouro, S/N	Centro	Glória do Goitá	LAP 1	-8,058908	-35,387949
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Escada	Av. São José, S/N	Nova Descoberta	Escada	LAP 1	-8,358548	-35,236757
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES Cadeia Pública de Petrolina	Av. Pacifico da Luz, S/N	Centro	Petrolina	LAP 1	-9,397006	-40,500823

SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES Cadeia Pública de Tuparetama	Av. Carlos Caribé, S/N	Vila Bom Jesus	Tuparetama	LAP 1	-7,608467	-37,314893
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Secretaria Cidad Política Social - Colônia Penal Feminina (Bom Pastor)	Rua Do Bom Pastor, 1407	Engenho do Meio	Recife	LAP 1	-8,04931239	-34,93906219
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Agrestina	Rua Cecílio Farias, 70	Centro	Agrestina	LAP 1	-8,449294	-35,950762
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Secretaria Cidad Política Social - Ct Classificação Triagem - Cotel	Av. Hugo Hering, S/N	Caetés II	Abreu e Lima	LAP 2	-8,775702	-36,624119
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Carnaíba	Rua Santa Luiza, S/N	Caixa D'água	Carnaíba	LAP 1	-7,80583201	-37,79404091
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Riacho Das Almas	Rua José Felismino, S/N	Centro	Riacho das Almas	LAP 1	-8,13218821	-35,86014836
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES-Cad Pública de Timbaúba	Rua Almirante Barroso, S/N	Três Cocos	Timbaúba	LAP 1	-7,507393	-35,315868
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública - São José do Egito	Av. Marechal Rodon, S/N	Centro	São José do Egito	LAP 1	-7,474771	-37,275905
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Venturosa	Rodovia Br 424 Km26, S/N	Centro	Venturosa	LAP 1	-8,57649	-36,874877
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Grp I	Av. Espírito Santo, 39	Vassoral	Caruaru	LAP 1	-8,300185	-35,965862
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Sao Joaquim do Monte	Rua Joao Cabral de Andrade, S/N	Centro	São Joaquim do Monte	LAP 1	-8,43152579	-35,80732711
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES Grpii	Rua HILDA PACHECO MAGALHÃES, S/N	Vila do Presídio	Arcoverde	LAP 1	-8,400064	-37,069996
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Industrial São João	Engenho São João, S/N	Centro	Ilha de Itamaracá	LAP 1	-7,768308	-34,87087
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Araripina	Av. Governador Muniz Falcão, S/N	Centro	Araripina	LAP 1	-7,5150965	-40,50264612
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presídio de Salgueiro - Psa Link2	Loteamento São José, S/N, Br 232, Km 418.	Nossa Sra. De Graças	Salgueiro	LAP 1	-8,221347	-35,749219

SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Penitenciária Desembargador Aug. Duque	Loteamento Portal de Pesqueira, S/N	Prado	Pesqueira	LAP 1	-8,366854	-36,684277
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presídio de Limoeiro - Pdepg	Sítio Arrombado De Quebra-jejum, Pe 90 - Km 23, S/N	Vila dos Coveiros	Limoeiro	LAP 1	-7,858651	-35,450981
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Lagoa do Carro	Rua Projetada, S/N	Centro	Lagoa do Carro	LAP 1	-7,845865	-35,315995
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - PPAB 1 - Presídio Asp. Marcelo Francisco de Araujo (PAMFA)	Av. Liberdade, S/N	Sancho	Recife	LAP 1	-8,081969	-34,961443
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Centro de Saúde Penitenciário	Av. Rinaldo Pinho Alves, S/N	Caetés II	Ilha de Itamaracá	LAP 1	-7,92771635	-34,92455652
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Gae - Gerência de Arquitetura e Engenharia (Escola Penitenciária)	Rua do Hospício Nº751	Boa Vista	Recife	LAP 2	-8,05800286	-34,88313453
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia de Exú	Rua Otacilio P. de Carvalho, S/N	Centro	Exu	LAP 1	-7,516979	-39,719288
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Gravata	Rua 4 de Outubro, S/N	Centro	Gravatá	LAP 1	-8,209093	-35,593942
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Grpili	Rua Otavio Leitinho, S/N	Centro	Salgueiro	LAP 1	-8,072888	-39,120339
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presídio Policial Penal Leonardo Lagos (PPPLL)	Av. Liberdade, S/N	Sancho	Recife	LAP 1	-8,0819687	-34,9614431
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Goiana	Rua Barro Vermelho, S/N	Centro	Goiana	LAP 1	-7,571094	-35,000118
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Carpina	Rua Tiradentes, S/N	Centro	Carpina	LAP 1	-7,850137	-35,251115
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Tabira	Bairro João Cordeiro, S/N	João Cordeiro	Tabira	LAP 1	-7,592507	-37,540358
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Colonia Penal Feminina de Caetés - Cpfal	Av. Rinaldo Pinho Alves, 50	Centro	Abreu e Lima	LAP 1	-7,92769	-34,92484
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Recife	Rua Gervázio Pirez, 850	Santo amaro	Recife	LAP 1	-8,055584	-34,883722

SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Sao José Belmonte	Av. Euclides de Carvalho, S/N	Centro	São José do Belmonte	LAP 1	-7,874171	-38,753549
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Lajedo	Travessa Major Capitu, S/N	Centro	Lajedo	LAP 1	-8,654596	-36,316553
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Saloá	Av. Jose Bezerra de Lima, 223	Centro	Saloá	LAP 1	-8,975167	-36,691443
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Capoeiras	Rua Jose Prachede Das Nedes, S/N	Centro	Capoeiras	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Bezerras	Rua Imaculada Conceição, S/N	Cruzeiro	Bezerras	LAP 1	-8,226917	-35,743888
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Ipubi	Rua José Batista ,S/N	Centro	Ipubi	LAP 1	-7,655525	-40,153306
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Gameleira	Rua Antonio Luiz Regueira, S/N	Centro	Gameleira	LAP 1	-8,585505	-35,385199
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presídio Advogado Brito Alves - Paba - Arcoverde	Rua Projetada, S/N	São Cristóvão	Arcoverde	LAP 1	-8,404584	-37,061216
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Gerencia de Producao	Rodovia Pe-35, Km 12, S/N	Engenho São João	Ilha de Itamaracá	LAP 1	-7,768888	-34,870559
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Afogados Ingazeira	Travessa da Cadeia, S/N	Sobreira	Afogados da Ingazeira	LAP 1	-7,748017	-37,634663
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Secretaria Cidad Política Social - Presídio de Igarassu - Pig	Rodovia Br 101 Norte, Km 32,5	Tabatinga	Igarassu	LAP 1	-7,875293	-34,905849
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Colônia Penal Feminina - Buique - Cpfb - Link2	Av. Amelia Cavalcanti, S/N	Centro	Buique	LAP 1	-8,62738	-37,16337
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Nazare da Mata	Rua Doutor Osvaldo Cruz, S/N	Centro	Nazaré da Mata	LAP 1	-7,731569	-35,21978
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Altinho	Zona Rural, S/N	Zona Rural	Altinho	LAP 1	-8,474212	-36,060123
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia de Verdejante	Av. Antonio Pedro da Silva, S/N	Centro	Verdejante	LAP 1	-7,934048	-38,969919

SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - PPAB 3 - Presídio Juiz Antonio Luiz Lins de Barros (PJALLB)	Av. Liberdade, S/N	Sancho	Recife	LAP 1	-8,082008	-34,962971
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES Cadeia Pública Macaparana	Rua Alberto José Bezerra, S/N	Centro	Macaparana	LAP 1		
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Sede	Rua Do Hospício, 751	Boa Vista	Recife	LAP 2	-8,04756	-34,876961
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Sede	Rua Do Hospício, 751	Boa Vista	Recife	LAP 2	-8,04756	-34,876961
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Presídio de Petrolina -Pdeg	Av. Jatobá, S/N	Jatobá	Petrolina	LAP 1	-9,394022	-40,470535
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública de Flores	Rua Cleto Campelo, S/N	Centro	Flores	LAP 1	-7,864394	-37,972976
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	SERES - Cadeia Pública Garanhuns	Sítio Varzea, 309	Sítio Vázea	Garanhuns	LAP 1	-8,894454	-36,52202
SECRETARIA DE ADMINISTRAÇÃO PENITENCIÁRIA E RESSOCIALIZAÇÃO	Secretaria Cidad Política Social - Presídio Vitória S Antão - PvsA - Link 2	Rua ASP WALTER FRAGOSO, S/N	Lídia Queiroz	Vitória de Santo Antão	LAP 1	-8,125156	-35,283694
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Palmira	Av. Conde da Boa Vista, 1410	Boa Vista	Recife	LAP 2	-8,056231	-34,893171
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Comunidade Rodolfo Aureliano (CRAUR)	R. Do Bom Pastor, S/N	Iputinga	Recife	LAP 1	-8,045158	-34,939904
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Casa de Acolhimento - Madalena	Rua Dom Bosco - 1329	Boa Vista	Recife	LAP 1	-8,06329	-34,91547
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Sede	Av Cruz Cabugá, 665	Santo Amaro	Recife	LAP 2	-8,048644	-34,878151
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Sede	Av Cruz Cabugá, 665	Santo Amaro	Recife	LAP 2	-9,39284502	-40,50546043
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Casa de Acolhimento - Lar Esperança	Rua Luiz Pereira de Farias, 156	Afogados	Recife	LAP 1	-8,082291	-34,918606

SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Fundação Emocy Krause (COMCK)	RUA JOAQUIM TENORIO DA SILVA	Cavaleiro	Jaboatão dos Guararapes	LAP 1	-8,090932	-34,975097
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Edf. Palmira - Wifi	Av. Conde da Boa Vista, 1410	Boa Vista	Recife	LAP 1	-8,04756	-34,876961
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Casa de Acolhimento - Lar do Aconchego	Rua do Grito - 96	Bonsucesso	Olinda	LAP 1	-8,031222	-34,879681
SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS	SAS - Centro de Atenção à Criança - CEAC	Praça Tavares Correia, 1332	Heliópolis	Garanhuns	LAP 1	-8,87715	-36,47741
SECRETARIA DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO	Espaço Ciência	Parque Memorial Arcoverde, S/N	Complexo de Salgadinho	Recife	LAP 1	-8,027567	-34,863706
SECRETARIA DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO	Secretaria de Ciência Tecnologia e Inovação - SECTI	Rua Vital De Oliveira, 32	Centro	Recife	LAP 1	-8,060511	-34,870577
SECRETARIA DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO	PARQTEL (Parque Tecnológico de Eletroeletrônicos e Tecnologia Associada)	RUA MINISTRO MARIO ANDREAZZA, SN		Recife	LAP 1	-8,066093	-34,985799
SECRETARIA DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO	Observatório Nacional	Rua Anibal Alves Cantareli, S/N	Fazendo Serrinha	Itacuruba	LAP 1	-8,728466	-38,6838
SECRETARIA DE COMUNICAÇÃO	Secretaria Especial de Imprensa - Sede	Praça Rio Branco, 104, terreo	Recife Antigo	Recife	LAP 2		
SECRETARIA DE CULTURA	SECRETARIA DE CULTURA DO ESTADO DE PERNAMBUCO - Sede	Rua José de Alencar, 368	Boa Vista	Recife	LAP 2	-8,061812	-34,889364
SECRETARIA DE CULTURA	SECULT - Casa do Conselho	Rua Oliveira Lima	Boa Vista	Recife	LAP 1	-8,056988	-34,887949
SECRETARIA DE DEFESA SOCIAL	SDS.SEDE.LINK-PRINCIPAL	Rua São Geraldo, 111.	Santo Amaro	Recife	LAP 2	-8,05351	-34,880088
SECRETARIA DE DEFESA SOCIAL	SDS.REAPARELHAMENTO.LINK-PRINCIPAL	Avenida Presidente Dutra, 180	Imbiribeira	Recife	LAP 1	-8,121628	-34,91803
SECRETARIA DE DEFESA SOCIAL	SDS.CIODS-CICCR-ATI.LINK-TELEFONIA	Av. Rio Capibaribe, 147	São Jose	Recife	LAP 2	-8,066551	-34,884418
SECRETARIA DE DEFESA SOCIAL	PMPE.4ºBPM.POLICLINICA	BR 104	Pinheiropolis	Recife	LAP 1	-8,30054	-35,97671
SECRETARIA DE DEFESA SOCIAL	SDS.AIS-VARZEA.LINK-PRINCIPAL	Rua Maria Lacerda, S/N	Várzea	Recife	LAP 1	-8,04812	-34,961331
SECRETARIA DE DEFESA SOCIAL	SDS.CIIDS-ESINT.LINK-PRINCIPAL	Rua Artur Coutinho - 98, Santo Amaro, Recife - PE	Santo Amaro	Recife	LAP 1	-8,049029	-34,879207
SECRETARIA DE DEFESA SOCIAL	SDS.AIS.PETROLINA-DINTER2.LINK-PRINCIPAL	Av. Cardoso de Sa S/N	Vila Eduardo	Petrolina	LAP 1	-9,384205	-40,483849
SECRETARIA DE DEFESA SOCIAL	SDS.CIIDS-SEDE.LINK-PRINCIPAL	Av Rio Capibaribe 147	São José	Recife	LAP 2	-8,068837	-34,885962

SECRETARIA DE DEFESA SOCIAL	SDS.AIS-PAZERES.LINK-PRINCIPAL	Estrada da Batalha, S/N	Prazeres	Jaboatão dos Guararapes	LAP 1	-8,153934	-34,920667
SECRETARIA DE DEFESA SOCIAL	SDS.AIS-APIUCOS.LINK-PRINCIPAL	Rua Dois Irmãos, Nº15	Apipucos	Recife	LAP 1	-8,020632	-34,936271
SECRETARIA DE DEFESA SOCIAL	SDS.GTA-CARUARU.LINK-PRINCIPAL	Avenida Oscar Laranjeira, S/N, Aeroporto do Cajá	Vila do Aeroporto	Caruaru	LAP 1	-8,284771	-36,010756
SECRETARIA DE DEFESA SOCIAL	SDS.NUPREV-SEDE.LINK-PRINCIPAL	Av. Recife, SN	Ipsep	Recife	LAP 1	-8,110363	-34,926689
SECRETARIA DE DEFESA SOCIAL	SDS.ENGENHARIA-OUVIDORIA.LINK-PRINCIPAL	Rua São Geraldo, 111	Santo Amaro	Recife	LAP 2	-8,053627	-34,880446
SECRETARIA DE DEFESA SOCIAL	SDS.AIS-AFOGADOS-INGAZEIRA.LINK-PRINCIPAL	Rua PADRE LUIZ GONZAGA CAMPOS DE GOIZ, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,753618	-37,632381
SECRETARIA DE DEFESA SOCIAL	SDS.AIS-PALMARES.LINK-PRINCIPAL	Av. José Américo de Miranda, S/N	Santa Rosa	Palmares	LAP 1	-8,679116	-35,580084
SECRETARIA DE DEFESA SOCIAL	SDS.SEPDEC-NOVO.LINK-PRINCIPAL	Cais de Santa Rita / São José - Recife - antiga sede do Grande Recife Consórcio		Recife	LAP 2	-8,069042	-34,876561
SECRETARIA DE DEFESA SOCIAL	SDS.CERCPAT.LINK-PRINCIPAL	Rua Coelho Leite, 393	Santo Amaro	Recife	LAP 1	-8,050396	-34,880894
SECRETARIA DE DEFESA SOCIAL	SDS.SEPDEC.LINK-PRINCIPAL	Cais Santa Rita, 600	São José	Recife	LAP 1	-8,0715043	-34,8789201
SECRETARIA DE DEFESA SOCIAL	SDS.CIODS-CICCR-ATI.LINK-PRINCIPAL	Av Rio Capibaribe, Nº 147	São José	Recife	LAP 2	-8,069177	-34,88617
SECRETARIA DE DEFESA SOCIAL	SDS.CICOM.LINK-PRINCIPAL	R. São Geraldo, Nº 126		Recife	LAP 1	-8,053598	-34,879724
SECRETARIA DE DESENVOLVIMENTO AGRÁRIO	Sec de Agricultura e Reforma Agrária - Ebape (Sara Anexo)	Av. General San Matin, 1371	San Martin	Recife	LAP 1	-8,063117	-34,926454
SECRETARIA DE DESENVOLVIMENTO ECONÔMICO	SDETE - Sede - SDEC	AV RIO BRANCO, 104	BAIRRO DO RECIFE	Recife	LAP 2	-8,062653	-34,87238
SECRETARIA DE DESENVOLVIMENTO ECONÔMICO	SDETE - Sede - SDEC	AV RIO BRANCO, 104	BAIRRO DO RECIFE	Recife	LAP 2	-8,062653	-34,87238
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Serra Talhada	Rua Enoc Inacio De Oliveira, 1312	Centro	Serra Talhada	LAP 1	-7,99213052	38,29500371
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Bezerros	Praça Duque de Caxias, S/N	Centro	Bezerros	LAP 1	-8,234678	-35,752455
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Paudalho	Rua Senador Pinheiros Ramos, S/N	Centro	Paudalho	LAP 1	-7,89652	-35,178222
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Camaragibe	Rua Getúlio Alves de Albuquerque - 17	Vila Doutor Chico	Camaragibe	LAP 1	-8,02316776	34,99100641
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	SEDEPE - Anexo I	Rua da Saudade	Boa Vista	Recife	LAP 1	-8,058185	-34,880819

SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Santa Cruz Capibaribe	Avenida Padre Zuzinha - 178	Centro	Santa Cruz do Capibaribe	LAP 1	-7,959282	-36,200415
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Igarassu	Av. Alfredo Bandeira de Melo, 220	Saramandaia	Igarassu	LAP 1	-7,827703	-34,914561
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Caruaru	Rua Floriano Peixoto, 147	Centro	Caruaru	LAP 1	-8,283674	-35,972535
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	SEDEPE - Vitória de Santo Antão	Av. Henrique de Holanda, 3000	Redenção	Vitória de Santo Antão	LAP 1	-8,116767	-35,270252
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Goiana	Rua Luiz Gomes, 130	Centro	Goiana	LAP 1	-7,560593	-34,998334
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	SEDEPE - União - Anexo II	Rua da União, Nº 293	Centro	Recife	LAP 1	-8,059412	-34,880899
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Garanhuns	Rua Amauri De Medeiros, 20	Heliópolis	Garanhuns	LAP 1	-8,886006	-36,487755
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Belo Jardim	Rua Monsenhor Francisco de Assis Neves, 80	Centro	Belo Jardim	LAP 1	-8,333818	-36,41849
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Cabo	Rua Dr Antonio De Souza Leao, S/N	Centro	Cabo de Santo Agostinho	LAP 1	-8,287955	-35,038419
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Salgueiro	Av. Antonio Angelim - 570	Santo Antônio	Salgueiro	LAP 1	-8,072433	-39,124081
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - São Lourenço da Mata	Rua Pedro Celestino Munir, 175	Centro	São Lourenço da Mata	LAP 1	-7,990367	-35,040923
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Araripina	Rua Antônio Alexandre Alves, 385	Centro	Araripina	LAP 1	-7,57845119	-40,49791296
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Ipojuca	Rua MARIO COSTA MONTEIRO, 95	Centro	Ipojuca	LAP 1	-8,400453	-35,061869
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Paulista	Praça Coronel Alberto Lundgren, Sn	Centro	Paulista	LAP 1	-7,941085	-34,882196
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Arcoverde	Rua Coronel Antonio Japiassú, S/N	Centro	Arcoverde	LAP 1	-8,417644	-37,058521

SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Palmares	Av. Frei Caneca, S/N	Centro	Palmares	LAP 1	-8,682182	-35,591349
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Pesqueira	Av. Ézio Araújo, 400	Centro	Pesqueira	LAP 1	-8,35452533	36,69057324
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Nazaré	Br 408, 160	Centro	Nazaré da Mata	LAP 1	-7,74467403	35,23472734
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Aurora	Rua Da Aurora, 425	Boa vista	Recife	LAP 1	-8,05993322	34,88055377
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Aurora	Rua Da Aurora, 425	Boa vista	Recife	LAP 2	-8,060107	-34,880618
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	Agência do Trabalho - Escada	Rua Paulo Parizo - 21	Jaguaribe	Escada	LAP 1	-8,363746	-35,236641
SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO	SEDEPE - Caruaru	Rua Armando da Fonte, 15	Maurício de Nassau	Caruaru	LAP 1	-8,281993	-35,972345
SECRETARIA DE EDUCAÇÃO E ESPORTES	26044447 ESCOLA ESTADUAL INDIGENA FULNI-O MARECHAL RONDON   GRE 10	ALDEIAMENTO INDIGENA FULNI-O	ALDEIA FULNIO	Águas Belas	LAP 1	-9,11637	-37,12306
SECRETARIA DE EDUCAÇÃO E ESPORTES	26032082 EREM MINISTRO MARCOS FREIRE GRE 14	Rua Professora Maria Do Carmo Novaz, 7	Cohab	Cabrobó	LAP 2	-8,50652	-39,319885
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123509 ESCOLA EDWIGES DE SA PEREIRA GRE 02	Rua: Rivadavia Guerra, 50	Tegipio	Recife	LAP 2	-8,089933	-34,952395
SECRETARIA DE EDUCAÇÃO E ESPORTES	26108046 ESCOLA MAJOR LÉLIO GRE 04	Est Aldeia, Sn	Aldeia De Baixo	Camaragibe	LAP 2	-7,967574	-35,003769
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127415 EREM OLINTO VICTOR GRE 02	Av. Afonso Olindense, 153	Várzea	Recife	LAP 1	-8,03241358	34,95546182
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123819 ETE MARIANO TEIXEIRA GRE 02	Av. Capitão Felipe Ferreira, S/N	Areias	Recife	LAP 2	-8,095653	-34,930882
SECRETARIA DE EDUCAÇÃO E ESPORTES	26052776 EREM CORSINA BRAGA GRE 09	Av. Prefeito José Raimundo, S/N	Centro	Cachoeirinha	LAP 2	-8,490356	-36,242956
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178230 ETE CICERO DIAS GRE 02	Rua Marquês De Valença, Nº 470	Boa Viagem	Recife	LAP 2	-8,128649	-34,906631
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059150 ESCOLA ESTADUAL INDIGENA INTERMEDIÁRIA MONS OLÍMPIO TORRES GRE 11	ALDEIA CAPIM DE PLANTA, ZONA RURAL		Pesqueira	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26032090 ESCOLA ESTADUAL INDIGENA ACILON CIRIACO DA LUZ GRE 14	Aldeia Camaleão, s/n	Ilha Assunção	Cabrobó	LAP 1	-8,51876508	-39,3928379
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034310 ESCOLA ESTADUAL DE ALTERNANCIA   GRE 14	Estrada das Pedrinhas, 20	Carneiro	Petrolina	LAP 1	-9,383297	-40,484597
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009617 ESCOLA FRANCISCO ALVES DE CARVALHO GRE 15	Rua Laudelino Geronimo da Silva, S/N	Centro	Mirandiba	LAP 2	8,121476929	38,72850773

SECRETARIA DE EDUCAÇÃO E ESPORTES	26043408 ESCOLA ESTADUAL INDIGENA PRINCESA ISABEL GRE 13	ALDEIA CARRAPATEIRA	ZONA RURAL	Tacaratu	LAP 1	-8,93384	-38,10545
SECRETARIA DE EDUCAÇÃO E ESPORTES	26099365 ESCOLA DR FERNANDO CAMPELO GRE 06	Rua Sete De Setembro, 104	Riacho do Navio	Escada	LAP 1	-8,36118961	35,22490854
SECRETARIA DE EDUCAÇÃO E ESPORTES	26147190 ESCOLA ESTADUAL INDÍGENA ORORUBA GRE 11	ALDEIA CANA BRAVA	Zona Rural	Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134177 ESCOLA OLGA BENÁRIO PRESTES GRE 02	Rua Bom Pastor, 1407	Engenho do Meio	Recife	LAP 1	-8,048254	-34,939788
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186446 ESCOLA ESTADUAL INDIGENA QUITERIA MARIA DE JESUS GRE 13	Aldeia Saco dos Barros, S/N	Terra Indígena Pankararu	Jatobá	LAP 1	-9,125617	-38,207849
SECRETARIA DE EDUCAÇÃO E ESPORTES	26182092 ESCOLA ESTADUAL ESCRITOR MAXIMIANO ACCIOLY CAMPOS GRE 07	Rua José Francisco de Arruda, 85	COHAB	Sirinhaém	LAP 1	-8,590605	-35,117978
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115964 ESCOLA GOVERNADOR ERALDO GUEIROS LEITE GRE 03	Rua Serra Talhada, S/N	Arthur Lundgren Dois	Paulista	LAP 2	-7,92338	-34,893071
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069210 EREM PROFª JANDIRA DE ANDRADE LIMA GRE 08	Loteamento Santo Antonio, 1165	Ladeira Vermelha	Limoeiro	LAP 2	-7,8812	-35,437908
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050064 ESCOLA FREI CASSIANO COMACCHIO GRE 09	Rua Amelia Soares Da Paz, S/N	Boa Vista	Belo Jardim	LAP 2	-8,33234006	36,41832267
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001225 ESCOLA SAO JOAO BATISTA - ARARIPINA GRE 16	Rua Genuino de Albuquerque, Lagoa Do Barro, S/N	Lagoa do Barro	Araripina	LAP 1	-7,768385	-40,368336
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128462 EREM PROFª PEDRO AUGUSTO CARNEIRO LEAO GRE 01	Av. Beberibe, 2595	Beberibe	Recife	LAP 2	-8,015549	-34,89103
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001942 EREM ARTUR BARROS CAVALCANTI GRE 16	Rua Agamanom Magalhães, 83	Centro	Bodocó	LAP 2	-7,780583	-39,937162
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024659 CENTRO DE ATENDIMENTO EDUCACIONAL ESPECIALIZADO DE ARCOVERDE GRE 11	Av. João Pessoa, 280	São Miguel	Arcoverde	LAP 2	-8,425632	-37,057203
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124874 ESCOLA MISSIONARIO SAO BENTO GRE 02	Rua Capitão Vicente Curado, 350	UR4 - Ibura	Recife	LAP 2	-8,131444	-34,947714
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114135 EREM SANTO INACIO DE LOYOLA GRE 03	Estrada Da Caenga 294	São Benedito	Olinda	LAP 2	-8,000041	-34,894884
SECRETARIA DE EDUCAÇÃO E ESPORTES	26014564 EREM NORMAL ESTADUAL PROFESSORA IONE DE GÔES BARROS GRE 12	Rua Pe Luiz Gonzaga Campos De Gois, S/N	Centro	Afogados da Ingazeira	LAP 2	-7,748017	-37,634663
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127423 EREM PINTOR LAURO VILLARES GRE 02	Clarice Lispector, SN	Torrões	Recife	LAP 2	-8,060612	-34,937776
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035073 ESCOLA POETA CARLOS DRUMOND DE ANDRADE GRE 14	Proj Senador Nilo Coelho, S/N	Zona Rural	Petrolina	LAP 2	-9,292466	-40,430223
SECRETARIA DE EDUCAÇÃO E ESPORTES	26065401 EREM ANA FAUSTINA GRE 08	Rua Agamenom Magalhães, 279	Centro	Surubim	LAP 2	-7,839688	-35,76012

SECRETARIA DE EDUCAÇÃO E ESPORTES	26140179 EREM ENEIDE COELHO PAIXAO CAVALCANTI GRE 14	Rua Projetada, S/N	João de Deus	Petrolina	LAP 2	-9,3947	-40,500661
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111020 EREM HUMBERTO LINS BARRADAS GRE 04	R. Riacho da Plata, S/N	Muribeca	Jaboatão dos Guararapes	LAP 2	-8,177403	-34,975758
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040441 ESCOLA ESTADUAL INDIGENA MANOEL JOAO DE SOUZA GRE 13	ALDEIA TRAVESSA DA PEDRA	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,463405	-38,700565
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040220 ESCOLA CELESTINO NUNES GRE 13	Av. Tenente Domingos Nogueira de Sa, S/N	Centro	Belém de São Francisco	LAP 1	-8,439151	-39,032216
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113538 EREM GUEDES ALCOFORADO GRE 03	Av. Joaquim Nabuco, 838	Varadouro	Olinda	LAP 2	-8,013241	-34,855583
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058596 ESCOLA ESTADUAL INDIGENA DAMIÃO MONTEIRO GRE 11	ALDEIA LAGOA		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26133974 EREM PEDRO SANTOS ESTIMA GRE 12	Rua Pedro Santos Estima, S/N	Centro	Flores	LAP 2	-7,86411	-37,977017
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122847 EREM AMAURY DE MEDEIROS GRE 02	Rua São Miguel, S/N	Afogados	Recife	LAP 2	-8,08073	-34,915559
SECRETARIA DE EDUCAÇÃO E ESPORTES	26108240 ESCOLA TIMBI GRE 04	Rua Oscar André de Albuquerque 154	Timbí	Camaragibe	LAP 2	-8,026001	-34,997271
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024675 EREM SENADOR VITORINO FREIRE GRE 11	Rua Gumercindo Cavalcante, S/N	São cristóvão	Arcoverde	LAP 2	-8,41166792	-37,691931
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111071 ESCOLA JOSE GLICERIO GRE 04	Rua Sete De Setembro, S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,206425	-34,957832
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110199 EREM MURILO BRAGA GRE 04	Av. Agamenon Magalhães, N° 719	Cavaleiro	Jaboatão dos Guararapes	LAP 1	-8,159066	-34,921298
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125293 EREM SENADOR ANTONIO FARIAS GRE 02	Rua Ibirapua, 757	Três Carneiros Baixos	Recife	LAP 1	-8,126395	-34,957485
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075970 ESCOLA SAO CRISTOVAO GRE 10	Rua da Liberdade, S/N	Eliópolis	Garanhuns	LAP 2	-8,889387	-36,475971
SECRETARIA DE EDUCAÇÃO E ESPORTES	26167158 ESCOLA PROFª GALTEMIR LINS GRE 07	Travessa N.S. de Lourdes, S/N	Centro	Palmares	LAP 1	-8,683417	-35,591523
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126079 EREM AGEU MAGALHAES GRE 01	Estrada Do Arraial, N° 3208		Recife	LAP 2	-8,030552	-34,906061
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113813 EREM COMPOSITOR ANTÔNIO MARIA GRE 03	Av. Das Acácias S/Nº	Rio Doce 2ª Etapa	Olinda	LAP 2	-7,959149	-34,844384
SECRETARIA DE EDUCAÇÃO E ESPORTES	26062410 EREM AGAMENON MAGALHAES GRE 09	Av. Antonio C. Araujo, S/N	Centro, Margem da BR-232	São Caetano	LAP 2	-8,327627	-36,137065
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169738 ESCOLA ESTADUAL INDIGENA SANTA MADALENA GRE 13	Aldeia Jatobá Serra UMA, s/n	Zona Rural	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26056577 EREM PROFª ANTONIO FARIAS GRE 06	Rua Quintino Bocaiúva, S/N	São José	Gravatá	LAP 2	-8,198744	-35,569268
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091828 EREM PROFª JOSE MENDES DA SILVA GRE 05	Rua Sete De Setembro, S/N	Centro	Timbaúba	LAP 2	-7,514469	-35,310455

SECRETARIA DE EDUCAÇÃO E ESPORTES	26084040 EREM EZEQUIEL BERTINO DE ALMEIDA GRE 09	Av. Miguel Pereira Neto, 835	Novo Horizonte	Cupira	LAP 1	-8,595572	-35,95297
SECRETARIA DE EDUCAÇÃO E ESPORTES	26005689 ESCOLA SAO VICENTE DE PAULA - OURICURI GRE 16	Praça Voluntarios Da Patria - 320 - Ouricuri	Centro	Ouricuri	LAP 1	-7,885796	-40,083115
SECRETARIA DE EDUCAÇÃO E ESPORTES	26076357 ESCOLA INSTITUTO PRESBITERIANO DE HELIOPOLIS GRE 10	Av. Frei Caneca, S/N	Heliópolis	Garanhuns	LAP 2	-8,883979	-36,481067
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185113 ETE PEDRO LEÃO LEAL GRE 15	Rodovia pe 430, S/N	Centro	São José do Belmonte	LAP 2	-7,88917967	-38,74140269
SECRETARIA DE EDUCAÇÃO E ESPORTES	26016010 ESCOLA JOAO GOMES DOS REIS GRE 12	Rua Mário Melo, S/N	Centro	Carnaíba	LAP 1	-7,802815	-37,794386
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110970 EREM EDMUR ARLINDO DE OLIVEIRA GRE 04	Av. Oito, S/N - Quadra 23	Curado IV	Jaboatão dos Guararapes	LAP 2	-8,072255	-34,997021
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185750 ETE JORNALISTA CYL GALLINDO GRE 11	Rua São Jorge S/N	Frei Damião	Buíque	LAP 1	-8,61539158	-37,15891631
SECRETARIA DE EDUCAÇÃO E ESPORTES	26187973 EREM PROFª EVANIRA DE SOUZA DIAS EREM DE SÃO GONÇALO GRE 14	Rua 7	São Gonçalo	Petrolina	LAP 2	-9,38497	-40,547792
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090058 EREM DOUTOR FRANCISCO SIQUEIRA C DA CUNHA GRE 05	Rua Jose Edson Neves, S/N	Centro	Lagoa do Carro	LAP 2	-7,844453	-35,316211
SECRETARIA DE EDUCAÇÃO E ESPORTES	26165112 ESCOLA SANTA SOFIA GRE 04	Rua Manoel Ribeiro, 800		Camaragibe	LAP 2	-8,021406	-34,979189
SECRETARIA DE EDUCAÇÃO E ESPORTES	26004593 EREM JOAQUIM EUGÊNIO SILVA GRE 16	Rua Fernando Bezerra, S/N	Centro	Ipupi	LAP 2	-7,65453163	-40,15007567
SECRETARIA DE EDUCAÇÃO E ESPORTES	26026902 ESCOLA APOLONIO ALVES DA SILVA GRE 11	Rua A DENOCS, 80	Centro	Ibimirim	LAP 1	-8,534383	-37,695221
SECRETARIA DE EDUCAÇÃO E ESPORTES	26055210 ESCOLA JOSE CARLOS FLORENCIO GRE 09	Rua Zeneide Maria Dos Vasconcelos, S/N	Divinópolis	Caruaru	LAP 2	-8,27148978	-35,97908055
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126311 ESCOLA MATIAS DE ALBUQUERQUE GRE 01	Rua Fernando De Souza Catés S/N	Casa Amarela	Recife	LAP 1	-8,058079	-34,879205
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054060 ESCOLA DOM VITAL - CARUARU GRE 09	Praça Dom Vital, S/N	Divinópolis	Caruaru	LAP 2	-8,279688	-35,977867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26014190 EREM ANISIO VERAS GRE 15	Rua Antônio Cecílio Rangel, 100	Centro	Verdejante	LAP 2	-7,92582516	-38,97140675
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040956 ETE DEPUTADO AFONSO FERRAZ GRE 13	Av. Deputado Audomar Ferraz, 99	Centro	Floresta	LAP 2	-8,599566	-38,571897
SECRETARIA DE EDUCAÇÃO E ESPORTES	26177790 ESCOLA ESTADUAL BENTO XVI GRE 14	AVENIDA FAZENDA JATOBA, 640	Jatoba	Petrolina	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26154803 EREM ELVIRA GRANJA DE SOUZA GRE 16	Av. Antônio Floresta, S/N	Centro	Santa Cruz	LAP 1	-8,239743	-40,332844
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116324 EREM PROFª ARNALDO CARNEIRO LEAO GRE 03	Rua Cento E Vinte E Seis, S/N	Maranguape I	Paulista	LAP 2	-7,946749	-34,862012

SECRETARIA DE EDUCAÇÃO E ESPORTES	26148021 EREM GREGÓRIO BEZERRA - PANELAS GRE 09	Travessa João Timóteo De Andrade, S/N	Centro	Panelas	LAP 2	-8,666203	-36,008998
SECRETARIA DE EDUCAÇÃO E ESPORTES	26183021 ETE MIGUEL BATISTA GRE 01	AV NORTE MIGUEL ARRAES DE ALENCAR Nº7800	MACAXEIRA	Recife	LAP 2	-8,012994	-34,931574
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129124 ESCOLA DONA LEONOR PORTO GRE 04	Av. Um	Parque Capibaribe	São Lourenço da Mata	LAP 2	-8,012517	-35,039631
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176220 ETE CELIA DE SOUZA LEAO ARRAES DE ALENCAR GRE 06	RODOVIA PE 109, KM 2, S/N	Distrito Industrial	Bonito	LAP 1	-8,483957	-35,745648
SECRETARIA DE EDUCAÇÃO E ESPORTES	26037904 EREM PADRE MAURILO SAMPAIO GRE 14	Av. Dr.Oscar Sampaio, 421	Centro	Santa Maria da Boa Vista	LAP 1	-8,80399	-39,82287
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106698 ESCOLA ORFANATO ESTRELA DE BETHEL GRE 03	Rua Sidiney Carson, S/N	Planalto	Abreu e Lima	LAP 2	-7,905487	-34,917602
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034476 EREM MOYSES BARBOSA GRE 14	Av. São Francisco, S/N	Areia Branca	Petrolina	LAP 2	-9,387198	-40,489395
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178699 EREM DE ARCOVERDE GRE 11	Rua Acelino De Brito, 280	Boa Vista	Arcoverde	LAP 2	-8,417113	-37,039268
SECRETARIA DE EDUCAÇÃO E ESPORTES	26029910 EREM OLAVO BILAC GRE 11	Av. Agamenom Magalhães, 703	Centro	Sertânia	LAP 2	-8,067982	-37,26488
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125650 EREM LIONS DE PARNAMIRIM GRE 01	Rua Manuel De Medeiros, S/N	Dois Irmãos	Recife	LAP 2	-8,01414	-34,947712
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090856 ESCOLA CAPITAO PLINIO DE SOUZA MONTEIRO GRE 05	Rua João Antônio Pessoa Guerra, S/N	Juá	Nazaré da Mata	LAP 1	-7,749061	-35,234265
SECRETARIA DE EDUCAÇÃO E ESPORTES	26053853 EREM NICANOR SOUTO MAIOR GRE 09	Rua Carlos Laete, S/N	Indianópolis	Caruaru	LAP 2	-8,290527	-35,960955
SECRETARIA DE EDUCAÇÃO E ESPORTES	26048949 ESCOLA ESTADUAL INDÍGENA TOMÁS CALIXTO GOMES GRE 11	ALDEIA PALMEIRA	ZONA RURAL	Tupanatinga	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26029812 ESCOLA AMARO LAFAYETTE GRE 11	Rua Araújo Guimarães, S/N	Centro	Sertânia	LAP 2	-8,07371	-37,267043
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123720 EREM BARAO DO BONITO GRE 02	Praça 4 De Outubro, S/N	Areias	Recife	LAP 2	-8,095415	-34,939029
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050196 EREM PROFª DONINO GRE 09	Rua Coronel Antônio Marinho, 129	Centro	Belo Jardim	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26049406 EREM QUITERIA WANDERLEY SIMOES GRE 11	Rua Capitão Justino Alto, 177	Centro	Venturosa	LAP 2	-8,57649	-36,874877
SECRETARIA DE EDUCAÇÃO E ESPORTES	26099497 EREM VIGARIO PEDROSA GRE 06	Rua Dr Alfredo Correia, S/N	Centro	Escada	LAP 2	-8,365532	-35,236126
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126214 EREM GOV CARLOS DE LIMA CAVALCANTI GRE 01	Rua Desembargador Mota Júnior, 120	Casa Amarela	Recife	LAP 2	-8,026472	-34,910429

SECRETARIA DE EDUCAÇÃO E ESPORTES	26125080 EREM LUIS DE CAMOES GRE 02	Rua Dr Henrique Lins, S/N	Brasília Teimosa	Recife	LAP 2	-8,085284	-34,88257
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091879 EREM ANA EUFRASIA CABRAL DE MOURA GRE 05	Av. Dr. Ferreira Lima, S/N	Centro	Timbaúba	LAP 2	-7,51594471	35,31077766
SECRETARIA DE EDUCAÇÃO E ESPORTES	26045656 EREM SAO FELIX DE CANTALICE GRE 11	Rua Rene Barbosa De Lima, S/N	Frei Damião	Buique	LAP 2	-8,615372	-37,156667
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111349 EREM SUPERVISORA MIRIAM SEIXAS GRE 04	RUA MATA GRANDE,N°100	PRAZERES	Jaboatão dos Guararapes	LAP 1	-8,203057	-34,960049
SECRETARIA DE EDUCAÇÃO E ESPORTES	26104083 EREM ELOY MALTA DE ALENCAR GRE 07	Rua Do Futuro, S/N	Centro	São Benedito do Sul	LAP 2	-8,811424	-35,932732
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070618 EREM PROFº ANTONIO PEDRO DE AGUIAR GRE 08	Rua JOAO FIRMINO DE MELO, 150	Centro	Orobó	LAP 1	-7,664809	-35,620685
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121654 EREM OLIVEIRA LIMA GRE 01	RUA BARÃO DE SÃO BORJA, 347	BOA VISTA	Recife	LAP 1	-8,06066	-34,890491
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107104 ESCOLA DE ABREU E LIMA GRE 03	Rua Cedro, S/N	Matinha	Abreu e Lima	LAP 1	-7,900104	-34,905931
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107937 EREM PROFº ANTONIO CARNEIRO LEAO GRE 04	Rua Teófila Da Melo, S/N		Camaragibe	LAP 2	-8,021759	-34,980069
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116391 ESCOLA PROFª ZULMIRA DE PAULA ALMEIDA GRE 03	Rua 29, S/N	Jardim Paulista Baixo	Paulista	LAP 2	-7,93238	-34,856955
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011654 EREM JOSE VITORINO DE BARROS GRE 15	Rua Ermirio Ribeiro, 207	Nossa Senhora Das Graças	Salgueiro	LAP 1	-8,067526	-39,123736
SECRETARIA DE EDUCAÇÃO E ESPORTES	26102250 EREM DR FERNANDO PESSOA DE MELLO GRE 07	Trav. Rio Branco, S/N	Alto do Areias	Quipapá	LAP 2	-8,827633	-36,006598
SECRETARIA DE EDUCAÇÃO E ESPORTES	26039770 EREM DR ALIPIO LUSTOSA GRE 13	Rua Projetada, S/N	Belo Horizonte	Belém de São Francisco	LAP 2	-8,750878	-38,962606
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090970 ESCOLA DE APLICACAO PROFº CHAVES GRE 05	Rua Prof Americo P Brandao, 43	Centro	Nazaré da Mata	LAP 2	-7,742209	-35,229038
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124904 EREM VILA DOS MILAGRES GRE 02	Rua Nossa Senhora Do Carmo, 340	Ibura	Recife	LAP 1	-8,101015	-34,916416
SECRETARIA DE EDUCAÇÃO E ESPORTES	26095297 EREM PROFª AMELIA COELHO GRE 06	Rua Jornalista José Miranda, 20	Centro	Vitória de Santo Antão	LAP 2	-8,11145921	35,28396334
SECRETARIA DE EDUCAÇÃO E ESPORTES	11999999 GRE 11 - Sertão do Moxotó-Ipanema / Arcoverde Secret	Rua Castro Alves, S/N	São Cristóvão	Arcoverde	LAP 1	-8,41393979	-37,7144376
SECRETARIA DE EDUCAÇÃO E ESPORTES	26004488 ESCOLA NOSSA SENHORA DO SOCORRO GRE 16	Rua Agripina De Sá Maranhão, 25	Centro	Ipupi	LAP 2	-7,652818	-40,149104
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122855 EREM DEBORA FEIJO GRE 02	Rua Jovelino Selva, Nº 71	Afogados	Recife	LAP 1	-8,080397	-34,920827
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124696 EREM MARIA RITA DA SILVA LESSA GRE 02	Av Ind Mendo Sampaio, S/N	Jordao	Recife	LAP 2	-8,136055	-34,938429
SECRETARIA DE EDUCAÇÃO E ESPORTES	26175509 ESCOLA ESTADUAL QUILOMBOLA PROFª ROSA DORALINA MENDES GRE 15	Distrito Conceição das Creoulas, S/N	Centro	Salgueiro	LAP 1	-8,304441	-38,937589

SECRETARIA DE EDUCAÇÃO E ESPORTES	09999999 GRE 09 - Agreste Centro Norte / Caruaru Secret	Rua Olavo Bilac, S/N	Indianópolis	Caruaru	LAP 1	-8,290674	-35,958925
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130149 EREM EMÍDIO CAVALCANTI DE ALBUQUERQUE GRE 04	Rua Petronilo Capistrano Dos Santos, 90	Ponte dos Carvalhos	Cabo de Santo Agostinho	LAP 2	-8,240164	-34,9781
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042487 ESCOLA ESTADUAL INDIGENA RAMIRO DANTAS GRE 13	Aldeia Bem Querer de Cima, s/n	Zona Rural	Jatobá	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058936 EREM DOM ADELMO CAVALCANTI MACHADO GRE 11	Rua Paes Barreto, 800	São Sebastião	Pesqueira	LAP 2	-8,359795	-36,69746
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185946 ETE ADVOGADO JOSÉ DAVID GIL RODRIGUES GRE 04	BR 101, Km 78, SN	Jordão	Jaboatão dos Guararapes	LAP 2	-8,137654	-34,947047
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063310 EREM JOSE LEITE BARROS GRE 09	Rua Inês Carmelita De Araújo, 290	Centro	Tacaimbó	LAP 2	-8,31283013	-36,29443314
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031272 EREM JOSE CALDAS CAVALCANTI GRE 14	Av. 11 Setembro, 647	Centro	Cabrobó	LAP 2	-8,512649	-39,30843
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121670 EREM POETA MANUEL BANDEIRA GRE 01	Pca Miguel Cervantes, 0	Ilha Do Leite	Recife	LAP 2	-8,067035	-34,893844
SECRETARIA DE EDUCAÇÃO E ESPORTES	26187051 ETE MINISTRO FERNANDO LYRA GRE 09	Alameda NC2, S/N	Loteamento Cidade Alta	Caruaru	LAP 2	-8,309054	-35,971857
SECRETARIA DE EDUCAÇÃO E ESPORTES	26057743 EREM JOSÉ LOPES DE SIQUEIRA GRE 09	Praça Rodolfo Graussá, S/N	Centro	Jataúba	LAP 2	-7,98569684	-36,49534383
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058898 ESCOLA ESTADUAL INDIGENA SAO SEBASTIAO - PESQUEIRA GRE 11	ALDEIA PE DE SERRA, Pesqueira		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26067137 EREM DR MOTA SILVEIRA GRE 08	Av. Presidente Castelo Branco, S/N	Noelândia	Bom Jardim	LAP 2	-7,790954	-35,595253
SECRETARIA DE EDUCAÇÃO E ESPORTES	26051702 EREM DOM JOSE LAMARTINE SOARES GRE 06	Rua 16, S/N	Cohab	Bezerros	LAP 1	-8,241281	-35,742842
SECRETARIA DE EDUCAÇÃO E ESPORTES	26015315 EREM JOSE SEVERINO DE ARAUJO GRE 12	Rua Severino C Nogueira, 14	Centro	Brejinho	LAP 1	-7,347231	-37,286982
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020998 EREM IRMA ELIZABETH GRE 12	Av. Afonso Magalhaes , 446	Centro	Serra Talhada	LAP 2	-7,9917	-38,293225
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525879 ESCOLA ESTADUAL PAULO FREIRE GRE 08	RODOVIA PE 90, 23 S/N	Coqueiros	Limoeiro	LAP 1	-7,877229	-35,445088
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058880 ESCOLA ESTADUAL INDÍGENA PADRE CÍCERO GRE 11	ALDEIA BREJINHO		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123592 EREM PROFº TRAJANO DE MENDONÇA GRE 02	Rua Capetinga, S/N	Jardim São Paulo	Recife	LAP 2	-8,07834418	-34,94089376
SECRETARIA DE EDUCAÇÃO E ESPORTES	26182106 ETE ANTONIO DOURADO CAVALCANTI  GRE 10	Rua PROJETADA S/N	Loteamento Frei Damião	Lajedo	LAP 1		

SECRETARIA DE EDUCAÇÃO E ESPORTES	26179474 EREM JOSIAS INOJOSA DE OLIVEIRA GRE 16	Rua Vitor José Modesto, 95	Centro	Araripina	LAP 2	-7,58201515	-40,50001483
SECRETARIA DE EDUCAÇÃO E ESPORTES	26000024 EREM LUIZ GONZAGA DUARTE GRE 16	Rua Vereador José Barreto de Alencar, 222	Centro	Araripina	LAP 1	-7,576688	-40,50269
SECRETARIA DE EDUCAÇÃO E ESPORTES	26005468 ESCOLA NOSSA SENHORA DE FATIMA - OURICURI GRE 16	Rua Nossa Senhora De Fátima, 142	Centro	Ouricuri	LAP 1	-7,88134	-40,083824
SECRETARIA DE EDUCAÇÃO E ESPORTES	26016028 EREM JOAQUIM MENDES DA SILVA GRE 12	Rua Presidente Kennedy, S/N	Centro	Carnaíba	LAP 2	-7,807661	-37,794433
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999900 SEE - DADOS Secret	Rua Afonso Olidense, 1513	Varzea	Recife	LAP 1	-8,044306	-34,958027
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999900 SEE - DADOS Secret	Rua Afonso Olidense, 1513	Varzea	Recife	LAP 2	-8,044306	-34,958027
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178192 EREM PROFª ADAUTO CARVALHO GRE 12	Av. João Gomes De Lucena, 3054	Bomba	Serra Talhada	LAP 2	-7,981887	-38,290391
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011352 EREM PROFª MAURINA RODRIGUES DOS SANTOS GRE 15	Rua Vinte E Dois, S/N	Cohab	Salgueiro	LAP 2	-8,071568	-39,142018
SECRETARIA DE EDUCAÇÃO E ESPORTES	26026627 EREM JOSE PEREIRA BURGOS GRE 11	Av. José Gonçalves Florencio, S/N	Centro	Custódia	LAP 2	-8,086168	-37,640264
SECRETARIA DE EDUCAÇÃO E ESPORTES	26191261 ETE MARIA FERREIRA MARTINS GRE 11	Av. Rio Branco	Centro	Itaíba	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26093600 ESCOLA PAROQUIAL DE MENORES GRE 06	Rua Capitão José Da Penha, S/N	Centro	Glória do Goitá	LAP 2	-8,001851	-35,292791
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035111 EREM PROFª MANOEL XAVIER PAES BARRETO GRE 14	Travessa Mauricio De Nassau, S/N	Gercino Coelho	Petrolina	LAP 2	-9,3947	-40,500661
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128403 EREM PADRE NERCIO RODRIGUES GRE 01	Rua Uriel De Holanda S/N	Linha Do Tiro	Recife	LAP 1	-8,007816	-34,903156
SECRETARIA DE EDUCAÇÃO E ESPORTES	26078872 ESCOLA JORNALISTA MANUEL AMARAL GRE 10	Av. 19 De Maio, 353	Centro	Lajedo	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26051737 EREM PROFª MARIA ANA GRE 06	Rua Dr. Paulo Viana De Queiroz, S/N	São Sebastiao	Bezerros	LAP 2	-8,470308	-35,734533
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070880 EREM MANOEL GUILHERME DA SILVA GRE 08	Rua ALTO SÃO JOSE, S/N	Centro	Passira	LAP 2	-7,98292701	-35,57870996
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128160 ESCOLA DOUTOR FABIO CORREA GRE 01	Travessa Adalberto Elias Da Costa, SN	Beberibe	Recife	LAP 2	-8,005838	-34,898276
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113660 ESCOLA MARECHAL MASCARENHAS DE MORAES GRE 03	Rua A, S/N - 7º Ro	Vila da Cohab	Olinda	LAP 2	-8,00245	-34,867836
SECRETARIA DE EDUCAÇÃO E ESPORTES	26173638 ESCOLA ESTADUAL INDÍGENA ANTÔNIO MANOEL DA SILVA GRE 13	Aldeia Angico	Povo Atikum	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682

SECRETARIA DE EDUCAÇÃO E ESPORTES	26143666 ESCOLA ESTADUAL INDIGENA PROC GERALDO ROLIM MOTA FILHO GRE 11	ALDEIA PEDRA D AGUA, ZONA RURAL - Pesqueira/PE		Pesqueira	LAP 1	-8,358218	-36,698289
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124645 EREM JORNALISTA COSTA PORTO GRE 02	Rua Bahia, S/N	Jordão De Baixo	Recife	LAP 2	-8,133961	-34,935513
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042037 EREM DE JATOBÁ GRE 13	Rua Da Matriz, 50	Centro	Petrolândia	LAP 2	-8,985375	-38,219119
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127741 EREM PROFª HELENA PUGO GRE 02	Rua Quinze De Marco, S/N	Bongi	Recife	LAP 2	-8,067808	-34,932046
SECRETARIA DE EDUCAÇÃO E ESPORTES	26103052 EREM JOAQUIM NABUCO - RIBEIRAO GRE 07	Rua da Igreja, S/N	Centro	Ribeirão	LAP 2	-8,464935	-35,404475
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105730 ESCOLA PROFª ADERBAL JUREMA - MN GRE 03	Rua José Lacerda Leite S/N	Centro - Igarassu	Igarassu	LAP 2	-7,826702	-34,913052
SECRETARIA DE EDUCAÇÃO E ESPORTES	26065592 EREM SEVERINO CORDEIRO DE ARRUDA GRE 09	Rua Severino Tavares, 44	Centro	Taquaritinga do Norte	LAP 2	-7,904023	-36,039363
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126141 EREM DONA MARIA TERESA CORREA GRE 01	Rua Maragogi, S/N	Alto Jose Do Pinho	Recife	LAP 2	-8,022099	-34,907795
SECRETARIA DE EDUCAÇÃO E ESPORTES	26076250 EREM VIRGEM DO SOCORRO GRE 10	Rua Professor Jaime Alves Pinheiro, 255	Severiano Moraes Filho	Garanhuns	LAP 1	-8,885566	-36,461768
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127431 EREM PROFª LEAL DE BARROS GRE 02	R. Antonio Borges Uchoa, S/N	Engenho Do Meio	Recife	LAP 2	-8,056351	-34,942925
SECRETARIA DE EDUCAÇÃO E ESPORTES	26153157 ESCOLA ESTADUAL INDIGENA CLOVIS GOMES DE SÁ GRE 11	Aldeia (Mangue Sitio) Peitudo, s/n	Área Indígena Kambiá	Inajá	LAP 1	-8,77814	-37,69143
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042126 ESCOLA ESTADUAL INDIGENA DOUTOR CARLOS ESTEVAO GRE 13	ALDEIA BREJO DOS PADRES	ZONA RURAL	Jatobá	LAP 1	-9,19301	-38,21109
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024721 EREM ANTONIO JAPIASSU GRE 11	Rua Padre Roma, S/N	Centro	Arcoverde	LAP 2	-8,420105	-37,047029
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091259 EREM CONFEDERACAO DO EQUADOR GRE 05	Av. Confederação Do Equador, 1030	Alto Dois Irmãos	Paudalho	LAP 2	-7,903018	-35,185075
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063891 EREM JOSE FRANCELINO ARAGAO GRE 09	Av. 29 De Dezembro, 648	Bairro Novo	Santa Cruz do Capibaribe	LAP 2	-7,953576	-36,206345
SECRETARIA DE EDUCAÇÃO E ESPORTES	26071673 ESCOLA PROFª JOAO BARBOSA DE ALMEIDA GRE 05	Rua João De Araujo, S/N	Centro	São Vicente Férrer	LAP 2	-7,590262	-35,48987
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054914 EREM PROFª ELISETE LOPES DE LIMA PIRES GRE 09	Rua CRISTO REDENTOR, S/N	Caiuca	Caruaru	LAP 2	-8,313658	-35,99292
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042169 ESCOLA ESTADUAL INDIGENA LOGRADOURO GRE 13	ALDEIA LOGRADOURO-ENTRE SERRAS	ZONA RURAL	Petrolândia	LAP 1	-9,10141216	-38,22120874
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090902 EREM DON VIEIRA GRE 05	Rua Coelho Neto, S/N	Juá	Nazaré da Mata	LAP 2	-7,743499	-35,230552
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116014 EREM MAESTRO NELSON FERREIRA GRE 03	Rua Andre E Karina, S/N	Centro	Paulista	LAP 1	-7,91334653	-34,8428791
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034298 EREM ANTONIO PADILHA GRE 14	Av. Projetada, S/N	José e Maria	Petrolina	LAP 2	-9,400778	-40,541784
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034360 EREM EDSON NOLASCO GRE 14	Rua Projetada, S/N	Projeto Senador Nilo Coelho	Petrolina	LAP 2	-9,32057	-40,56587

SECRETARIA DE EDUCAÇÃO E ESPORTES	26191229 ESCOLA TÉCNICA PROFª MARIA AMELIA DE FREITAS ARAÚJO GRE 14	Rua Agnelo Gonçalves dos Santos	Cohab	Cabrobó	LAP 1	-8,513545	-39,309645
SECRETARIA DE EDUCAÇÃO E ESPORTES	26426714 ESCOLA ESTADUAL INDIGENA CAPITAO DENA GRE 14	ILHA ASSUNCAO		Cabrobó	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113236 EREM AUREA DE MOURA CAVALCANTI GRE 03	Av Dr Joaquim Nabuco, Sn	Ouro Preto	Olinda	LAP 2	-7,987711	-34,855826
SECRETARIA DE EDUCAÇÃO E ESPORTES	26045540 ESCOLA ESTADUAL INDÍGENA SATURNINO VIEIRA DE MELO GRE 11	ALDEIA MALHADOR - ETNIA KAPINAWA	Zona Rural	Buíque	LAP 1	-8,621092	-37,159438
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035146 ESCOLA PROFª ADELINA ALMEIDA GRE 14	Av. Monsenhor Angelo Sampaio, S/N	Areia Branca	Petrolina	LAP 2	-9,382063	-40,488673
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024756 EREM INDUSTRIAL DE ARCOVERDE GRE 11	Rua Castro Alves, S/N	São Cristóvão	Arcoverde	LAP 2	-8,41437	-37,070931
SECRETARIA DE EDUCAÇÃO E ESPORTES	26187825 ETE JURANDIR BEZERRA LINS GRE 03	BR 101 NORTE, KM 43,6	ENCANTO IGARASSU	Igarassu	LAP 2	-7,878806	-34,905346
SECRETARIA DE EDUCAÇÃO E ESPORTES	26004518 EREM ARAO PEIXOTO DE ALENCAR GRE 16	Rua Projetada , S/N	Centro	Ipubi	LAP 2	-7,650639	-40,153767
SECRETARIA DE EDUCAÇÃO E ESPORTES	26094860 EREM GUIOMAR KRAUSE GONÇALVES  GRE 06	Rua Prof Adao Barnabe, S/N	Centro	Vitória de Santo Antão	LAP 2	-8,129641	-35,293852
SECRETARIA DE EDUCAÇÃO E ESPORTES	26099853 EREM DOUTOR JAIME MONTEIRO GRE 07	Av. Luiz Rodolfo, S/N	Centro	Gameleira	LAP 2	-8,587031	-35,385507
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011956 ESCOLA ESTADUAL INDIGENA PROFESSOR EPIFANIO BEZERRA GRE 15	ALDEIA PAUS BRANCOS	ZONA RURAL	Salgueiro	LAP 1	-8,235456	-38,913697
SECRETARIA DE EDUCAÇÃO E ESPORTES	26173719 ESCOLA ESTADUAL INDIGENA VO OLINDINA GRE 13	ALDEIA CACARIA	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040603 ESCOLA ESTADUAL INDIGENA ANTONIO DUDU GRE 13	Aldeia Serra do Jacaré	Zona Rural	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110997 EREM EDSON MOURY FERNANDES GRE 04	Rua 2 CONJUNTO RESIDENCIAL MURIBECA S/N	Muribeca	Jaboatão dos Guararapes	LAP 2	-8,145635	-34,968505
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088894 EREM BENIGNO PESSOA DE ARAUJO GRE 05	Rua Djalma Raposo, S/N	Cidade nova	Goiana	LAP 2	-7,564083	-34,997653
SECRETARIA DE EDUCAÇÃO E ESPORTES	26074907 EREM AUGUSTO LUCIO DA SILVA GRE 10	Rua Emidio Tenorio, 77	Bahia	Correntes	LAP 2	-9,132792	-36,328977
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114488 ESCOLA CAPITAO ANDRE PEREIRA TEMUDO GRE 03	Rua Golfinho, Qd B Vinte, Sn	Ouro Preto	Olinda	LAP 1	-7,992359	-34,865107
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176238 ETE PROFª LUCILO AVILA PESSOA GRE 02	Av. caxanga,3345	CENTRO	Recife	LAP 2	-8,04235996	-34,93532127
SECRETARIA DE EDUCAÇÃO E ESPORTES	26140187 EREM PROFª SUZEL GALIZA GRE 08	Travessa Augusto Costa, S/N	Centro	Limoeiro	LAP 1	-7,862158	-35,442486

SECRETARIA DE EDUCAÇÃO E ESPORTES	26142570 ESCOLA ESTADUAL INDIGENA JOSE GOMES DA SILVA GRE 15	ALDEIA IPOEIRA, ZONA RURAL		Salgueiro	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185741 ETE PROFª FRANCISCO JONAS FEITOSA COSTA GRE 11	Lote nº 07, S/N	Por do Sol	Arcoverde	LAP 2	-8,44093727	-37,5555895
SECRETARIA DE EDUCAÇÃO E ESPORTES	26046040 EREM VIGARIO JOAO INACIO GRE 11	Rua Aurora Laerte Cavalcant, S/N	Centro	Buíque	LAP 2	-8,624977	-37,160455
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178095 EREM CLEMENTINO COELHO GRE 14	Av. Da Integração, S/N	Jardim Maravilha	Petrolina	LAP 2	-9,383797	-40,505597
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091771 EREM MARIANA FERREIRA LIMA GRE 05	Rua Delmira Aboba, S/N	Centro	Timbaúba	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26157985 ETE DE CRIATIVIDADE MUSICAL GRE 01	Rua Aurora, 439	Boa Vista	Recife	LAP 1	-8,059969	-34,880574
SECRETARIA DE EDUCAÇÃO E ESPORTES	26148447 EREM DR ADILSON BEZERRA DE SOUZA GRE 09	Av. Brasil, S/N	Centro	Santa Cruz do Capibaribe	LAP 2	-7,945098	-36,210175
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043130 EREM SERGIO MAGALHAES GRE 13	Rua Da Matriz, 63	Centro	Tacaratu	LAP 1	-9,105569	-38,149421
SECRETARIA DE EDUCAÇÃO E ESPORTES	26188295 EREM POMPÉIA CAMPOS GRE 01	Avenida Norte Miguel Arraes de Alencar - s/n	Apipucos	Recife	LAP 2	-8,013806	-34,931588
SECRETARIA DE EDUCAÇÃO E ESPORTES	26179873 EREM DE BELO JARDIM GRE 09	Av. Sebastião R da Costa, 270	São Pedro	Belo Jardim	LAP 2	-8,326515	-36,419323
SECRETARIA DE EDUCAÇÃO E ESPORTES	26053845 ETE DE CARUARU NELSON BARBALHO GRE 09	Av. Dom Bosco, S/N	Maurício de Nassau	Caruaru	LAP 1	-8,275334	-35,967751
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058910 EREM CACILDA ALMEIDA GRE 11	Rua Anísio Galvão, 16	Centro	Pesqueira	LAP 2	-8,357885	-36,699882
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126150 ESCOLA ERUNDINA NEGREIROS DE ARAUJO GRE 01	Rua Erundina Negreiros De Araujo	Corrego Do Jenipapo	Recife	LAP 1	-8,006675	-34,936461
SECRETARIA DE EDUCAÇÃO E ESPORTES	26540720 EREM PROFª IRENE MARIA RAMOS COELHO GRE 14	Rua Irene Maria Ramos Coelho, S/N	Maria Auxiliadora	Afrânio	LAP 2	-8,512672	-41,012226
SECRETARIA DE EDUCAÇÃO E ESPORTES	26086077 EREM JOÃO PESSOA SOUTO MAIOR GRE 06	Rua Coronel José Pessoa, S/N	Centro	Sairé	LAP 2	-8,331542	-35,706784
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031833 ESCOLA ESTADUAL INDIGENA ROSA MARIA DA CONCEICAO GRE 14	ILHA DA ASSUNCAO	ALDEIA CAITITU	Cabrobó	LAP 1	-8,45577	-39,40359
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110857 ESCOLA ALZIRA DA FONSECA BREUEL GRE 04	Rua 11, S/N	Cajueiro Seco	Jaboatão dos Guararapes	LAP 2	-8,168878	-34,928151
SECRETARIA DE EDUCAÇÃO E ESPORTES	26003082 ESCOLA PADRE MEDEIROS GRE 16	Rua Coronel Romão Sampaio, 60	Centro	Exu	LAP 2	-7,677684	-39,800284
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020955 ETE CLOVIS NOGUEIRA ALVES  GRE 12	Rua Inerio Inagio, S/N	Várzea	Serra Talhada	LAP 1	-7,993523	-38,298454

SECRETARIA DE EDUCAÇÃO E ESPORTES	26064618 EREM NATALICIA MARIA FIGUEIROA DA SILVA GRE 08	Vila Cohab 2, S/N	Santo Antônio	Surubim	LAP 2	-7,8415	-35,76074
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043548 ESCOLA ESTADUAL INDIGENA AMBROSIO PEREIRA JUNIOR GRE 10	SITIO XIXIAKLHA, S/N	Centro	Águas Belas	LAP 1	-9,1288577	-37,0829593
SECRETARIA DE EDUCAÇÃO E ESPORTES	26037653 ESCOLA PROFº AGAMENON MAGALHAES GRE 14	Rua Prefeito Elebar Coelho De Amorim, 144	Centro	Santa Maria da Boa Vista	LAP 2	-8,803066	-39,830218
SECRETARIA DE EDUCAÇÃO E ESPORTES	26131668 ESCOLA ANIBAL CARDOSO GRE 04	Praça Cap. Antonio Braz Pereira, S/N	Nossa Senhora do Ó	Ipojuca	LAP 2	-8,441294	-35,013385
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134213 ETE MARIA EMILIA CANTARELLI GRE 13	Rua Itacuruba, 291	Centro	Belém de São Francisco	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26103834 EREM TAMANDARÉ GRE 07	Av. Leopoldo Lins, 635	Centro	Tamandaré	LAP 2	-8,757866	-35,105071
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125978 EREM ALVARO LINS GRE 01	Av Ver Otacilio Azevedo, 4538	Brejo da Guabiraba	Recife	LAP 2	-7,988713	-34,932599
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050200 EREM PROFª MARIA GALVAO GRE 09	Av. Senador Paulo Guerra, S/N	Santa luzia	Belo Jardim	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26003821 ESCOLA NELSON ARAUJO GRE 16	Rua CORONEL ROMÃO SDAMPAIO, S/N	Centro	Exu	LAP 1	-7,683009	-39,801982
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040972 ESCOLA JÚLIO DE MELLO GRE 13	Praça Major João Novais, S/N	Centro	Floresta	LAP 2	-8,601474	-38,570796
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185725 ESCOLA ESTADUAL LUIZ GOMES DINIZ GRE 16	Rua Projetada, S/N	Centro	Bodocó	LAP 1	-7,69137265	39,99803262
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129566 ESCOLA 10 DE AGOSTO GRE 04	Rua agrestina, s/n	Centro	São Lourenço da Mata	LAP 1	-7,994338	-35,038859
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091720 EREM JORNALISTA JADER DE ANDRADE GRE 05	Rua Emilia C De Moraes, S/N	Barro	Timbaúba	LAP 2	-7,511775	-35,316951
SECRETARIA DE EDUCAÇÃO E ESPORTES	26008530 EREM GOVERNADOR MUNIZ FALCAO GRE 16	Rua Vinte E Cinco De Abril, 268	Centro	Trindade	LAP 2	-7,76043	-40,268083
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089190 EREM ANDRE VIDAL DE NEGREIROS GRE 05	Av. André Vidal De Nageiros, S/N	Centro	Goiana	LAP 2	-7,55766961	-35,1385374
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050048 EREM BENTO AMERICO GRE 09	Rua Cel. Antonio Marinho, 163	Boa Vista	Belo Jardim	LAP 1	-8,333097	-36,417097
SECRETARIA DE EDUCAÇÃO E ESPORTES	26171198 EREM PROFª MARIA EUGENIA LOPES GOMES GRE 04	R. Petrolino Capistrano Dos Santos, S/N	Centro	Cabo de Santo Agostinho	LAP 2	-8,239344	-34,979642
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121867 EREM CONEGO ROCHAEL DE MEDEIROS GRE 01	Av. Jorn Mario Melo, S/N	Santo Amaro	Recife	LAP 2	-8,055639	-34,879702
SECRETARIA DE EDUCAÇÃO E ESPORTES	26175533 ETE PEDRO MUNIZ FALCAO GRE 16	Rua PROJETADA, S/N	Alto da Boa Vista	Arapirina	LAP 1	-7,568721	-40,485231
SECRETARIA DE EDUCAÇÃO E ESPORTES	26038536 EREM GUMERCINDO CABRAL GRE 15	Rua Livino Leite Azevedo, S/N	Centro	Terra Nova	LAP 2	-8,226987	-39,37715
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121824 CENTRO EJA VALDEMAR DE OLIVEIRA GRE 01	Rua Jornalista Mário Melo S/N		Recife	LAP 1	-8,055639	-34,879702
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111926 EREM MARIA DO CÉU BANDEIRA GRE 04	Av. Agamenon Magalhaes, 193	Alto Novo Horizonte	Moreno	LAP 2	-8,106127	-35,194999

SECRETARIA DE EDUCAÇÃO E ESPORTES	26188643 ESCOLA ESTADUAL INDIGENA ANANIAS DE SENA GRE 13	Aldeia Cachoeira I, S/N	Povo Atikum	Carnaubeira da Penha	LAP 1	-8,331116	-38,771865
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113783 EREM PADRE FRANCISCO CARNEIRO GRE 03	Rua Alta Macedo, S/N	São Benedito	Olinda	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26135396 Conservatório Pernambucano de Música - Sede (Cpm) Secret	Av. João De Barros, 594	Soledade	Recife	LAP 1	-8,049242	-34,889927
SECRETARIA DE EDUCAÇÃO E ESPORTES	26153742 ESCOLA ESTADUAL MADRE IVA BEZERRA DE ARAUJO GRE 04	Rua Tenente Manoel Barbosa Da Silva S/N	Centro	Cabo de Santo Agostinho	LAP 2	-8,281518	-35,03062
SECRETARIA DE EDUCAÇÃO E ESPORTES	26118742 EREM SENADOR PAULO PESSOA GUERRA GRE 02	Av. Doutor José Rufino, N: 2993	Tejipió	Recife	LAP 2	-8,091616	-34,949274
SECRETARIA DE EDUCAÇÃO E ESPORTES	26000636 EREM MANOEL RIBEIRO DAMASCENO GRE 16	Travessa Castelo Branco, S/N	Centro	Araripina	LAP 1	-7,809448	-40,485999
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113210 EREM ARGENTINA CASTELLO BRANCO GRE 03	Joaquim Nabuco S/N	Jatobá	Olinda	LAP 2	-8,016505	-34,850151
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058790 ESCOLA ESTADUAL INDÍGENA JOAQUIM NABUCO - PESQUEIRA GRE 11	ALDEIA CAPIM DE PLANTA	ZONA RURAL	Pesqueira	LAP 1	-8,283395	-36,656553
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525810 ETE MIGUEL ARRAES DE ALENCAR  GRE 05	Rodovia Pe-82, S/N	Sapucaia	Timbaúba	LAP 2	-7,511157	-35,317926
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127636 EREM EDUCADOR PAULO FREIRE GRE 02	Av. Abdias De Carvalho S/N	Bongi	Recife	LAP 2	-8,061601	-34,923495
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034352 EREM DR PACIFICO RODRIGUES DA LUZ GRE 14	Rua Cabrobo, S/N	Centro	Petrolina	LAP 2	-9,388062	-40,486286
SECRETARIA DE EDUCAÇÃO E ESPORTES	26062585 EREM PIO XII GRE 09	Av. Luiz Coimbra, S/N	Centro	São Caetano	LAP 2	-8,328534	-36,137628
SECRETARIA DE EDUCAÇÃO E ESPORTES	26132735 EREM SOLIDONIO PEREIRA DE CARVALHO GRE 12	Rua João de Oliveira Lima, 100	Centro	Quixabá	LAP 2	-7,7174798	-37,84322583
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087880 EREM DEPUTADO JOÃO TEOBALDO DE AZEVEDO GRE 05	Rua Praça Vila Da Coab, S/N	Santo Antônio	Carpina	LAP 1	-7,843504	-35,250274
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128497 ETE PROFª ALFREDO FREYRE GRE 01	Rua Zeferino Agra, 193	Arruda	Recife	LAP 1	-8,021136	-34,892679
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176262 ETE PROFª CELIA SIQUEIRA GRE 12	RODOVIA PE-320, S/N	Distrito Industrial	São José do Egito	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113333 ESCOLA CONEGO JONAS TAURINO GRE 03	Rua Libano, S/N	Peixinhos	Olinda	LAP 2	-8,003579	-34,880791
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036045 EREM PROFª HUMBERTO SOARES GRE 14	Rua Roberto Patricio Araújo, 88	Cohab 5	Petrolina	LAP 2	-9,384322	-40,536658
SECRETARIA DE EDUCAÇÃO E ESPORTES	26083493 ESCOLA PE JOSE AUGUSTO GRE 06	Av. Cândido Viana, 175	Centro	Bonito	LAP 2	-8,47335471	-35,73367652

SECRETARIA DE EDUCAÇÃO E ESPORTES	26101203 EREM DR PEDRO AFONSO DE MEDEIROS GRE 07	Rua DIÁRIO DE PERNAMBUCO, S/N	Modelo	Palmares	LAP 2	-8,686344	-35,597366
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109441 EREM DESPORTISTA RUBEM RODRIGUES MOREIRA GRE 04	Nova Travessa, Dr. Julio Maranhao S/N	Cajueiro Seco	Jaboatão dos Guararapes	LAP 2	-8,169995	-34,937885
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034379 EREM EDUARDO COELHO GRE 14	Rua Velha Matias, 108	São José	Petrolina	LAP 1	-9,396578	-40,489796
SECRETARIA DE EDUCAÇÃO E ESPORTES	15999999 GRE 15 - Sertão Central / Salgueiro Secret	Trav. Lourival Sampaio, 395	Nossa Sra. das Graças	Salgueiro	LAP 1	-8,067312	-39,123492
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106159 ESCOLA SENADOR PAULO PESSOA GUERRA GRE 03	Av. João Pessoa Guerra S/N	Pilar	Ilha de Itamaracá	LAP 2	-7,789053	-35,09148
SECRETARIA DE EDUCAÇÃO E ESPORTES	26065606 ESCOLA JOSE BEZERRA DE ANDRADE GRE 09	Rua Lucas Evangelista, 288	Centro	Taquaritinga do Norte	LAP 2	-7,905034	-36,048975
SECRETARIA DE EDUCAÇÃO E ESPORTES	26096072 ESCOLA MIRANDOLINA PESSOA DE QUEIROZ GRE 07	Rua Jose Abel, S/N	Centro	Água Preta	LAP 1	-8,873409	-35,624803
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040760 ESCOLA ESTADUAL INDIGENA ODILON NUNES GRE 13	ALDEIA POCO DO MATO	Zona Rural	Carnaubeira da Penha	LAP 1	-8,39208	-38,736819
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031850 ESCOLA ESTADUAL INDIGENA MANOEL DEODATO DOS SANTOS GRE 14	TRIBO INDIGENA TRUKA ILHA DA ASSUNCAO	ALDEIA CAATINGUINHA	Cabrobó	LAP 1	-8,45577	-39,40359
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114496 EREM CAPITAO LUIZ REIS GRE 03	R. da Linha, S/N	Alto da Bondade	Olinda	LAP 1	-7,989192	-34,906228
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054949 ESCOLA PROFª ROSILDA MACIEL VIEIRA GRE 09	Rua Gustavo Bezerra, 1	Agamenom Magalhães	Caruaru	LAP 1	-8,302696	-35,976953
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128420 EREM PEDRO CELSO GRE 01	Rua Uriel De Holanda, S/N	Beberibe	Recife	LAP 2	-8,007816	-34,903156
SECRETARIA DE EDUCAÇÃO E ESPORTES	26138875 COLEGIO DA POLICIA MILITAR DE PETROLINA - ANEXO I Secret	Av. Coronel Otacilio Ferraz, 20	Jatobá	Petrolina	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115972 EREM HISTORIADOR PEREIRA DA COSTA GRE 03	Av. Brasil, S/N	Maranguape I	Paulista	LAP 2	-7,945184	-34,859944
SECRETARIA DE EDUCAÇÃO E ESPORTES	26419823 EREM TERESINHA DE SOUZA LIRA GRE 13	Av. CENTRAL, S/N	Centro	Floresta	LAP 1	-8,322348	-38,412872
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126613 EREM ROSA DE MAGALHAES MELO GRE 01	Av Anibal Benevolo - 1378	Alto Sta. Terezinha	Recife	LAP 2	-8,010507	-34,901617
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069288 EREM AUSTRO COSTA GRE 08	Rua São Sebastião, 1071	Centro	Limoeiro	LAP 2	-7,861631	-35,441848
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042711 ESCOLA ESTADUAL INDIGENA DO ESPINHEIRO GRE 13	ALDEIA ESPINHEIRO		Tacaratu	LAP 1	-9,1051314	-38,1498128
SECRETARIA DE EDUCAÇÃO E ESPORTES	26068877 EREM NOSSA SENHORA AUXILIADORA GRE 08	Rua Severino Apolho, S/N	Centro	João Alfredo	LAP 2	-7,868067	-35,587688
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106060 EREM ALBERTO AUGUSTO DE MORAIS PRADINES GRE 03	Av. João Pessoa Guerra, S/N	Pilar	Ilha de Itamaracá	LAP 2	-7,759793	-34,828458
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054884 EREM PROFª ADELIA LEAL FERREIRA GRE 09	Av. Cicero Jose Dutra, S/N	Vassoural	Caruaru	LAP 1	-8,300871	-35,973211

SECRETARIA DE EDUCAÇÃO E ESPORTES	26037726 EREM ANTONIO DE AMORIM COELHO GRE 14	Rua Vasco Da Gama, S/N,	Centro	Lagoa Grande	LAP 2	-9,000928	-40,27501
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059371 ESCOLA ESTADUAL INDÍGENA ANTONIO MARINHO FALCAO GRE11	Aldeia Sozinha, Zona Rural - Pesqueira/PE		Pesqueira	LAP 1	-8,358391	-36,698114
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110881 EREM AUGUSTO SEVERO GRE 04	Rua Cosmorama, S/N	Piedade	Jaboatão dos Guararapes	LAP 2	-8,146343	-34,91313
SECRETARIA DE EDUCAÇÃO E ESPORTES	26092492 EREM DR JOAQUIM CORREIA GRE 05	Av. Estefania Carneiro da Cunha, S/N	Centro	Vicência	LAP 2	-7,657808	-35,328103
SECRETARIA DE EDUCAÇÃO E ESPORTES	26021820 EREM MANOEL PEREIRA LINS GRE 12	Rua Severino Pereira Lins, S/N	Alto da Conceição	Serra Talhada	LAP 2	-7,986654	-38,291777
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999900 SEE - DADOS SEDE 2 Secret	Av. AFONSO OLINDENSE, 1513	Várzea	Recife	LAP 2	-8,044306	-34,958027
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035600 EREM GERCINO COELHO GRE 14	Av. Integração, S/N	Loteamento Arcoiris	Petrolina	LAP 2	-9,383797	-40,505597
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059789 EREM COMENDADOR MANOEL CAETANO DE BRITO GRE 11	Rua Francisco Bezerra, S/N	Centro	Poção	LAP 2	-8,18570295	36,70146732
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087529 EREM LAURINDO GOMES GRE 05	Av. Carlos Gomes Pereira, S/N	Centro	Buenos Aires	LAP 1	-7,726853	-35,327092
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169754 ESCOLA ESTADUAL INDÍGENA CAXUA GRE 13	ALDEIA CAXUA	ZONA RURAL	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110270 EREM PROFº MOACYR DE ALBUQUERQUE GRE 04	Av. Joaquim Tenório, S/N	Cavaleiro	Jaboatão dos Guararapes	LAP 2	-8,090828	-34,972731
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126290 ESCOLA MARIA AMALIA GRE 01	Av. Norte, 7750	Macaxeira	Recife	LAP 2	-8,013976	-34,93128
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075903 EREM PROFº JERONIMO GUEIROS GRE 10	Rua Cel Antonio Vitor, 359	São José	Garanhuns	LAP 2	-8,886515	-36,490394
SECRETARIA DE EDUCAÇÃO E ESPORTES	26046130 ESCOLA ESTADUAL INDÍGENA JUSSARA BARBOSA GRE 11	SÍTIO CALDEIRAO	ZONA RURAL	Buíque	LAP 1	-8,67976	-37,16873
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040522 ESCOLA ESTADUAL INDÍGENA SAGRADA FAMILIA GRE 13	ALDEIA ENJEITADO	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059363 ESCOLA ESTADUAL INDÍGENA ANTONIO FEITOZA CHALEGRE GRE 11	ALDEIA MASCARENHAS		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26018314 EREM TERESA TORRES GRE 12	Av. Clístenes Leal, 81	Centro	Itapetim	LAP 2	-7,379253	-37,189334
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115069 ESCOLA NOSSA SENHORA DO CARMO - OLINDA GRE 03	Estrada Do Caenga, 23	Beberibe	Olinda	LAP 1	-8,001605	-34,896489
SECRETARIA DE EDUCAÇÃO E ESPORTES	13999999 GRE 13 - Sertão do SubMédio São Francisco / Floresta Secret	Av. Audomar Ferraz, 65	Centro	Floresta	LAP 1	-8,600399	-38,572026
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058812 ESCOLA PROFº ARRUDA MARINHO GRE 11	Av. Dr. Joaquim De Brito, 229	Prado	Pesqueira	LAP 2	-8,357083	-36,68838
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069652 EREM GINÁSIO ARTHUR CORREIA DE OLIVEIRA GRE 08	Rua Vigário Joaquim Pinto, 732	Centro	Limoeiro	LAP 2	-7,879213	-35,452503

SECRETARIA DE EDUCAÇÃO E ESPORTES	26004453 EREM NOSSA SENHORA DO BOM CONSELHO GRE 16	Av. José Saraiva Xavier, 15	Centro	Granito	LAP 1	-7,710972	-39,615097
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124599 ESCOLA ENEIDA RABELLO GRE 02	Av. Doná Carentina, S/N	Jordão	Recife	LAP 2	-8,136015	-34,936867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115085 ESCOLA THEMISTOCLES DE ANDRADE GRE 03	Rua Dr. Miguel Lima Valverdê, S/N	Monte	Olinda	LAP 1	-8,007944	-34,853926
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098415 EREM SOFIA FEIJO SAMPAIO GRE 07	Av. João Clementino, 255	Centro	Catende	LAP 2	-8,598056	-35,781771
SECRETARIA DE EDUCAÇÃO E ESPORTES	26079739 EREM NARCISO CORREIA GRE 10	Av. Rui Barbosa, 227	Centro	Paranatama	LAP 1	-8,919589	-36,65499
SECRETARIA DE EDUCAÇÃO E ESPORTES	26181975 EREM DJALMA MACÊDO GOMES GRE 11	Povoado Socorro - Fazenda Riacho, 0	Santa Filomena	Arapirina	LAP 1	-7,57656	-40,497632
SECRETARIA DE EDUCAÇÃO E ESPORTES	26019922 EREM OLIVEIRA LIMA - SJ Egito GRE 12	Rua Vereador Raimundo Eufrásio, S/N	Centro	São José do Egito	LAP 2	-7,47669553	37,27341726
SECRETARIA DE EDUCAÇÃO E ESPORTES	26067552 EREM RAIMUNDO HONÓRIO GRE 08	Rua Alto Do Carmo, S/N	Bom Jardim	Bom Jardim	LAP 2	-7,798587	-35,59007
SECRETARIA DE EDUCAÇÃO E ESPORTES	05999999 GRE 05 - Mata Norte / Nazaré da Mata Secret	Rua Coelho Neto, S/N	Juá	Nazaré da Mata	LAP 1	-7,743499	-35,230552
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033879 EREM OTACILIO NUNES DE SOUZA GRE 14	Rua Tchecoslováquia, 500	Areia Branca	Petrolina	LAP 2	-9,386632	-40,493812
SECRETARIA DE EDUCAÇÃO E ESPORTES	26136455 EREM MARECHAL FLORIANO PEIXOTO GRE 03	R. Jose Dias Raposo, S/N	Ouro Preto	Olinda	LAP 1	-7,993719	-34,862987
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121948 EREM SYLVIO RABELLO GRE 01	Av. Jorn Mario Melo	Santo Amaro	Recife	LAP 2	-8,055608	-34,879141
SECRETARIA DE EDUCAÇÃO E ESPORTES	26045753 ESCOLA ESTADUAL INDÍGENA KAPINAWA GRE 11	Aldeia Mina Grande, S/N	Zona Rural	Buíque	LAP 1	-8,67976	-37,16873
SECRETARIA DE EDUCAÇÃO E ESPORTES	26135060 ESCOLA ESTADUAL INDÍGENA CAXIADO GRE 13	ALDEIA CAXIADO, SN POVO PANKARARU, ZONA RURAL		Jatobá	LAP 1	-9,16537	-38,233311
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123231 EREM MACIEL PINHEIRO GRE 02	Praça Barreto Campelo S/N	Torre	Recife	LAP 1	-8,047015	-34,913466
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122510 EREM CLOVIS BEVILAQUA GRE 01	Praça Tertuliano Feitosa, 111	Hipódromo	Recife	LAP 1	-8,081031	-34,938426
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121859 EREM ANIBAL FERNANDES GRE 01	MARQUES DO POMBAL, S/N	SANTO AMARO	Recife	LAP 1	-8,047998	-34,881769
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024578 EREM ERNESTO DE SOUZA LEITE GRE 12	Rua Do Bom Jesus, S/N	Centro	Tuparetama	LAP 2	-7,601726	-37,310758

SECRETARIA DE EDUCAÇÃO E ESPORTES	26098482 EREM MENDO SAMPAIO GRE 07	Praça Ana Maltam, S/N	Centro	Catende	LAP 2	-8,663677	-35,719396
SECRETARIA DE EDUCAÇÃO E ESPORTES	26173697 ESCOLA ESTADUAL INDIGENA NOSSA SENHORA APARECIDA GRE 13	Aldeia Ladeira, S/N	Área Indígena Povo Pankara	Carnaubeira da Penha	LAP 1	-8,320596	-38,7436607
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111225 EREM PROFº EPITACIO ANDRE DIAS GRE 04	Av. Santo Elias, S/N		Jaboatão dos Guararapes	LAP 2	-8,166621	-34,927091
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121344 EREM LUIZ DELGADO GRE 01	Rua Do Hospício, S/N	Boa Vista	Recife	LAP 2	-8,055731	-34,882809
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116308 EREM PRESIDENTE CASTELO BRANCO GRE 03	Av Joao Paulo II, S/N, Mirueira	Mirueira	Paulista	LAP 2	-7,963097	-34,890303
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999909 EREM PROFª MARIA DE MENEZES GUIMARAES - POLO EAD GRE 13	Rua Antônio Cabral Campos, 120	Centro	Itacuruba	LAP 1	-8,727683	-38,684773
SECRETARIA DE EDUCAÇÃO E ESPORTES	26073102 EREM PROFª ISMENIA LEMOS WANDERLEY GRE 10	Av. Da Sé, S/N	Centro	Brejo	LAP 2	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26103370 EREM JOAQUIM SILVERIO PIMENTEL  GRE 07	Rua Barão Do Rio Branco, S/N	Centro	Rio Formoso	LAP 1	-8,670117	-35,142372
SECRETARIA DE EDUCAÇÃO E ESPORTES	26068508 EREM ANTONIO INACIO GRE 08	Rua São Sebastiao da Rocha, S/N	Centro	Feira Nova	LAP 1	-7,950544	-35,38542
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031841 ESCOLA ESTADUAL INDIGENA MARIA ROSA DO ESPIRITO SANTO GRE 14	ALDEIA CORONHEIRA	ILHA DA ASSUNCAO, S/N	Cabrobó	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26056623 EREM CLETO CAMPELO GRE 06	Av. Agamenon Magalhães, 443	Prado	Gravatá	LAP 2	-8,199299	-35,562942
SECRETARIA DE EDUCAÇÃO E ESPORTES	26093030 EREM PRESIDENTE COSTA E SILVA GRE 06	Rua Barbosa Lima, S/N	Centro	Chã de Alegria	LAP 2	-7,99429969	-35,2131735
SECRETARIA DE EDUCAÇÃO E ESPORTES	26142813 ESCOLA ESTADUAL INDÍGENA SÃO JOÃO GRE 11	Aldeia São João, s/n - Zona Rural		Pesqueira	LAP 1	-8,35818	-36,69803
SECRETARIA DE EDUCAÇÃO E ESPORTES	26093995 EREM CAPITAO MANOEL GOMES D ASSUNCAO GRE 06	Rua Espiridião Vieira Santos, 86		Pombos	LAP 1	-8,141975	-35,395807
SECRETARIA DE EDUCAÇÃO E ESPORTES	26101653 ETE DE PALMARES GRE 07	Br 101 Sul - Km 185, S/N	Santa Rosa	Palmares	LAP 1	-8,669523	-35,574749
SECRETARIA DE EDUCAÇÃO E ESPORTES	26112701 EREM DE OLINDA GRE 03	Rua Bonfim , S/N	Carmo	Olinda	LAP 2	-8,015569	-34,84995
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054965 ESCOLA PROFº JOSE BIONE DE ARAUJO GRE 09	Rua Antônio Carlos, 136	Universitário	Caruaru	LAP 2	-8,279622	-35,959245
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107082 ESCOLA PROFª ISaura DE FRANCA GRE 03	Rua 176, S/N	Caetés I	Abreu e Lima	LAP 2	-7,91753199	34,92626632
SECRETARIA DE EDUCAÇÃO E ESPORTES	26029936 EREM PROFº JORGE DE MENEZES GRE 11	Av. Agamenon Magalhães, S/N	Centro	Sertânia	LAP 2	-8,069845	-37,26569
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128454 ESCOLA PROFº JOSE DOS ANJOS GRE 01	Av Hildebrando Vasconcelo Sg, 0	Dois Unidos	Recife	LAP 2	-7,996076	-34,909248
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123703 EREM ANIBAL FALCAO GRE 02	R. Aprigio Guimarães N: 102	Tejipió	Recife	LAP 1	-8,08729	-34,957349
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126125 ETE DOM BOSCO - RECIFE GRE 01	Est Arraial, 3208	Tamarineira	Recife	LAP 1	-8,028085	-34,910795

SECRETARIA DE EDUCAÇÃO E ESPORTES	26129922 JEREM LUISA GUERRA GRE 04	Historiador Pereira Da Costa , Nº 250	Centro	Cabo de Santo Agostinho	LAP 2	-8,283242	-35,033501
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034425 JEREM JOAQUIM ANDRE CAVALCANTI  GRE 14	Av. Francisco Coelho De Amorim, S/N	José Maria	Petrolina	LAP 2	-9,369151	-40,493315
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999913 Secretaria Especial Esporte Centro Santos Dumont Secret	Almirante Nelson Fernandes S/N	Boa Viagem	Recife	LAP 1	-8,131219	-34,908879
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999913 Secretaria Especial Esporte Centro Santos Dumont Secret	Almirante Nelson Fernandes S/N	Boa Viagem	Recife	LAP 1	-8,131111	-34,908864
SECRETARIA DE EDUCAÇÃO E ESPORTES	26135400 ESCOLA ESTADUAL PROFª MARIZA JOSE BARBOSA DA SILVA GRE 08	Vila Bengalas, SN	Centro	Passira	LAP 1	-8,01307	-35,484011
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050137 ESCOLA MINISTRO MARCOS DE BARROS FREIRE GRE 09	Rua Silvestre Pacheco Lins, 385	Santo Antônio	Belo Jardim	LAP 2	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024047 ESCOLA MONSENHOR LUIZ SAMPAIO GRE 12	Rua Padre Ibiapina, 77	Centro	Triunfo	LAP 1	-7,838106	-38,103777
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035138 ESCOLA PROFª WILMA WZELY CUNHA COELHO AMORIM  GRE 14	Projeto Senador Nilo Coelho, S/N	Zona Rural	Petrolina	LAP 1	-9,348561	-40,684724
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031302 ESCOLA ESTADUAL INDIGENA ANTONIO CIRILO DOS SANTOS GRE 14	Aldeia Caatinga Grande, s/n	Ilha da Assunção - Zona Rural	Cabrobó	LAP 1	-8,55	-39,35
SECRETARIA DE EDUCAÇÃO E ESPORTES	26099322 JEREM PROFª ERALDO CAMPOS GRE 06	Rua 24 De Maio, S/N	Santo Antônio	Escada	LAP 2	-8,357444	-35,237533
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106728 JEREM POLIVALENTE DE ABREU E LIMA GRE 03	Rua Praça Bandeira, S/N	Centro	Abreu e Lima	LAP 2	-7,90759802	-34,89893724
SECRETARIA DE EDUCAÇÃO E ESPORTES	26076047 ESCOLA SIMOA GOMES GRE 10	Rua JOSE DILEPIERI S/N	Francisco Siqueira	Garanhuns	LAP 2	-8,905396	-36,480817
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111268 ESCOLA JOAO PAULO I GRE 04	Rua: Fabio Maranhao, Nº 108	Bairro: Prazeres	Jaboatão dos Guararapes	LAP 2	-8,16376	-34,933725
SECRETARIA DE EDUCAÇÃO E ESPORTES	26060124 JEREM MANOEL BACELAR GRE 09	Rua Coronel Joaquim Bezerra, S/N	Centro	Riacho das Almas	LAP 2	-8,13790788	-35,85849024
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098920 ETE LUIZ DIAS LINS  GRE 06	Br-101 Sul, S/N	Riacho do Navio	Escada	LAP 1	-8,361306	-35,221746
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035979 JEREM PADRE LUIZ CASSIANO GRE 14	Rua Vinte E Seis, S/N	Loteamento Recife	Petrolina	LAP 2	-9,368828	-40,483522
SECRETARIA DE EDUCAÇÃO E ESPORTES	26102153 JEREM ELISA MARQUES DE ASSIS GRE 07	Praça Marechal Castelo Branco, S/N	Centro	Primavera	LAP 2	-8,3294507	-35,35303894
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109468 JEREM VILA RICA GRE 04	Av. I - Cohab	Vila Rica	Jaboatão dos Guararapes	LAP 1	-8,122255	-35,027238
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105888 JEREM NOVA CRUZ GRE 03	Rua Anita M. da Fonseca, S/N	Distrito Nova Cruz	Igarassu	LAP 1	-7,855569	-34,897
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111241 JEREM DESEMBARGADOR JOSE NEVES FILHO GRE 04	Rua 10 Vila Social S/N	Cajueiro Seco - Jaboatão	Jaboatão dos Guararapes	LAP 2	-8,167025	-34,926231

SECRETARIA DE EDUCAÇÃO E ESPORTES	26121310 EREM MANOEL BORBA GRE 02	Rua Almirante Nelson Fernandes, S/N	Boa Viagem	Recife	LAP 2	-8,131219	-34,908879
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186713 ESCOLA IRMÃ DULCE GRE 03	Rua Rivaldo Pinho Alves, 50	Caetes II - Distrito	Abreu e Lima	LAP 2	-7,92769	-34,92484
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009633 ESCOLA ESTADUAL INDÍGENA JANUÁRIO DA SILVA GRE 15	FAZENDA TAMBORIL - S/Nº	Zona Rural	Mirandiba	LAP 1	-8,25390333	-38,7102525
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040310 ESCOLA ESTADUAL INDÍGENA BOM JESUS DOS AFLITOS GRE 13	Aldeia Boqueirão, s/n - Zona Rural		Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26136460 EREM SANTA ANA GRE 03	Rua Santana, 0	Jardim Atlantico	Olinda	LAP 2	-7,995636	-35,03555
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113953 EREM COSTA AZEVEDO GRE 03	Av Antonio Da Costa Azevedo, 1039	Jardim Brasil	Olinda	LAP 2	-8,010963	-34,872235
SECRETARIA DE EDUCAÇÃO E ESPORTES	26082179 EREM PROFº FRANCISCO JOAQUIM DE BARROS CORREIA GRE 09	Rua Barão De Contendas, S/N	Centro	Altinho	LAP 2	-8,488796	-36,057955
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042797 ESCOLA ESTADUAL INDÍGENA CABRAL GRE 13	Aldeia Espinheiro, s/n POVOPANKARARU	Zona Rural	Tacaratu	LAP 1	-9,1008627	-38,1781633
SECRETARIA DE EDUCAÇÃO E ESPORTES	26142830 ESCOLA ESTADUAL INDÍGENA SAO JOSE GRE 11	Aldeia Sao Jose, Zona Rural, Area Indigena, Pesqueira		Pesqueira	LAP 1	-8,358391	-36,698114
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111870 EREM CARDEAL DOM JAIME CAMARA GRE 04	Primeiro De Maio Nº 212	Centro	Moreno	LAP 2	-8,11977	-35,097517
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110016 EREM FREI JABOATAO GRE 04	Rua Frei Jaboatão, S/N	Jaboatão	Jaboatão dos Guararapes	LAP 1	-8,109748	-35,023079
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054027 EREM ARNALDO ASSUNCAO GRE 09	Rua Prudente De Moraes, S/N	Salgado	Caruaru	LAP 2	-8,27929	-35,959573
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020882 EREM METHODIO DE GODOY LIMA GRE 12	Br 232 - Km 414, S/N	Tancredo Neves	Serra Talhada	LAP 1	-7,981335	-38,304978
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128560 ESCOLA SAO FRANCISCO DE ASSIS - RN GRE 01	Rua São Bento, 157	Agua Fria	Recife	LAP 2	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26010151 EREM ODORICO MELO GRE 15	Av. Capitão João Lopez Machado, 43	Centro	Parnamirim	LAP 2	-8,090807	-39,581594
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075911 ESCOLA PROFª ELISA COELHO GRE 10	Rua Manoel Ouro Preto, 14	São José	Garanhuns	LAP 2	-8,886388	-36,491632
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127865 EREM PROFº CANDIDO DUARTE GRE 02	Praça Pinto Damázio S/N	Várzea	Recife	LAP 1	-8,020966	-34,938991
SECRETARIA DE EDUCAÇÃO E ESPORTES	26066220 EREM PROTAZIO SOARES DE SOUZA GRE 09	Rua Adalgiza Moura, S/N	Centro	Toritama	LAP 2	-8,006943	-36,054687
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105195 EREM BRASILINO JOSE DE CARVALHO GRE 03	Loteamento Bonfim, S/N	Cruz de Rebouças	Igarassu	LAP 2	-7,870054	-34,911368
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127334 EREM JORNALISTA TRAJANO CHACON GRE 02	Av. Do Forte, S/N	Cordeiro	Recife	LAP 2	-8,062006	-34,932153

SECRETARIA DE EDUCAÇÃO E ESPORTES	26011050 ESCOLA ANTONIO VIEIRA DE BARROS GRE 15	Rua Pimenta, S/N	Pimenta	Salgueiro	LAP 2	-8,078602	-39,114497
SECRETARIA DE EDUCAÇÃO E ESPORTES	26041529 ESCOLA ESTADUAL INDIGENA MENINO JESUS - FLORESTA GRE 13	FAZ CAPOEIRA DO BARRO	Zona Rural	Floresta	LAP 1	-8,6609582	-38,1460765
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178338 ESCOLA ESTADUAL INDIGENA SAO FRANCISCO GRE 14	ALDEIA PORTO APOLONIO SALES, S/N	ILHA TRUKA TAPERA	Orocó	LAP 1	-8,606492	-39,582582
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111853 ESCOLA ARTUR MENDONCA GRE 04	Rua Djalma Montenegro, N 140	Bela Vista	Moreno	LAP 2	-8,118835	-35,093027
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123584 ESCOLA PROFA OLINDINA ALVES SEMENTE GRE 02	Rua Paulo Afonso S/N	Barro	Recife	LAP 2	-8,088488	-34,942746
SECRETARIA DE EDUCAÇÃO E ESPORTES	26053608 EREM NOSSA SENHORA DO PERPETUO SOCORRO GRE 10	Rua Bolívia, S/N	Centro	Capoeiras	LAP 2	-8,729971	-36,62872
SECRETARIA DE EDUCAÇÃO E ESPORTES	26025981 ESCOLA GENERAL JOAQUIM INACIO GRE 11	Av. Profº Manoel Borba, 251	Centro	Custódia	LAP 2	-8,087226	-37,640393
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126109 EREM PADRE MACHADO GRE 01	Rua Major Nereu Guerra, Nº92	Casa Amarela	Recife	LAP 2	-8,025966	-34,913995
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176254 ETE JOSE NIVALDO PEREIRA RAMOS GRE 09	Rua Projetada, S/N	Santa Tereza	Santa Cruz do Capibaribe	LAP 2	-7,944894	-36,22207
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169762 ESCOLA ESTADUAL INDIGENA SAO JOSE - CARNAUBEIRA GRE 13	ALDEIA PEDRA DE FOGO	ZONA RURAL	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111314 EREM SATURNINO DE BRITO GRE 04	Estrada Da Batalha, S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,153934	-34,920667
SECRETARIA DE EDUCAÇÃO E ESPORTES	26000792 EREM PROFº MANOEL BONIFACIO COSTA GRE 16	Rua Josafá Soares, 185	Vila Santa Isabel	Arapirina	LAP 1	-7,58379	-40,500829
SECRETARIA DE EDUCAÇÃO E ESPORTES	26179997 EREM PROFª EDITE MATOS GRE 14	Rua da Independência, S/N	José Lustosa	Santa Maria da Boa Vista	LAP 2	-8,80246	-39,82532
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011115 ESCOLA ESTADUAL INDIGENA JOAQUIM VIEIRA GRE 15	Aldeia Curtume, s/n	Zona Rural	Salgueiro	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26150131 EREM PROFº PAULO FREIRE GRE 03	Av. Cel. João De Melo Moraes, S/N	Centro	Olinda	LAP 2	-7,987182	-34,851567
SECRETARIA DE EDUCAÇÃO E ESPORTES	26029243 EREM CORONEL MANOEL DE SOUZA NETO GRE 11	Rua Dom Pedro I, 85	Centro	Manari	LAP 2	-8,961366	-37,626309
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043076 ESCOLA ESTADUAL INDIGENA PANKARARUS EZEQUIEL GRE 13	BREJO DOS PADRES	POVO PANKARARU	Tacaratu	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121638 ESCOLA MONSENHOR FRANCISCO SALLES GRE 01	Oliveira Lima, 1029	Boa Vista	Recife	LAP 2	-8,056404	-34,889702
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114720 EREM PROFº ERNESTO SILVA GRE 03	End: Rua Profº Enio Carlos De Albuquerque N 133	4º Etapa De Rio Doce ,S/N-Rio Doce Et Dois	Olinda	LAP 1	-7,96365	-34,84544
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110148 ESCOLA ALFREDO TENORIO GRE 04	Travessa Sargento Bernado Foncaca de Lima, S/N		Jaboatão dos Guararapes	LAP 1	-8,168812	-34,920874
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113198 ESCOLA ANTONIO SOUTO FILHO GRE 03	Praça Do Mercado, S/N	1ª Etapa De Rio Doce	Olinda	LAP 2	-7,964341	-34,834322
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059436 ESCOLA ESTADUAL INDIGENA ELIZEU LIBERATO DA SILVA GRE 11	Aldeia Viração, s/n - Zona Rural		Pesqueira	LAP 1	-8,358339	-36,698122

SECRETARIA DE EDUCAÇÃO E ESPORTES	26096030 EREM JOAO VICENTE DE QUEIROZ GRE 07	Rua Marcianilo Pedrosa, S/N	Centro	Água Preta	LAP 2	-8,70840986	-35,52075268
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035340 EREM ANTONIO CASSIMIRO GRE 14	Avenida do Agricultor - s/n	Antônio Cassimiro	Petrolina	LAP 1	-9,372795	-40,51368
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134839 ESCOLA JUIZ ANTONIO LUIS LINS DE BARROS GRE 03	Rua Engenho São João, S/N	Centro	Ilha de Itamaracá	LAP 1	-7,768308	-34,87087
SECRETARIA DE EDUCAÇÃO E ESPORTES	26028573 EREM JOEL PEDRO DA SILVA  GRE 11	Rua Santos Dundom, S/N	Centro	Inajá	LAP 2	-8,89899946	-37,82888895
SECRETARIA DE EDUCAÇÃO E ESPORTES	26028409 ESCOLA ESTADUAL INDÍGENA MARIA GILDETE ARAUJO GRE 11	SITIO FUNIL	ZONA RURAL	Inajá	LAP 1	-8,7779	-37,89367
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176203 ETE PROFº PAULO FREIRE GRE 12	Rua projetada, S/N	Centro	Carnaíba	LAP 1	-7,806106	-37,794035
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040530 ESCOLA ESTADUAL INDÍGENA TIA AMELIA CAXIADO GRE 13	ALDEIA LAGOA SERRA DO-ARAPUA	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,3208391	-38,7424661
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122952 EREM SENADOR NILO DE SOUZA COELHO GRE 02	Avenida Recife, S/N	Areias	Recife	LAP 2	-8,094023	-34,929097
SECRETARIA DE EDUCAÇÃO E ESPORTES	26100940 EREM MIGUEL PELLEGRINO GRE 07	AVENIDA DORINHA RODRIGUES, 79	Centro	Jaqueira	LAP 2	-8,73187	-35,797036
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088282 EREM JOAQUIM OLAVO GRE 05	Av. Getúlio Vargas, S/N	São José	Carpina	LAP 2	-7,844473	-35,251095
SECRETARIA DE EDUCAÇÃO E ESPORTES	26044404 ESCOLA ESTADUAL INDÍGENA BILINGUE ANTONIO JOSE MOREIRA GRE 10	Aldeamento Indígena Fulni-O, s/n	Zona Rural	Recife	LAP 1	-9,119317	-37,122213
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124602 EREM ENGENHEIRO LAURO DINIZ GRE 02	Pca Marechal Soares D'andrea, S/N	Ipsep	Recife	LAP 2	-8,113933	-34,92185
SECRETARIA DE EDUCAÇÃO E ESPORTES	26133920 EREM PADRE ANTONIO BARBOSA JUNIOR GRE 10	Rua 1ª De Janeiro, S/N	Centro	Jurema	LAP 2	-8,71950574	-36,13568634
SECRETARIA DE EDUCAÇÃO E ESPORTES	26005107 EREM SAO SEBASTIAO - OURICURI GRE 16	Esplanada São Sebastião, 110	Centro	Ouricuri	LAP 1	-7,88657519	-40,8049459
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126052 EREM CORONEL OTHON GRE 01	Rua Ida, 0	Macaxeira	Recife	LAP 2	-8,015404	-34,928204
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525798 ETE ADERICO ALVES DE VASCONCELOS GRE 05	Loteamento Coração de Jesus, S/N	Bairro Novo	Goiana	LAP 2	-7,56416	-34,996306
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113325 EREM CLIDIO DE LIMA NIGRO GRE 03	Rua Do Cacimão, S/N -Salgadinho	Salgadinho	Olinda	LAP 1	-8,0275	-34,870421
SECRETARIA DE EDUCAÇÃO E ESPORTES	26183030 ESCOLA ESTADUAL DE MATRIZ DA LUZ GRE 04	Rua DAS PEDREIRAS, S/N	Matriz da Luz	São Lourenço da Mata	LAP 1	-8,03477461	-35,10276933
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011344 ETE PROFº URBANO GOMES DE SA GRE 15	Rua Valdemar Menezes, 940	Nossa Sra. Aparecida	Salgueiro	LAP 1	-8,07353	-39,128249

SECRETARIA DE EDUCAÇÃO E ESPORTES	26034344 ESCOLA DR DIEGO REGO BARROS GRE 14	Rua Projeto Nilo Coelho, S/N, C 2	Zona Rural	Petrolina	LAP 1	-9,3447375	40,63916664
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043505 EREM JULIA GOMES DE ARAUJO GRE 13	Largo Pedro Pereira de Araujo, 03	Caraibeiras	Tacaratu	LAP 2	-9,103833	-38,074045
SECRETARIA DE EDUCAÇÃO E ESPORTES	26012359 EREM DR WALMY CAMPOS BEZERRA GRE 15	Av. Euclides Carvalho, S/N	Centro	São José do Belmonte	LAP 2	-7,874171	-38,753549
SECRETARIA DE EDUCAÇÃO E ESPORTES	26051761 EREM CONEGO ALEXANDRE CAVALCANTI GRE 06	Av. Prof. Agamenon Magalhães, S/N	Imaculada Conceição	Bezerros	LAP 2	-8,233137	-35,744304
SECRETARIA DE EDUCAÇÃO E ESPORTES	26047187 EREM PEDRO DE ALCANTARA RAMOS GRE 11	Travessa João Martins De Oliveira, S/N	Centro	Itaíba	LAP 2	-8,950154	-37,41581
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027488 ESCOLA JOAQUIM GUEDES CORREIA GONDIM NETO GRE 11	Agrovila 1 Rua B, 78	Agrovila	Ibimirim	LAP 1	-8,54144789	37,69139189
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001594 EREM MOISES BOM DE OLIVEIRA GRE 16	Rua Projetada, S/N	Centro	Arapirina	LAP 2	-7,568721	-40,485231
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097591 EREM PROFº JOAQUIM AUGUSTO DE NORONHA FILHO GRE 07	Manoel Nogueira Mendes, S/N	Centro	Barreiros	LAP 2	-8,81364	-35,198504
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042118 ESCOLA ESTADUAL INDIGENA BARRIGUDA GRE 13	ZONA RURAL	ALDEIA BARRIGUDA	Petrolândia	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069555 ESCOLA SERAFICO RICARDO GRE 08	Rua José Cordeiro, S/N	Santo Antônio	Limoeiro	LAP 2	-7,880748	-35,457522
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034336 EREM DOM MALAN GRE 14	Av. Cardoso De Sá, S/N	Centro	Petrolina	LAP 2	-9,384205	-40,483849
SECRETARIA DE EDUCAÇÃO E ESPORTES	26179857 ETE PORTO DIGITAL GRE 02	Av. Rio Branco, Nº193	Recife Antigo	Recife	LAP 1	-8,062564	-34,873159
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087030 ESCOLA DOM BOSCO GRE 05	Rua Joao Hilario, 93	Centro	Aliança	LAP 2	-7,59901196	35,23081383
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043009 ESCOLA ESTADUAL INDIGENA SANTA CLARA GRE 13	ALDEIA BARROCAO - 0	ZONA RURAL	Tacaratu	LAP 1	-8,93384	-38,10545
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036134 EREM NÚCLEO DE MORADORES - 11 GRE 14	Rua Projeto Senador Nilo Coelho, S/N	Centro	Petrolina	LAP 2	-9,25310324	40,42263693
SECRETARIA DE EDUCAÇÃO E ESPORTES	26135555 EREM ESCRITOR PAULO CAVALCANTI GRE 03	Rua 16, 140	5ª Etapa - Rio Doce	Olinda	LAP 1	-7,956057	-34,853275
SECRETARIA DE EDUCAÇÃO E ESPORTES	26064626 EREM SEVERINO FARIAS GRE 08	Av. Severino Clemente De Arruda, 307	Centro	Surubim	LAP 2	-7,839145	-35,762372
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113724 EREM MONSENHOR ARRUDA CAMARA GRE 03	Av. Nacional, 345	Peixinhos	Olinda	LAP 2	-8,012654	-34,877163
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113929 ESCOLA RAIMUNDO DINIZ GRE 03	Estrada de Águas Compridas, S/N		Olinda	LAP 2	-7,989872	-34,898292
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107600 EREM FREI CANECA GRE 04	Belmiro Correia, S/N		Camaragibe	LAP 2	-8,022691	-34,992826
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125641 EREM JOSE VILELA GRE 01	Estrada Do Encanamento, 277	Parnamirim	Recife	LAP 1	-8,032583	-34,912835
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105187 ESCOLA BARAO DE VERA CRUZ GRE 03	1ª Travessa Jacob Pinto De Freitas S/N	Cruz De Rebouças	Igarassu	LAP 2	-7,868727	-34,9042

SECRETARIA DE EDUCAÇÃO E ESPORTES	26125072 ESCOLA LANDELINO ROCHA GRE 02	Rua Cap Rebelinho, S/N	Pina	Recife	LAP 1	-8,093094	-34,883805
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024764 ESCOLA JORNALISTA EDSON REGIS GRE 11	Rua Castro Alves, 271	São Critóvão	Arcoverde	LAP 2	-8,412456	-37,070922
SECRETARIA DE EDUCAÇÃO E ESPORTES	26055040 ESCOLA SANTO AMARO GRE 09	Rua Erminia L Dos Santos, S/N	Presidente Kennedy	Caruaru	LAP 2	-8,293217	-35,983502

SECRETARIA DE EDUCAÇÃO E ESPORTES	26049422 EREM CONEGO EMANUEL VASCONCELOS GRE 11	Rua Pedro Francisco Bezerra, 68	Centro	Venturosa	LAP 2	-8,577124	-36,87682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178656 EREM DE PANEAS GRE 09	Rodovia Pe 158, Km 1, S/N	Centro	Panelas	LAP 2	-8,679588	-36,105482
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176882 ETE PROFº JOSE LUIZ DE MENDONÇA GRE 06	R. Luís Toscano de Brito S/N	Centro	Gravatá	LAP 2	-8,205762	-35,579983
SECRETARIA DE EDUCAÇÃO E ESPORTES	26139081 EREM JOAO RODRIGUES LEITE GRE 13	VILA BARRA DO SILVA, S/N	Centro	Carnaubeira da Penha	LAP 1	-8,444202	-38,841207
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122685 ETE PROFº AGAMENON MAGALHAES - ETEPAM GRE 01	Av. João De Barros, 1769	Espinheiro	Recife	LAP 2	-8,039208	-34,892409
SECRETARIA DE EDUCAÇÃO E ESPORTES	26101084 EREM MONSENHOR ABILIO AMERICO GALVAO GRE 07	Av. José Americo De Miranda, S/N	Santa Rosa	Palmares	LAP 2	-8,679439	-35,579396
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113260 ESCOLA CARLOS GONCALVES GRE 03	Av. Professor Andrade Bezerra, 998	Peixinhos	Olinda	LAP 1	-8,029753	-34,869676
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525720 ETE MARIA EDUARDA RAMOS DE BARROS GRE 05	Av. Pe Rocha, S/N	São José	Carpina	LAP 2	-7,836702	-35,253775
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134085 EREM ALFREDO DE CARVALHO GRE 12	Av. Frei Fernando, S/N	Centro	Triunfo	LAP 2	-7,831764	-38,103615
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011506 ESCOLA ESTADUAL INDIGENA JOSE PEDRO PEREIRA GRE 15	Aldeia Massapé, s/n - Zona Rural		Salgueiro	LAP 1	-8,26315494	-38,86811696
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087910 EREM JOAO CAVALCANTI PETRIBU GRE 05	Rua Agostinho Bezerra, S/N	Centro	Carpina	LAP 2	-7,846342	-35,25747
SECRETARIA DE EDUCAÇÃO E ESPORTES	26117010 ESCOLA ESTADUAL SAO JOSE GRE 03	Av. Floresta, 130	Janga	Paulista	LAP 1	-7,932527	-34,892805
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070456 EREM PROFª RITA MARIA DA CONCEICAO GRE 08	Rua Antônio De Moura, S/N	Centro	Orobó	LAP 2	-7,754089	-35,598915
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525780 EREM GOVERNADOR MIGUEL ARRAES DE ALENCAR GRE 16	Av. SÃO PAULO, S/N	Centro	Granito	LAP 2	-7,711995	-39,618226
SECRETARIA DE EDUCAÇÃO E ESPORTES	26159422 ESCOLA ESTADUAL INDÍGENA SAO MARCOS GRE 11	Aldeia Coqueiro, s/n	Zona Rural	Buíque	LAP 1	-8,67976	-37,16873
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124432 EREM APOLONIO SALES GRE 02	Rua Prof Jose Brasileiro V Nova, 38	Ibura	Recife	LAP 2	-8,108752	-34,933897
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109042 EREM RODOLFO AURELIANO GRE 04	Praça Nossa Do Senhora Do Rosário, 665	Centro	Jaboatão dos Guararapes	LAP 1	-8,113137	-35,019488

SECRETARIA DE EDUCAÇÃO E ESPORTES	26088851 EREM AUGUSTO GONDIM GRE 05	Loteamento Coração De Jesus, S/N	Nova Goiana	Goiana	LAP 2	-7,560979	-35,012385
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033364 EREM JACOB ANTONIO DE OLIVEIRA GRE 14	Av. Prefeito Ulysses Novaes Dione, 517	Centro	Orocó	LAP 2	-8,62076701	-39,59934313
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063530 EREM SAO JOSE GRE 08	Av. Bela Vista, S/N	Centro	Frei Miguelinho	LAP 2	-7,942909	-35,926117
SECRETARIA DE EDUCAÇÃO E ESPORTES	14999999 GRE 14 - Sertão do MEDIO São Francisco / Petrolina Secret	Rua Monsenhor Ângelo Sampaio, S/N	Vila Eduardo	Petrolina	LAP 1	-9,384546	-40,489025
SECRETARIA DE EDUCAÇÃO E ESPORTES	26047837 EREM PROFº BRASILIANO DONINO DA COSTA LIMA GRE 11	Rua Jerônimo Siqueira, 20	Centro	Pedra	LAP 2	-8,50007	-36,94826
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124424 EREM PROFº MARCOS DE BARROS FREIRE GRE 02	Av. Engenho Babilônia S/N	Ur3 - Ibura	Recife	LAP 2	-8,112631	-34,947587
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043017 ESCOLA ESTADUAL INDIGENA SANTA INES DA TAPERA GRE 13	Aldeia Tapera, S/N	Povo Pankararu	Tacaratu	LAP 1	-8,93384	-38,10545
SECRETARIA DE EDUCAÇÃO E ESPORTES	26145677 EREM JUSTA BARBOSA DE SALES GRE 08	Rua Idelfonso José de Sales, S/N	Centro	Vertente do Lério	LAP 2	-7,77378233	-35,8498083
SECRETARIA DE EDUCAÇÃO E ESPORTES	26019949 EREM PROFº SEBASTIAO FERREIRA RABELO SOBRINHO GRE 12	Av. Adalberto Veras, S/N	Planalto	São José do Egito	LAP 2	-7,463405	-37,272667
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033089 ESCOLA NOSSA SENHORA DAS GRACAS - DORMENTES GRE 14	Av. Central, S/N	Lagoas	Dormentes	LAP 1	-8,441771	-40,766641
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106701 EREM PASTOR AMARO DE SENA GRE 03	Rua 07 s/N	Caetés II	Abreu e Lima	LAP 2	-8,775702	-36,624119
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091291 EREM MONSENHOR LANDELINO BARRETO LINS GRE 05	Rua 4, Vila Asa Branca, S/N	Vila Asa Branca	Paudalho	LAP 1	-7,88678362	-35,18564365
SECRETARIA DE EDUCAÇÃO E ESPORTES	26000741 EREM PADRE LUIZ GONZAGA GRE 16	Rua 11 De Setembro, 163	Centro	Araripina	LAP 2	-7,574887	-40,501681
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124653 EREM LAGOA ENCANTADA GRE 02	Rua Doutor Moacir Sales, S/N	Cohab	Recife	LAP 2	-8,123138	-34,951722
SECRETARIA DE EDUCAÇÃO E ESPORTES	26171600 EREM RURAL MANOEL GOMES DE SA GRE 13	Av. Eletrobras Norte, S/N	Centro	Jatobá	LAP 1	-9,174744	-38,247585
SECRETARIA DE EDUCAÇÃO E ESPORTES	26305615 EREM CARLOS SOARES DA SILVA GRE 08	Avenida Engenheiro Doutor José Pedrosa de Oliveira - 653	Centro	Salgadinho	LAP 1	-7,940871	-35,633327
SECRETARIA DE EDUCAÇÃO E ESPORTES	26093219 EREM JOAO BATISTA DE VASCONCELOS - CHA GRANDE GRE 06	Rua José Alves Varela, S/N	Camela	Chã Grande	LAP 2	-8,239586	-35,462939
SECRETARIA DE EDUCAÇÃO E ESPORTES	26100614 EREM FABIO DA SILVEIRA BARROS GRE 07	Rua 11 De Novembro, 145	Centro	Maraial	LAP 2	-8,784498	-35,808645
SECRETARIA DE EDUCAÇÃO E ESPORTES	26047365 ESCOLA FREI JOAO PEREIRA DE SOUZA GRE 11	Rua Major Antonio Inacio, S/N	Distrito de Itaíba	Itaíba	LAP 1	-8,98826	-37,487099

SECRETARIA DE EDUCAÇÃO E ESPORTES	26008467 ESCOLA CORONEL CHICO ROMAO GRE 15	Rua Sta Terezinha, 260	Centro	Moreilândia	LAP 1	-7,630088	-39,550675
SECRETARIA DE EDUCAÇÃO E ESPORTES	26149907 EREM JUAZEIRO GRE 13	Povoado agrovila 9 bloco 2, S/N	Centro	Tacaratu	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031914 EREM SENADOR PAULO GUERRA GRE 14	Av. Brigida Deaalencar, S/N	Centro	Cabrobó	LAP 1	-8,508716	-39,310499
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129094 EREM CONDE PEREIRA CARNEIRO GRE 04	Oito De Maio, 223	Centro	São Lourenço da Mata	LAP 2	-7,995636	-35,03555
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185938 ETE EDSON MORORÓ MOURA GRE 09	Rua Inhumas, S/N	Bom Conselho	Belo Jardim	LAP 2	-8,332985	-36,429672
SECRETARIA DE EDUCAÇÃO E ESPORTES	26062836 EREM JOAQUIM RIBEIRO DA ROCHA GRE 09	Rua Rodolfo Torres, S/N	Cabugá	São Caetano	LAP 1	-8,32400824	-36,13374817
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124807 ESCOLA PROFª JOSÉ VICENTE BARBOSA GRE 02	Pca Aleixo De Oliveira, 0	Ipsep	Recife	LAP 2	-8,112818	-34,92459
SECRETARIA DE EDUCAÇÃO E ESPORTES	26010607 ESCOLA EUCLIDES DA CUNHA GRE 15	Rua Agamenon Magalhães, 24	Centro	Parnamirim	LAP 2	-8,090953	-39,579245
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169193 EREM TEOTONIO CORREIA DA SILVA GRE 07	Rua do comercio, S/N	Ibiratinga	Sirinhaém	LAP 1	-8,522248	-35,259457
SECRETARIA DE EDUCAÇÃO E ESPORTES	26174570 ESCOLA ESTADUAL PIO XII GRE 04	TELEMACO BORBA - s/n		Camaragibe	LAP 2	-8,020454	-34,989989
SECRETARIA DE EDUCAÇÃO E ESPORTES	12999999 GRE 12 - Sertão do Alto Pajeú / Afogados da Ingazeira Secret	Av. Arthur Padilha, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,747791	-37,634762
SECRETARIA DE EDUCAÇÃO E ESPORTES	26073498 EREM LUIZ PEREIRA JUNIOR GRE 10	Rua Professor Miriam Solto Maior, 45	Centro	Caetés	LAP 2	-8,777292	-36,622693
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035316 EREM JORNALISTA JOAO FERREIRA GOMES GRE 14	Rua Dom Tomaz, S/N	COHAB São Francisco	Petrolina	LAP 2	-9,398888	-40,545083
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107627 ESCOLA JOAQUIM AMANONAS GRE 04	Rua Teófilo de Melo S/N	Novo centro	Camaragibe	LAP 2	-8,021759	-34,980069
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011611 EREM CARLOS PENA FILHO GRE 15	Av. Getúlio Vargas, 326	Centro	Salgueiro	LAP 2	-8,072963	-39,129856
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054019 EREM ANTONIA CAVALCANTI DE ALBUQUERQUE GRE 09	Rua Manaus, S/N	São Francisco	Caruaru	LAP 2	-8,287441	-35,978312
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116316 EREM PROFª AMARINA SIMOES GRE 03	Praça Republica, 0 Nobre, S/N	Nobre	Paulista	LAP 2	-7,937246	-34,872359
SECRETARIA DE EDUCAÇÃO E ESPORTES	26061023 EREM NOSSA SENHORA DE FATIMA GRE 11	Praça Prefeito Antônio Cordeiro de Souza, S/N	Centro	Sanharó	LAP 2	-8,35784651	-36,56498586
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088258 ESCOLA ALUISIO GERMANO GRE 05	Rua 1, Casa 5 E 6, S/N	Bairro Novo	Carpina	LAP 2	-7,848795	-35,24056
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115913 EREM DR LUIZ CABRAL DE MELO GRE 03	Rua Vinte E Sete, S/N	Maranguape Dois	Paulista	LAP 2	-7,933664	-34,856295
SECRETARIA DE EDUCAÇÃO E ESPORTES	26053756 CENTRO DE REABILITAÇÃO E EDUCAÇÃO ESPECIAL ROTARY CLUB GRE 09	Av. Dom Bosco, 696	Maurício de Nassau	Caruaru	LAP 1	-8,274246	-35,967823

SECRETARIA DE EDUCAÇÃO E ESPORTES	26179610 EREM NOBREGA GRE 01	Estrada De Belém, 257	Encruzilhada	Recife	LAP 2	-8,035587	-34,88912
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088037 ESCOLA PAULA FRASSINETTI GRE 05	Rua José Nazário Coutinho, 100	Bairro novo	Carpina	LAP 1	-7,845672	-35,240427
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020971 EREM CORNELIO SOARES  GRE 12	Rua Joaquim Godoy, 339	Nossa Sra. da Penha	Serra Talhada	LAP 2	-7,990582	-38,295613
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122545 ESCOLA DOM CARLOS COELHO - RECIFE GRE 01	Rua Mal Deodoro, 626	Encruzilhada	Recife	LAP 1	-8,036056	-34,883172
SECRETARIA DE EDUCAÇÃO E ESPORTES	26108984 EREM POETA MAURO MOTA GRE 04	Rua Arthur Xavier, S/N - Socorro	Jaboatão	Jaboatão dos Guararapes	LAP 1	-8,102609	-34,99697
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999905 BIBLIOTECA PUBLICA DE PERNAMBUCO Secret	Rua Joao Lira, S/N	Santo Amaro	Recife	LAP 1	-8,05564	-34,88058
SECRETARIA DE EDUCAÇÃO E ESPORTES	26112108 EREM SOFRONIO PORTELA GRE 04	Rua Educadora Brandina Rocha, S/N	Centro	Moreno	LAP 2	-8,11888	-35,105381
SECRETARIA DE EDUCAÇÃO E ESPORTES	26016729 EREM DARIO GOMES DE LIMA GRE 12	Rua Getulio Vargas, S/N	Centro	Flores	LAP 1	-7,86388	-37,974915
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176246 ETE ALCIDES DO NASCIMENTO LINS GRE 04	Avenida General Newton Cavalcante, S/N	Camaragibe	Camaragibe	LAP 2	-8,017136	-34,971266
SECRETARIA DE EDUCAÇÃO E ESPORTES	26032325 ESCOLA ESTADUAL INDIGENA BERTO CIRILO DOS SANTOS GRE 14	Ilha Assunção, S/N	Aldeia Pambuzinho	Cabrobó	LAP 1	-8,45577	-39,40359
SECRETARIA DE EDUCAÇÃO E ESPORTES	26092786 EREM PADRE GUEDES GRE 05	Rua Dr. Manuel Borba, S/N	Centro	Vicência	LAP 2	-7,656494	-35,322898
SECRETARIA DE EDUCAÇÃO E ESPORTES	26014572 EREM CONEGO JOAO LEITE GONÇALVES DE ANDRADE GRE 12	Rua Antônio Rafael De Freitas, S/N	Centro	Afogados da Ingazeira	LAP 1	-7,745413	-37,63874
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059460 ESCOLA ESTADUAL INDÍGENA JOAQUIM MOTA VALENÇA - GRE 11	Aldeia Imbe, zona rural - Pesqueira/PE		Pesqueira	LAP 1	-8,283791	-36,819224
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042312 EREM SAO FRANCISCO GRE 13	Projeto Apolonio Sales, S/N	Matriz	Petrolândia	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26095530 EREM PROFª EUDÓXIA DE ALCÂNTARA FERREIRA GRE 06	Rua Eurico Valuar, S/N	Mauses	Vitória de Santo Antão	LAP 2	-8,118031	-35,306889
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097982 EREM PRESIDENTE TANCREDO NEVES GRE 07	Rodovia Pe 123, S/N	Zona Rural	Belém de Maria	LAP 2	-8,627708	-35,838509
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113880 EREM PROFª INÊS BORBA GRE 03	Rua: Santana, Nº 133	Jardim Atlantico	Olinda	LAP 1	-7,972531	-34,836817
SECRETARIA DE EDUCAÇÃO E ESPORTES	02999999 GRE 02 - Recife Sul Secret	Av. Academico Helio Ramos, 500	Várzea	Recife	LAP 2	-8,050491	-34,955208
SECRETARIA DE EDUCAÇÃO E ESPORTES	02999999 GRE 02 - Recife Sul Secret	Av. Academico Helio Ramos, 500	Várzea	Recife	LAP 1	-8,05031212	-34,95521921

SECRETARIA DE EDUCAÇÃO E ESPORTES	26109115 ESCOLA SOUZA BRANDAO GRE 04	Rua Manoel Rabelo, Nº 1.	Centro	Jaboatão dos Guararapes	LAP 2	-8,103541	-34,974708
SECRETARIA DE EDUCAÇÃO E ESPORTES	26017750 EREM PROFª ROSETE BEZERRA DE SOUZA GRE 12	Rua Ne Santana, S/N	Centro	Iguaraci	LAP 2	-7,836603	-37,514399
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058502 ESCOLA ESTADUAL INDÍGENA OLAVO BILAC GRE 11	Aldeia Sao Jose, Zona Rural, Area Indigena		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26030950 ESCOLA ANTONIO CAVALCANTI FILHO GRE 14	Av. FRANCISCO RODRIGUES, S/N	Centro	Afrânio	LAP 2	-8,516231	-41,006143
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036207 ESCOLA ÉRIKA THAYNARA DA SILVA LEITE GRE 14	Rua E, S/N	Areia Branca	Petrolina	LAP 1	-9,385576	-40,492947
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040581 ESCOLA ESTADUAL INDIGENA GOV ESTACIO COIMBRA GRE 13	ALDEIA SEDE SERRA UMA	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26019825 EREM EDSON SIMOES GRE 12	Rua Marechal Rondon, S/N	Centro	São José do Egito	LAP 2	-7,47535118	37,27571483
SECRETARIA DE EDUCAÇÃO E ESPORTES	26046210 ESCOLA ESTADUAL INDÍGENA BARAO DO RIO BRANCO GRE 11	SITIO PONTA DE VARZEA	ZONA RURAL	Buíque	LAP 1	-8,67976	-37,16873
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126443 EREM NOSSA SENHORA DE FATIMA GRE 01	TRAVESSA ESTRADA DA MUMBECA, S/N	GUABIRABA	Recife	LAP 1	-7,95147	-34,96122
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169223 ESCOLA ESTADUAL DR CAETANO MONTEIRO GRE 07	Rua Professor Aurino Niceia, 21	Centro	Rio Formoso	LAP 1	-8,659683	-35,153627
SECRETARIA DE EDUCAÇÃO E ESPORTES	26048337 EREM JOSE EMILIO DE MELO GRE 11	Rua Jardim Santa Clara, S/N	Centro	Tupanatinga	LAP 2	-8,753213	-37,343249
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122227 EREM GOVERNADOR BARBOSA LIMA GRE 01	Rua Joaquim Nabuco, S/N	Graças	Recife	LAP 2	-8,052634	-34,896597
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122677 EREM SANTA PAULA FRASSINETTI GRE 01	Rua Gomes Pacheco, S/N	Espinheiro	Recife	LAP 1	-8,040725	-34,888225
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036037 ESCOLA PROFª SIMAO AMORIM DURANDO GRE 14	Rua Tangerina S/N	Rio Corrente	Petrolina	LAP 2	-9,39946	-40,502356
SECRETARIA DE EDUCAÇÃO E ESPORTES	26096358 EREM JOAO VICENTE DE QUEIROZ - USINA GRE 07	Rua Da Praça, S/N	Centro	Água Preta	LAP 1	-8,829294	-35,563204
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116359 ESCOLA PROFª JOSE BRASILEIRO VILA NOVA GRE 03	Rua Honorato Fernandes Da Paz, S/N	Janga	Paulista	LAP 2	-7,917884	-34,828148
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036266 ESCOLA SAO JOSE - PETROLINA GRE 14	Rua A, S/N	Centro	Petrolina	LAP 1	-9,399922	-40,529089
SECRETARIA DE EDUCAÇÃO E ESPORTES	26067382 EREM JUSTULINO FERREIRA GOMES GRE 08	SITIO UMARI, S/N	Zona Rural	Bom Jardim	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089530 ESCOLA ARRUDA CAMARA GRE 05	Praça Maria José Sá De Andrade, 25	Centro	Itambé	LAP 2	-7,404505	-35,114946
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109506 EREM HENRIQUETA DE OLIVEIRA GRE 04	Estrada Da Luz, S/N	Santaleixo	Jaboatão dos Guararapes	LAP 2	-8,101103	-35,019842

SECRETARIA DE EDUCAÇÃO E ESPORTES	26011018 EREM PROFª MARIA DA CONCEICAO CISNEIRO SAMPAIO GRE 15	Br 232, S/N	Nossa Senhora da Conceição	Salgueiro	LAP 2	-8,06781064	39,14157596
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040476 ESCOLA ESTADUAL INDIGENA OLIMPIO PEREIRA GRE 13	Aldeia Mingu, s/n	Zona Rural	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26041200 EREM TRES MARIAS GRE 13	Rua Sete, S/N	Cohab	Floresta	LAP 2	-8,597911	-38,581884
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107074 EREM PROFª AZINETE RAMOS CARNEIRO GRE 03	Rua 43 S/N	Caetés Iii	Abreu e Lima	LAP 2	-7,918	-34,907855
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001896 ESCOLA VITALINA MARIA DE JESUS GRE 16	Rua duque de caxias, S/N	Centro	Arapirina	LAP 1	-7,57501479	40,49792578
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027984 ESCOLA ESTADUAL INDIGENA CASTELO BRANCO GRE 11	Sítio Carabeirinha	Área Indígena Kambiawá	Inajá	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26188554 ETE FRANCISCO DE MATOS SOBRINHO (ETE DE BOM CONSELHO) GRE 10	Rodovia PE-218, KM 14, S/N	Centro	Bom Conselho	LAP 2	-9,158265	-36,692275
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059002 ESCOLA ESTADUAL INDIGENA PEDRO QUINQUIM DE ESPÍNDOLA GRE 11	ALDEIA CAJUEIRO	ZONA RURAL	Pesqueira	LAP 1	-8,36273	-36,73885
SECRETARIA DE EDUCAÇÃO E ESPORTES	26019493 EREM SANTA TEREZINHA GRE 12	Rua José Romão De Araujo, S/N	Centro	Santa Terezinha	LAP 2	-7,378445	-37,479112
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186411 ESCOLA ESTADUAL INDIGENA JOSEFA ALICE DA CONCEICAO GRE 13	Aldeia Serrote dos Campos - S/N	Território Indígena do Povo Pankará	Itacuruba	LAP 1	-8,738494	-38,714912
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116634 EREM PROFª MARIA DO CARMO PINTO RIBEIRO GRE 03	Rua 108, S/N	Jardim Paulista Baixo	Paulista	LAP 1	-7,878618	-34,834376
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087715 EREM PEDRO TAVARES GRE 05	Rua Agamenon Magalhães, 152	Centro	Camutanga	LAP 2	-7,40649419	35,27410574
SECRETARIA DE EDUCAÇÃO E ESPORTES	26155559 EREM DOM HELDER CAMARA GRE 14	Rua Evangélica, S/N	Centro	Lagoa Grande	LAP 2	-8,0390177	34,88834236
SECRETARIA DE EDUCAÇÃO E ESPORTES	26181282 ETE JOSE ALENCAR GOMES DA SILVA GRE 03	Rua João Francisco Batista, 170	Janga	Paulista	LAP 2	-7,942087	-34,826206
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059185 ESCOLA ESTADUAL INDIGENA PROFESSOR JOSE CARLOS DE LIMA GRE 11	Aldeia Curral Velho, Zona Rural - Pesqueira/PE		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26102633 EREM PADRE AMERICO NOVAIS  GRE 07	Rua Joaquin Nabuco, 162	Centro	Ribeirão	LAP 2	-8,511732	-35,375681
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525933 ETE ARLINDO FERREIRA DOS SANTOS  GRE 11	Rua Luiz Cajueiro de Albuquerque, S/N	Centro	Sertânia	LAP 1	-8,064624	-37,286759
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125757 EREM PROFº CANDIDO DUARTE GRE 01	Rua Dois Irmão, 2727	Apipucos	Recife	LAP 1	-8,016109	-34,944969
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097354 EREM CRISTIANO BARBOSA E SILVA GRE 07	Rua Antonio F Miranda, S/N	Centro	Barreiros	LAP 1	-8,814592	-35,202128
SECRETARIA DE EDUCAÇÃO E ESPORTES	26080516 EREM MONSENHOR JOAO MARQUES GRE 10	CONJUNTO HABITACIONAL JOSE ALVEZ BEZERRA, S/N	Centro	Saloá	LAP 2	-8,98189319	36,69037027
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124440 EREM ASSIS CHATEAUBRIAND GRE 02	Rua Francisco Valpasso, 0	Brasília Teimosa	Recife	LAP 2	-8,086599	-34,88267
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126575 ESCOLA PADRE JOAO BARBOSA GRE 01	Rua Conceição S/N	Morro Da Conceição	Recife	LAP 1	-8,019579	-34,914201

SECRETARIA DE EDUCAÇÃO E ESPORTES	26155567 ESCOLA PROFª JOSEFINA GOMES ARAUJO GRE 14	Rua da Pista, S/N	Centro	Lagoa Grande	LAP 1	-8,635233	-40,241067
SECRETARIA DE EDUCAÇÃO E ESPORTES	26078805 EREM DEOLINDA AMARAL GRE 10	Av. Agamenon Magalhães, 309	Lajedo	Lajedo	LAP 2	-8,662155	-36,32075
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087928 EREM JOSE DE LIMA JUNIOR GRE 05	Av. Agamenon Magalhães, S/N	São José	Carpina	LAP 2	-7,842952	-35,255427
SECRETARIA DE EDUCAÇÃO E ESPORTES	26056658 EREM DEVALDO BORGES GRE 06	Av. Joaquim Didier, 153	Cruzeiro	Gravatá	LAP 2	-8,205326	-35,569933
SECRETARIA DE EDUCAÇÃO E ESPORTES	26101599 ESCOLA PROFª ELISEU PEREIRA DE MELO GRE 07	Rua Manuel Leandro, 477	Santo Onofre	Palmares	LAP 1	-8,679817	-35,58947
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031469 ESCOLA ESTADUAL INDIGENA JOAO ALBERTO MACIEL GRE 14	Aldeia Alto do Gavião, s/n	Ilha da Assunção	Cabrobó	LAP 1	-8,50644289	39,42895633
SECRETARIA DE EDUCAÇÃO E ESPORTES	26120992 EREM LICEU DE ARTES E OFICIOS GRE 01	Rua Oliveira Lima, Nº824	Boa Vista	Recife	LAP 2	-8,057368	-34,887166
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091836 ESCOLA PROFª ELISABETH LYRA GRE 05	Rua João Veiga, 48	Centro	Timbaúba	LAP 2	-7,514589	-35,316864
SECRETARIA DE EDUCAÇÃO E ESPORTES	26153688 CENTRO DE ATENDIMENTO EDUCACIONAL ESPECIALIZADO DO RECIFE  GRE 01	Rua Conselheiro Nabuco S/N	Casa Amarela	Recife	LAP 1	-8,028251	-34,918559
SECRETARIA DE EDUCAÇÃO E ESPORTES	26158531 CENTRO DE EDUC. INFANTIL BEM-ME-QUER  GRE 01	Br- 363, S/N	Vila dos Remédios	Fernando de Noronha	LAP 1	-3,849111	-32,417495
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125986 ESCOLA ANA MALTA DA COSTA AZEVEDO GRE 01	Rua Padre Oliveira	Alto José Do Pinho	Recife	LAP 1	-8,018924	-34,910018
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040387 ESCOLA ESTADUAL INDIGENA JOAO LIMA GRE 13	ALDEIA AREIA DOS PEDROS	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113449 EREM DOM PEDRO BANDEIRA DE MELO GRE 03	Rua Do Pêssego - S/N - 5ª Etapa	Rio Doce	Olinda	LAP 2	-7,961449	-34,850934
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122987 ESCOLA CARMELA DUTRA GRE 02	Rua Gen Souza Doca, 0	Afogados	Recife	LAP 2	-8,078627	-34,914487
SECRETARIA DE EDUCAÇÃO E ESPORTES	26066572 EREM GIL RODRIGUES GRE 08	Coronel Braz Bezerra, 188	Centro	Vertentes	LAP 2	-7,903801	-35,984286
SECRETARIA DE EDUCAÇÃO E ESPORTES	26043335 EREM JOAO BATISTA DE VASCONCELOS - TACARATU GRE 13	Rua Corrego Frederico, S/N	Centro	Tacaratu	LAP 2	-9,106253	-38,150251
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040468 ESCOLA ESTADUAL INDIGENA OLHO DAGUA DO PADRE GRE 13	ALDEIA OLHO DAGUA DO PADRE	ZONA RURAL	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999902 SULOG - GALPÃO CONE MULTIMODAL Secret	AV. GOV. MIGUEL ARRAES DE ALENCAR, 1380	PONTE DOS CARVALHOS	Cabo de Santo Agostinho	LAP 1	-8,28896	-35,019745
SECRETARIA DE EDUCAÇÃO E ESPORTES	26132790 ESCOLA PROFª MARIA BERNADETE MARINS DE BRITO GRE 15	Rua Getúlio Vargas, 326	Nossa Sra. Aparecida	Salgueiro	LAP 2	-8,074349	-39,12962

SECRETARIA DE EDUCAÇÃO E ESPORTES	26189585 ETE PASTOR ISAAC MARTINS RODRIGUES GRE 03	Rua do Cajueiro S/N	Centro	Abreu e Lima	LAP 1	-7,908841	-34,897615
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090309 EREM TRISTAO FERREIRA BESSA GRE 08	Rua 21 de Abril	Centro	Lagoa do Itaenga	LAP 2	-7,927814	-35,295075
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186438 ESCOLA ESTADUAL INDIGENA MESTRE OTAVIANO GRE 13	Aldeia São Gonçalo	Povo Pankará	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26117045 EREM DANTAS BARRETO GRE 03	Av Palmares, 0	Arthur Lundgren Um	Paulista	LAP 2	-7,934701	-34,888326
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178028 EREM DE IPOJUCA GRE 04	Rua Do Colegio S/N	Centro Ipojuca	Ipojuca	LAP 2	-8,439682	-35,012363
SECRETARIA DE EDUCAÇÃO E ESPORTES	26068729 EREM JARINA MAIA GRE 08	Rua Maria Eliete Soares, S/N	Boa Vista	João Alfredo	LAP 2	-7,858548	-35,589306
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178176 EREM DE TIMBAUBA PROFº ANTONIO JOSE BARBOZA DOS SANTOS GRE 05	Rua Manoel Xavier De Andrade, S/N	Centro	Timbaúba	LAP 2	-7,515633	-35,310299
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027186 ESCOLA ESTADUAL INDÍGENA PEDRO FERREIRA DE QUEIROZ GRE 11	ALD NAZARIO KAMBIWA, S/N	Zona Rural	Ibimirim	LAP 1	-8,636941	-37,807601
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123525 EREM MARCELINO CHAMPAGNAT GRE 02	Rua Rivadávia Guerra, Nº 55	Tejipió	Recife	LAP 2	-8,089713	-34,95232
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126044 EREM CLOTILDE DE OLIVEIRA GRE 01	Av Norte, 6760	Vasco Da Gama	Recife	LAP 2	-8,02061	-34,925645
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128101 EREM DE BEBERIBE GRE 01	Rua Uriel de Holanda, 219	Beberibe	Recife	LAP 1	-8,004469	-34,899355
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035553 ESCOLA ESTADUAL DE APLICAÇÃO PROFª VANDE DE SOUZA FERREIRA GRE 14	Br-203, Km-02, S/N	Campus Universitário	Petrolina	LAP 2	-9,397292	-40,478975
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075687 EREM DOM JOAO DA MATA AMARAL GRE 10	VI Ipiranga, S/N	Boa vista	Garanhuns	LAP 2	-8,904845	-36,498251
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169029 EREM RAIMUNDO DE CASTRO FERREIRA GRE 16	Rua Projetada, 1	Centro	Santa Filomena	LAP 2	-8,161572	-40,613228
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070090 EREM SEVERINO DE ANDRADE GUERRA GRE 08	Rua Antônio Albuquerque, 251	Centro	Machados	LAP 2	-7,686157	-35,512124
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063280 ESCOLA FRANCISCO DE ASSIS BARROS GRE 09	Av. Major João Gomes, S/N	Centro	Tacaimbó	LAP 1	-8,320751	-36,290092
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040794 ESCOLA ESTADUAL INDIGENA NOSSA SENHORA DE FATIMA - CARNAUBEIRA GRE 13	ALDEIA AGUA GRANDE	ZONA RURAL	Inajá	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26039702 EREM TERCINA RORIZ GRE 13	Av. Coronel Caribé, 132	Centro	Belém de São Francisco	LAP 2	-8,758057	-38,965745
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035049 EREM PADRE MANOEL DE PAIVA NETTO GRE 14	Rua 10, S/N- Jardim Amazonas, S/N	Jardim Amazonas	Petrolina	LAP 2	-9,379155	-40,529851
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125250 EREM PROFº FERNANDO MOTA GRE 02	Rua Copacabana, S/N	Setúbal	Recife	LAP 2	-8,135888	-34,914436

SECRETARIA DE EDUCAÇÃO E ESPORTES	99999908 C.A.P. DEFICIENTE VISUAL SEDE-ANEXO GRE 01	Rua Conselheiro Nabuco, S/N	Heliópolis	Recife	LAP 1	-8,029551	-34,916357
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127539 ESCOLA PROFª FONTAINHA DE ABREU GRE 02	Rua Antonio Carlos S/N	Cordeiro	Recife	LAP 2	-8,051806	-34,937382
SECRETARIA DE EDUCAÇÃO E ESPORTES	26108925 EREM NESTOR GOMES DE MOURA GRE 04	Boa Esperança, SN	Vila Rica	Jaboatão dos Guararapes	LAP 2	-8,145286	-34,933262
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009323 EREM VALDICLEWTON DA SILVA MENEZES GRE 15	Rua Campos, 873	São gonçalo	Cedro	LAP 1	-7,71961723	-39,23797371
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129132 ESCOLA DR LEONCIO GOMES DE ARAUJO GRE 04	RUA FELINTO ALVES SN LOT BELA VISTA	BAIRRO CAPIBARRIBE	São Lourenço da Mata	LAP 1	-8,014722	-35,015982
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088410 EREM ANTONIO CORREIA DE OLIVEIRA ANDRADE GRE 05	Av. 15 De Novembro, 888	Centro	Condado	LAP 2	-7,587694	-35,097645
SECRETARIA DE EDUCAÇÃO E ESPORTES	07999999 GRE 07 - Mata Sul / Palmares Secret	Av. Abel Fraga, S/N	São José	Palmares	LAP 1	-8,685751	-35,597594
SECRETARIA DE EDUCAÇÃO E ESPORTES	26174464 EREM HENRIQUE JUSTINO DE MELO GRE 10	Rua Nova, S/N	Centro	Jucati	LAP 2	-8,70727384	-36,48236786
SECRETARIA DE EDUCAÇÃO E ESPORTES	26000261 ESCOLA DA INDEPENDENCIA GRE 16	Rua Arno Campos, 206	Centro	Araripina	LAP 1	-7,57669387	-40,50140068
SECRETARIA DE EDUCAÇÃO E ESPORTES	26016540 EREM AIRES GAMA GRE 12	Rua Cleto Capelo, 51	Centro	Flores	LAP 1	-7,863503	-37,972589
SECRETARIA DE EDUCAÇÃO E ESPORTES	26064030 EREM MALAQUIAS CARDOSO ARAGAO GRE 09	Av. Teofanes F. Torres Fo, S/N	Malaquias	Santa Cruz do Capibaribe	LAP 1	-7,957088	-36,198679
SECRETARIA DE EDUCAÇÃO E ESPORTES	26366614 EREM JOSE DO PATROCINIO MOTA GRE 10	Rua Nelita Cintra, S/N	Loteamento Menino Jesus de Praga	São Bento do Una	LAP 2	-8,52733877	-36,4409803
SECRETARIA DE EDUCAÇÃO E ESPORTES	26117916 CENTRO EJA POETA JOAQUIM CARDOZO GRE 02	Av Dr José Rufino, N.º 3071	Tejipió	Recife	LAP 2	-8,091688	-34,950016
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040697 ESCOLA ESTADUAL INDIGENA COSME E DAMIAO GRE 13	Aldeia Carqueja, s/n	Zona Rural	Carnaubeira da Penha	LAP 1	-8,452262	-38,676531
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087022 EREM CORONEL LUIZ IGNACIO PESSOA DE MELO GRE 05	Rua Alto Santa Luzia, S/N	Centro	Aliança	LAP 2	-7,597655	-35,23088
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011883 ESCOLA PROFª MANUEL LEITE GRE 15	Av. Agamenon Magalhaes, 636	Centro	Salgueiro	LAP 2	-8,07035	-39,120107
SECRETARIA DE EDUCAÇÃO E ESPORTES	26413817 EREM TORQUATO DE CASTRO GRE 04	Estrada de Aldeia - Km: 12.5 - N.º100		Camaragibe	LAP 2	-7,953051	-35,020342
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035251 ESCOLA FRANCISCO XAVIER DOS SANTOS GRE 14	Rua B, S/N	Projeto Senador Nilo Coelho	Petrolina	LAP 1	-9,310181	-40,587706
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121891 ESCOLA JOSE MARIA GRE 01	Rua 13 De Maio, S/N	Sto Amaro	Recife	LAP 2	-8,050031	-34,882046
SECRETARIA DE EDUCAÇÃO E ESPORTES	26133985 EREM REGINA PACIS GRE 12	Rua Manoel da Cruz, 175	Centro	Santa Cruz da Baixa Verde	LAP 2	-7,8211679	-38,14750359
SECRETARIA DE EDUCAÇÃO E ESPORTES	26025175 EREM NOE NUNES FERRAZ GRE 11	Rua Um Cohab li, S/N	Santos Dumont	Arcoverde	LAP 1	-8,411625	-37,078578

SECRETARIA DE EDUCAÇÃO E ESPORTES	26065568 EREM JOAO XXIII GRE 08	Rua João 23, S/N	Centro	Casinhas	LAP 2	-7,7431231	35,72295023
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075768 EREM HENRIQUE DIAS GRE 10	Rua Pedro Rocha, 296	Heliópolis	Garanhuns	LAP 1	-8,885561	-36,485923
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127695 EREM JOAQUIM XAVIER DE BRITO GRE 02	Rua Cordilândia, 1120	Ipatinga	Recife	LAP 2	-8,041764	-34,931485
SECRETARIA DE EDUCAÇÃO E ESPORTES	26146991 ESCOLA ESTADUAL INDIGENA JULIO JOSE DA SILVA GRE 13	ALDEIA RIACHO GRANDE	ZONA RURAL	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129388 EREM PROFº AGAMENOM MAGALHAES GRE 04	Rua: Dr. Marcos Pessoa Guerra, S/N	Capibaribe	São Lourenço da Mata	LAP 2	-7,997222	-35,02886
SECRETARIA DE EDUCAÇÃO E ESPORTES	26023245 EREM ARNALDO ALVES CAVALCANTI GRE 12	Rua Genesia Masenas Veras, 42	Centro	Tabira	LAP 2	-7,58823	-37,537636
SECRETARIA DE EDUCAÇÃO E ESPORTES	26131692 EREM JOSE MARIO ALVES DA SILVA GRE 04	Praia De Porto De Galinhas, S/N	Centro	Ipojuca	LAP 2	-8,508723	-35,000453
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128527 ESCOLA ROTARY DO ALTO DO PASCOAL GRE 01	Rua Colegio, S/N	Agua Fria	Recife	LAP 2	-8,017218	-34,896899
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185768 ETE LUIZ ALVES LACERDA GRE 04	Rodovia BR 101 sul, SN		Cabo de Santo Agostinho	LAP 2	-8,3289	-35,106843
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178222 EREM DOS PALMARES DOM ACACIO RODRIGUES ALVES GRE 07	Rua Agamenon Magalhães, S/N	São José	Palmares	LAP 2	-8,673866	-35,589653
SECRETARIA DE EDUCAÇÃO E ESPORTES	26003066 EREM BARAO DE EXU GRE 16	Rua Coronel Zuza Saraiva, S/N	Centro	Exu	LAP 2	-7,511911	-39,721952
SECRETARIA DE EDUCAÇÃO E ESPORTES	26078562 EREM ABILIO MONTEIRO GRE 10	Rua João Monteiro, S/N	Centro	Lagoa do Ouro	LAP 2	-9,126775	-36,456765
SECRETARIA DE EDUCAÇÃO E ESPORTES	26051176 EREM EURICO QUEIROZ GRE 06	Av. Francisca De Moraes Lemos, S/N	São Pedro	Bezerros	LAP 2	-8,241496	-35,757066
SECRETARIA DE EDUCAÇÃO E ESPORTES	26101610 ESCOLA MAQUINISTA AMARO MONTEIRO GRE 07	Rua do Eucalipto, S/N	Bom Destino	Palmares	LAP 1	-8,677494	-35,597343
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110849 ESCOLA ALTO DOS GUARARAPES GRE 04	Av. Barreto De Menezes, S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,161465	-34,926897
SECRETARIA DE EDUCAÇÃO E ESPORTES	26187965 ETE PROFª MARIA WILZA BARROS DE MIRANDA GRE 14	Rua Natália Joana Alves, S/N	João de Deus	Petrolina	LAP 2	-9,361902	-40,543211
SECRETARIA DE EDUCAÇÃO E ESPORTES	26081059 EREM JOAO FERNANDES DA SILVA  GRE 10	Av. Joaquim Ferreira Santos, S/N	Centro	São João	LAP 2	-8,875221	-36,366189
SECRETARIA DE EDUCAÇÃO E ESPORTES	26021900 EREM SOLIDONIO LEITE GRE 12	Rua Francisca Godoi, S/N	Centro	Serra Talhada	LAP 2	-7,983107	-38,295369
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178087 EREM CABO DE SANTO AGOSTINHO GRE 04	Rua Luis Pereira Da Paz, S/N	Ponte Dos Carvalhos	Cabo de Santo Agostinho	LAP 2	-8,240678	-34,979318

SECRETARIA DE EDUCAÇÃO E ESPORTES	26108801 EREM FREI ROMEU PEREA GRE 04	Rua 14 S/N	Curado I	Jaboatão dos Guararapes	LAP 2	-8,083233	-34,983456
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121921 EREM SIZENANDO SILVEIRA GRE 01	Av. Jorn Mario Melo	Santo Amaro	Recife	LAP 2	-8,055608	-34,879141
SECRETARIA DE EDUCAÇÃO E ESPORTES	26013185 EREM PROFº MANOEL DE QUEIROZ GRE 15	Alto Da Boa Vista, S/N	Centro	São José do Belmonte	LAP 2	-7,869778	-38,765418
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129868 ETE EPITACIO PESSOA  GRE 04	Av. Historiador Pereira Da Costa, 820		Cabo de Santo Agostinho	LAP 2	-8,281013	-35,030427
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088886 EREM DR JOAO ALFREDO  GRE 05	Praça Duque De Caxias, 742	Centro	Goiana	LAP 2	-7,561875	-34,998958
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054825 ESCOLA PROFª JESUINA PEREIRA RÉGO GRE 09	Loteamento São João da Escócia, S/N	Salgado	Caruaru	LAP 2	-8,267597	-35,953331
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127571 EREM BARROS CARVALHO GRE 02	Rua Honório Correia, 167	Próx. ao Hospital Getúlio Vargas	Recife	LAP 2	-8,052681	-34,921264
SECRETARIA DE EDUCAÇÃO E ESPORTES	26177927 ESCOLA MALAQUIAS MENDES DA SILVA GRE 14	Av. Central, S/N	Povoado de Atalho	Petrolina	LAP 1	-8,749603	-40,621879
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525852 EREM PROFº DENIVAL JOSE RODRIGUES DE MELO GRE 05	Rua Agrovila Matori, S/N	Centro	Itaquitinga	LAP 2	-7,664765	-35,100867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185059 EREM GENIFA FELISBELA NOBRE GRE 16	Rua Projetada, S/N	Manaíba	Ipubi	LAP 1	-7,468605	-40,277615
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063522 ESCOLA TEOFILO SEVERINO DE ARRUDA GRE 08	Povoado Lagoa de João Carlos, S/N	Centro	Frei Miguelinho	LAP 2	-7,943476	-35,921563
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009390 EREM FRANCISCO PIRES GRE 15	Rua Tiburtino De Carvalho, S/N	Centro	Mirandiba	LAP 2	-8,117437	-38,727316
SECRETARIA DE EDUCAÇÃO E ESPORTES	26117088 ESCOLA WALFRIDO ADVINCULA GRE 03	Av. Chã da Mangabeira, 258	Tabajara	Paulista	LAP 2	-7,982633	-34,856573
SECRETARIA DE EDUCAÇÃO E ESPORTES	26153491 EREM MONSENHOR MANOEL LEONARDO DE BARROS BARRETO GRE 02	Rua Arariba, S/N		Recife	LAP 2	-8,073829	-34,891732
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122260 EREM PROFº MOTTA E ALBUQUERQUE GRE 01	Rua Soares Moreno - Nº117	Tamarineira	Recife	LAP 2	-8,029956	-34,905084
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113635 EREM MARIA EMILIA ROMEIRO ESTELITA GRE 03	Rua Camomila, S/N	Ouro Preto	Olinda	LAP 2	-7,995204	-34,865851
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105837 EREM MARIA GAYAO PESSOA GUERRA GRE 03	Av. João Pessoa Guerra - S/N	Centro	Araçoiaba	LAP 2	-7,78947655	-35,9099336
SECRETARIA DE EDUCAÇÃO E ESPORTES	26188325 ESCOLA ESTADUAL INDÍGENA MARIA CÂNDIDA DE QUEIRÓZ GRE 11	Sítio Ingá	Pólo Nazário	Inajá	LAP 1	-8,81024	-37,760233
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040751 ESCOLA ESTADUAL INDIGENA MONTEIRO LOBATO GRE 13	ALDEIA OITICA	ZONA RURAL	Petrolina	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059576 ESCOLA ESTADUAL INDÍGENA DIONÍSIO BARBOSA DOS SANTOS GRE 11	ALDEIA CALDEIRAO		Pesqueira	LAP 1	-8,36273	-36,73885
SECRETARIA DE EDUCAÇÃO E ESPORTES	26086638 EREM FREI EPIFANIO GRE 06	Av. Manoel Quintino, 30	Centro	São Joaquim do Monte	LAP 2	-8,430779	-35,810144
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040727 ESCOLA ESTADUAL INDIGENA PEDRO FRANCISCO DE OLIVEIRA GRE 13	ALDEIA BREJO DA GAMA	TERRITORIO INDIGENA ATIKUN	Carnaubeira da Penha	LAP 1	-8,314814	-38,626727

SECRETARIA DE EDUCAÇÃO E ESPORTES	26076780 EREM FRANCISCO PEREIRA DA COSTA GRE 10	Av. Sete De Setembro, S/N	Centro	Iati	LAP 2	-9,041564	-36,849299
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105519 EREM SANTOS COSME E DAMIAO GRE 03	Rua Joaquim Nabuco	Centro	Igarassu	LAP 2	-7,8301	-34,90909
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042070 EREM MARIA CAVALCANTI NUNES GRE 13	Rua Capitao Jose de Souza Ferraz, 17	Centro	Petrolândia	LAP 2	-8,979545	-38,220804
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036223 EREM NOSSA SENHORA APARECIDA - PETROLINA GRE 14	Rua B, S/N	Afogados	Petrolina	LAP 2	-9,366617	-40,565696
SECRETARIA DE EDUCAÇÃO E ESPORTES	26047845 ESCOLA ANETE VALE DE OLIVEIRA GRE 11	Rua Elvira Vale De Oliveira, 185	Centro	Pedra	LAP 2	-8,497701	-36,942659
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024802 EREM MONSENHOR JOSÉ KEHRLE GRE 11	Rua Antonio Tenorio Cavalcante	Boa Esperança	Arcoverde	LAP 2	-8,43353734	-37,6507195
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126010 EREM CAIO PEREIRA GRE 01	Rua José Bonifácio, 0	Brejo De Beberibe	Recife	LAP 2	-8,043095	-34,908041
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186004 ETE SENADOR WILSON CAMPOS GRE 05	Rodovia BR 408, S/N	Centro	Paudalho	LAP 2	-7,892983	-35,173712
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040948 EREM CAPITÃO NESTOR VALGUEIRO DE CARVALHO GRE 13	Av. Dep. Odomar Ferraz, 231	Centro	Floresta	LAP 2	-8,598455	-38,573856
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054876 EREM PROFº VICENTE MONTEIRO GRE 09	Rua Professor Dr. Julio De Melo, S/N	Centro	Caruaru	LAP 2	-8,283975	-35,966206
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113856 EREM PROFº ESTEVAO PINTO GRE 03	Avenida Presidente Kennedy, 154	Aguazinha	Olinda	LAP 2	-8,004341	-34,887547
SECRETARIA DE EDUCAÇÃO E ESPORTES	26049562 EREM GONCALO ANTUNES BEZERRA GRE 11	Rua Coronel Antonio Inojosa, 127	Centro	Alagoinha	LAP 1	-8,466242	-36,775483
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114860 EREM TABAJARA GRE 03	Av. Tabajara, 149	Cidade Tabaraja	Olinda	LAP 2	-7,968927	-34,869002
SECRETARIA DE EDUCAÇÃO E ESPORTES	26176211 ETE MARIA JOSE VASCONCELOS GRE 06	Rua Jose Mendonça Brainer, S/N	Santo Amaro II	Bezerros	LAP 2	-8,241971	-35,763327
SECRETARIA DE EDUCAÇÃO E ESPORTES	26077825 EREM SEBASTIAO TIAGO DE OLIVEIRA GRE 10	Rua Tenente Pedro Luis, 92	Centro	Jupi	LAP 2	-8,71407736	-36,41385337
SECRETARIA DE EDUCAÇÃO E ESPORTES	26094800 EREM ANTONIO DIAS CARDOSO GRE 06	Rua Dr. José Augusto, S/N	Centro	Vitória de Santo Antão	LAP 2	-8,11357286	-35,28969085
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088134 ESCOLA SAO JOSE GRE 05	Travessa Francisco Montenegro, S/N	Centro	Carpina	LAP 2	-7,843504	-35,250274
SECRETARIA DE EDUCAÇÃO E ESPORTES	26117258 EREM CUSTODIO PESSOA GRE 03	Av Lindolfo Collor, 0	Paratibe	Paulista	LAP 2	-7,935866	-34,89888

SECRETARIA DE EDUCAÇÃO E ESPORTES	26124580 EREM ELEANOR ROOSEVELT GRE 02	R. Jean Emile Favre, s/n - Ipsep, Recife - PE, 51350-250	Ipsep	Recife	LAP 2	-8,108206	-34,916585
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075920 ESCOLA PROFª ELVIRA VIANA GRE 10	Rua Santa Quitéria, S/N.	Heliópolis	Garanhuns	LAP 1	-8,885227	-36,469111
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091658 EREM CLOVIS SALGADO GRE 05	Rua Prof. Dionísio Dias De Oliveira, S/N	Jardim Guarani	Timbaúba	LAP 1	-7,50336451	35,31771445
SECRETARIA DE EDUCAÇÃO E ESPORTES	26072637 EREM MESTRA BEATRIZ GRE 10	Rua São Sebastião, 351	Centro	Bom Conselho	LAP 2	-9,17465288	36,68106551
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069202 CENTRO DE REABILITAÇÃO E EDUCACAO ESPECIAL - LIMOEIRO GRE 08	Loteamento Santo Antonio, S/N	Centro	Limoeiro	LAP 1	-7,88034881	35,43997903
SECRETARIA DE EDUCAÇÃO E ESPORTES	26104601 EREM BARRA DO SIRINHAEM GRE 07	Rua Antonio Ribeiro, S/N	Centro	Sirinhaém	LAP 1	-8,616157	-35,05649
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124785 EREM DOM SEBASTIAO LEME GRE 02	Rua Engenho Muribara, S/N	Ur-lí - Ibura	Recife	LAP 2	-8,114496	-34,949256
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070782 EREM CONEGO FERNANDO PASSOS GRE 08	Rua Otaviano Sloari De Albuquerque, S/N	Centro	Passira	LAP 2	-7,975974	-35,580445
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089947 ESCOLA SEVERINO GOUVEIA DE LIMA GRE 05	Av. Antônio Carlos De Almeida, 36	Centro	Itaquitinga	LAP 2	-7,66802	-35,100765
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123150 EREM CREUSA BARRETO DORNELAS GRE 02	Rua Cantora Clara Nunes, S/N	Torre	Recife	LAP 2	-8,044671	-34,915745
SECRETARIA DE EDUCAÇÃO E ESPORTES	26181649 EREM QUILOMBOLA ALZIRA TENORIO DO AMARAL GRE 11	Rua Comunidade Quilombola de Buenos Aires, S/N	Centro	Custódia	LAP 1	-8,086168	-37,640264
SECRETARIA DE EDUCAÇÃO E ESPORTES	26013452 EREM DESEMBARGADOR JOAO PAES GRE 15	Praça Coronel Chico Romão, 568	Centro	Serrita	LAP 2	-7,819325	-39,148282
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123479 EREM ALBERTO TORRES GRE 02	Av. Dr Jose Rufino, 2993	Tejipió	Recife	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124190 EREM SANTOS DUMONT GRE 02	Av Barao De Souza Leao, 792	Setúbal	Recife	LAP 2	-8,131926	-34,906976
SECRETARIA DE EDUCAÇÃO E ESPORTES	26140144 EREM PAU BRASIL GRE 14	Povoado Agrovila, 21	Centro	Santa Maria da Boa Vista	LAP 2	-8,799687	-39,827081
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111284 ESCOLA VILA JOAO DE DEUS GRE 04	Rua Ernertina Batista, S/N	Pontezinha	Jaboatão dos Guararapes	LAP 2	-8,155545	-34,92478
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128195 EREM JARBAS PERNAMBUCANO GRE 01	Rua Marquês De Tamandaré, S/N	Cajueiro	Recife	LAP 1	-8,032837	-34,925474
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059380 ESCOLA ESTADUAL INDÍGENA ANTONIO MONTEIRO LEITE GRE 11	Aldeia Rezende, Zona Rural - Pesqueira		Pesqueira	LAP 1	-8,354115	-36,893034
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124939 ESCOLA SARGENTO CAMARGO GRE 02	Rua Antonio Falcao, 136	Boa Viagem	Recife	LAP 2	-8,116471	-34,893936
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042053 EREM ESTADUAL DE ITAPARICA GRE 13	Rua Salto Da Divisa, S/N	Centro	Jatobá	LAP 2	-9,17455	-38,246836
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122960 EREM VIDAL DE NEGREIROS GRE 02	Rua Bezerra Da Palma, 100	Afogados	Recife	LAP 2	-8,074422	-34,913088
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121620 EREM JOAO BARBALHO GRE 01	Rua Do Hospício, 737	Centro	Recife	LAP 2	-8,056322	-34,882956

SECRETARIA DE EDUCAÇÃO E ESPORTES	26058480 ESCOLA ESTADUAL INDÍGENA CONEGO OLÍMPIO TORRES GRE 11	Aldeia Caetano	Zona Rural	Pesqueira	LAP 1	-8,324592	-36,743263
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121751 ETE GINASIO PERNAMBUCANO - CRUZ CABUGA GRE 01	Av. Cruz Cabugá, S/N		Recife	LAP 2	-8,046376	-34,876405
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036177 ESCOLA NÚCLEO DE MORADORES - 6 GRE 14	Rua B , S/N	Projeto Senador Nilo Coelho Nucleo 6	Petrolina	LAP 2	-9,27322853	-40,52997615
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121816 ETE ALMIRANTE SOARES DUTRA GRE 01	Praça General Abreu E Lima, S/N	Santo Amaro	Recife	LAP 2	-8,047463	-34,876024
SECRETARIA DE EDUCAÇÃO E ESPORTES	26064642 EREM MARIA CECILIA BARBOSA LEAL GRE 08	Av. São Sebastião, S/N	Centro	Surubim	LAP 2	-7,850899	-35,762419
SECRETARIA DE EDUCAÇÃO E ESPORTES	26137410 ESCOLA ESTADUAL INDÍGENA ROGÉRIO CAVALCANTE DE BRITO GRE 11	ALDEIA CURRAL DE BOI		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26008882 ESCOLA PROFª ANTONIA MARINHO APOLINÁRIO GRE 16	Rua Prudencio de Moraes, S/N	Vila São Sebastião	Trindade	LAP 2	-7,758907	-40,265631
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126559 ESCOLA COMANDANTE LUIZ GOMES GRE 01	Av. Ver. Otacilio Azevedo, 2567	Casa Amarela	Recife	LAP 2	-7,998836	-34,924381
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027836 EREM INOCENCIO CORREIA LIMA GRE 11	Av. Castro Alves, 1	Centro	Ibimirim	LAP 2	-8,53743348	-37,6899013
SECRETARIA DE EDUCAÇÃO E ESPORTES	26121247 EREM JOAQUIM NABUCO GRE 02	Rua Imperial, 1102	São Jose	Recife	LAP 1	-8,074696	-34,891447
SECRETARIA DE EDUCAÇÃO E ESPORTES	26101602 EREM DA FRATERNIDADE PALMARENSE GRE 07	Quilombo II, Quadra 5, S/N		Palmares	LAP 1	-8,700052	-35,603891
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126206 EREM GILBERTO FREYRE GRE 01	Rua Alto 13 De Maio, S/N	Vasco Da Gama	Recife	LAP 2	-8,009354	-34,92259
SECRETARIA DE EDUCAÇÃO E ESPORTES	26083159 EREM DR ALEXANDRINO DA ROCHA GRE 06	Av. Agamenom Magalhães, 301	Boa Vista	Bonito	LAP 2	-8,467705	-35,730577
SECRETARIA DE EDUCAÇÃO E ESPORTES	26072254 EREM FREI CAETANO DE MESSINA GRE 10	Praça Frei Caetano de Messina, S/N	Centro	Bom Conselho	LAP 2	-9,166254	-36,683591
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089718 EREM JOSE ANTONIO BEZERRA DE MENEZES GRE 05	Rua São Pedro, 266	Centro	Itambé	LAP 1	-7,40946078	-35,10885868
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105101 EREM JOAO PEREIRA SOBRINHO GRE 07	Rua Travessa Ipiranga, 74	Centro	Xexéu	LAP 2	-8,807678	-35,62596
SECRETARIA DE EDUCAÇÃO E ESPORTES	26044862 EREM CORONEL NICOLAU SIQUEIRA GRE 10	Rua Alegria, 60	Centro	Águas Belas	LAP 2	-9,11113048	-37,12269798
SECRETARIA DE EDUCAÇÃO E ESPORTES	26191814 CENTRO EDUCACIONAL INCLUSIVO ULISSES PERNAMBUCANO - CEIUP GRE 01	Rua Gouveia De Barros, S/N	Santo Amaro	Recife	LAP 1	-8,049569	-34,888696
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033356 EREM SENADOR NILO COELHO GRE 14	Rua Jacobi Vieira De Carvalho, S/N	Centro	Dormentes	LAP 1	-8,445703	-40,766388
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097710 ETE CENTRAL BARREIROS GRE 07	Rua Projetada, Quadra 1, Gleba B - 2, , S/N	Massa Falida	Barreiros	LAP 1	-8,812047	-35,199542
SECRETARIA DE EDUCAÇÃO E ESPORTES	26064294 EREM JOÃO DAVID DE SOUZA GRE 08	Rua Aglutino De Almeida, S/N	Centro	Santa Maria do Cambucá	LAP 2	-7,834222	-35,881567

SECRETARIA DE EDUCAÇÃO E ESPORTES	26126621 EREM ROTARY DE NOVA DESCOBERTA GRE 01	Av Ver Otacilio Azevedo, 0	Brejo de Beberibe	Recife	LAP 2	-7,999842	-34,922803
SECRETARIA DE EDUCAÇÃO E ESPORTES	26120100 EREM PROFª INALDA SPINELLI GRE 02	Jorge Couceiro Da Costa Eiras - S/N	Boa Viagem	Recife	LAP 1	-8,121825	-34,908266
SECRETARIA DE EDUCAÇÃO E ESPORTES	26041014 ESCOLA ESTADUAL INDIGENA ANTONIO FRANCISCO DA SILVA GRE 13	ALDEIA CARAIBAS	POVO PIPIPA	Floresta	LAP 1	-8,665375	-38,1489252
SECRETARIA DE EDUCAÇÃO E ESPORTES	26139120 EREM HONÓRIO BERNARDES DA SILVA GRE 13	Av. HONÓRIO BERNARDES SILVA, S/N	Centro	Belém de São Francisco	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26056798 EREM MONSENHOR JOSÉ ELIAS DE ALMEIDA GRE 06	Rua B5 ,Bairro: Nossa Senhora Das Graças, S/N	Nossa Sra. das Graças	Gravatá	LAP 1	-8,198282	-35,556615
SECRETARIA DE EDUCAÇÃO E ESPORTES	26136489 EREM ESCRITOR JOSE DE ALENCAR GRE 03	Rua 52, S/N	Maranguape I - Paulista	Paulista	LAP 2	-7,95024	-34,864102
SECRETARIA DE EDUCAÇÃO E ESPORTES	26084791 EREM PROFª MANOEL EDMUNDO GRE 07	Rua São Sebastião, S/N	Centro	Lagoa dos Gatos	LAP 2	-8,653292	-35,902797
SECRETARIA DE EDUCAÇÃO E ESPORTES	26052083 EREM ANDRE CORDEIRO GRE 09	Rua Dr. José Neri, 219	Centro	Brejo da Madre de Deus	LAP 2	-8,145048	-36,374228
SECRETARIA DE EDUCAÇÃO E ESPORTES	26158582 ESCOLA ESTADUAL INDIGENA SIMAO CICERO DA SILVA GRE 13	Aldeia Saquinho, s/n - Zona Rural		Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125358 EREM MONTE VERDE GRE 02	Rua Maria Lima Da Silva, 0	Monte Verde	Recife	LAP 2	-8,117913	-34,95984
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011972 ESCOLA ESTADUAL INDIGENA SAO DOMINGOS SAVIO GRE 15	Aldeia Mulungu, s/n - Zona Rural		Salgueiro	LAP 1	-8,10406106	-39,147632
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122278 EREM REGUEIRA COSTA GRE 01	Rua Regueira Costa, s/n	Rosarinho	Recife	LAP 1	-8,034095	-34,89863
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035561 ESCOLA DOM ANTONIO CAMPELO GRE 14	Av. 3, S/N	Centro	Petrolina	LAP 2	-9,390508	-40,547061
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040557 ESCOLA ESTADUAL INDIGENA VICENTE MUNIZ GRE 13	Aldeia Olho D'água do Muniz	Area Indígena Povo Pankara	Carnaubeira da Penha	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110245 EREM SENADOR ADERBAL JUREMA GRE 04	Rua 7, S/N	Curado 4	Jaboatão dos Guararapes	LAP 2	-8,068861	-34,994309
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178079 ESCOLA ESTADUAL FERNANDO SOARES LYRA GRE 04	Rodovia Br 28, Km 17, S/N	Enseada dos Corais	Cabo de Santo Agostinho	LAP 2	-8,316209	-34,948078
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122120 COLEGIO DA POLICIA MILITAR DE PERNAMBUCO GRE 01	Rua Henrique Dias, 609	Derby	Recife	LAP 2	-8,059392	-34,89993
SECRETARIA DE EDUCAÇÃO E ESPORTES	26173689 ESCOLA ESTADUAL INDIGENA SANTO EXPEDITO GRE 13	Aldeia Pitombeira, s/n - Zona Rural	Zona Rural	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124572 EREM DELMIRO GOUVEIA GRE 02	Av Cons Aguiar, 0	Pina	Recife	LAP 1	-8,092956	-34,884149

SECRETARIA DE EDUCAÇÃO E ESPORTES	26035120 EREM PROFª OSA SANTANA DE CARVALHO GRE 14	Conjunto Massangana, 454	COHAB Massangano	Petrolina	LAP 2	-9,38106358	-40,53501966
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036193 ESCOLA NUCLEO DE MORADORES-7 GRE 14	Projeto Senador Nilo Coelho, S/N	Projeto Senador Nilo Coelho	Petrolina	LAP 2	-9,286306	-40,506127
SECRETARIA DE EDUCAÇÃO E ESPORTES	26104245 EREM SAO FRANCISCO DE ASSIS - LT GRE 07	Rua Do Campo, S/N	Livio Tenório	São José da Coroa Grande	LAP 1	-8,89583795	-35,15390448
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075709 ESCOLA DOM JUVENCIO BRITTO GRE 10	Rua Pedro Rocha, 105	Heliópolis	Garanhuns	LAP 2	-8,883624	-36,486514
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107570 EREM DEPUTADO OSCAR CARNEIRO GRE 04	Rua Luiz Carlos Do Araujo, S/N	Vília Da Fábrica	Camaragibe	LAP 2	-8,009012	-34,978352
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090767 EREM ANTONIO COUTINHO GRE 05	Rua Dr. Manoel Coutinho, S/N	Piaruá	Macaparana	LAP 1	-7,524372	-35,475741
SECRETARIA DE EDUCAÇÃO E ESPORTES	26003210 ESCOLA SAO VICENTE DE PAULA - EXU GRE 16	Rua Anália Soares, 77	Centro	Exu	LAP 2	-7,514993	-39,721411
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097257 EREM DOUTOR ANTHENOR GUIMARAES GRE 07	Rua Engenho Pibiri, S/N	Pibiri	Barreiros	LAP 2	-8,809425	-35,209596
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090864 ESCOLA DOM CARLOS COELHO - NAZARE GRE 05	Rua Barão De Tamandaré, S/N	Centro	Nazaré da Mata	LAP 2	-7,742453	-35,224003
SECRETARIA DE EDUCAÇÃO E ESPORTES	26069318 EREM DR SEBASTIAO DE VASCONCELOS GALVAO GRE 08	Rua Professor Rivaldavia Bernardes De Paula, 83	José Fernandes Salsa	Limoeiro	LAP 2	-7,8834647	-35,45063777
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088533 ESCOLA JULIO CORREIA DE OLIVEIRA GRE 05	Rua José Gaião, 232	Centro	Condado	LAP 2	-7,584658	-35,106218
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125781 EREM SILVA JARDIM GRE 01	Praça Do Monteiro, 2727	Monteiro	Recife	LAP 1	-8,028182	-34,928653
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130319 ESCOLA PROFª NATANAEL BARBOSA MEDRADO GRE 04	Loteamento Rosa Dos Ventos - Rua Um, S/N	Charneca	Cabo de Santo Agostinho	LAP 2	-8,29576	-35,057309
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130114 EREM PASTOR JOSE FLORENCIO RODRIGUES GRE 04	Loteamento Jardim Sto. Inácio S/N	Vila Sto. Inácio	Cabo de Santo Agostinho	LAP 2	-8,285493	-35,025048
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999915 ESCOLA DESEMBARGADOR JOAO PAES - ANEXO GRE15	PRAÇA CORONEL CHICO ROMÃO, 568.	Centro	Serrita	LAP 1	-7,94837739	-39,29350136
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040280 EREM PROFª AURELIANO GONCALVES DOS SANTOS GRE 13	Rua Pedro Nunes, S/N	Centro	Carnaubeira da Penha	LAP 1	-8,32066543	-38,74234344
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042754 ESCOLA ESTADUAL INDIGENA AGRESTE GRE 13	ALDEIA AGRESTE	ZONA RURAL	Tacaratu	LAP 1	-8,93384	-38,10545
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186241 EREM PROFª JORDAO EMERENCIANO GRE 02	AV SANTAREM	IBURA - UR2	Recife	LAP 2	-8,111686	-34,938084
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185806 ETE GOVERNADOR EDUARDO CAMPOS GRE 04	Rua Pedro Correia, S/N	Centro	São Lourenço da Mata	LAP 2	-7,99376	-35,039247
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116383 ESCOLA PROFª MARIA ALVES MACHADO GRE 03	Rua Noventa E Um, S/N	Maranguape II	Paulista	LAP 2	-7,927502	-34,852851

SECRETARIA DE EDUCAÇÃO E ESPORTES	01999999 GRE 01 - Recife Norte Secret	Rua Coelho Leite, 80	Santo Amaro	Recife	LAP 1	-8,05273	-34,882353
SECRETARIA DE EDUCAÇÃO E ESPORTES	26055082 EREM PROFª LISBOA GRE 09	Rua Lagoa Do Ouro, S/N	Boa Vista I	Caruaru	LAP 2	-8,277038	-35,989525
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031400 ESCOLA INDIGENA HERMENEGILDO ANTONIO DOS SANTOS GRE 14	Aldeia Lagoa Branca, s/n - Ilha da Assunção - Zona Rural		Cabrobó	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130386 EREM JOSE RODRIGUES DE CARVALHO GRE 04	Rua 52, S/N		Cabo de Santo Agostinho	LAP 2	-8,28134	-35,01223
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127474 ESCOLA PADRE DEHON GRE 02	Av. Caxanga, 3560	Iputinga	Recife	LAP 2	-8,040935	-34,937378
SECRETARIA DE EDUCAÇÃO E ESPORTES	26132230 ESCOLA DE APLICAÇÃO PROFª IVONITA ALVES GUERRA GRE 10	Rua Capitão Pedro Rodrigues, 105	São José	Garanhuns	LAP 2	-8,883667	-36,496193
SECRETARIA DE EDUCAÇÃO E ESPORTES	26048078 EREM AMALIA CAVALCANTI DA COSTA LIMA GRE 11	Rua Alice Japiassú Simões, S/N	Centro	Pedra	LAP 2	-8,500129	-36,945907
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999907 ANEXO - ESCOLA ESTADUAL DE ALTERNÂNCIA GRE 14	Rua Febronio de Souza, S/N	Jardim Massangano	Petrolina	LAP 1	-9,392577	-40,521599
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114054 ESCOLA SAO LUCAS GRE 03	Rua Catarina Batista De Alencar, 791	Casa Caiada	Olinda	LAP 1	-7,992856	-34,844785
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123258 EREM MARTINS JÚNIOR GRE 02	Av Padre José Regueira, 136	Torre	Recife	LAP 1	-8,047491	-34,912648
SECRETARIA DE EDUCAÇÃO E ESPORTES	06999999 GRE 06 - Mata Centro / Vitória de Santo Antão Secret	Rua Dr José Augusto S/N	Matriz	Vitória de Santo Antão	LAP 1	-8,11328746	-35,2864227
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097249 EREM DOM LUIZ DE BRITO GRE 07	Praça Dom Luiz de Brito, S/N	Centro	Amaraji	LAP 1	-8,379755	-35,451811
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128179 ESCOLA DR FRANCISCO PESSOA DE QUEIROZ GRE 01	Hidelbrando De Vasconcelos, S/ N	Dois Unidos	Recife	LAP 2	-7,996076	-34,909248
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125013 EREM GERCINO DE PONTES GRE 02	R. Álvaro Amorim	Imbiribeira	Recife	LAP 1	-8,086569	-34,908991
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127857 ESCOLA FERNANDES VIEIRA GRE 02	AV Caxanga, 3595	Iputinga	Recife	LAP 2	-8,041357	-34,938021
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020572 ESCOLA MAXIMA VIEIRA DE MELO GRE 12	Rua LUZIA PASSOS, S/N	Centro	São José do Egito	LAP 1	-7,537641	-37,377557
SECRETARIA DE EDUCAÇÃO E ESPORTES	26155435 ESCOLA ESTADUAL INDIGENA JOAQUIM ROSENO DOS SANTOS GRE 13	ALDEIA TRAVESSAO DO OURO - S/N	ZONA RURAL	Floresta	LAP 1	-8,57726	-37,93532
SECRETARIA DE EDUCAÇÃO E ESPORTES	26044412 ESCOLA JOAO RODRIGUES CARDOSO GRE 10	3ª Travessa Av. Cel Alfredo Duarte, S/N	Centro	Águas Belas	LAP 2	-9,115326	-37,118013
SECRETARIA DE EDUCAÇÃO E ESPORTES	26032066 ESCOLA ESTADUAL INDIGENA MARIA ANTONIA DA CONCEICAO PRACA GRE 14	ILHA DA ASSUNCAO	ALDEIA PANELA	Cabrobó	LAP 1	-8,54998143	39,34989807
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059207 ESCOLA ESTADUAL INDIGENA SANTA ÁGUEDA GRE 11	Aldeia Caipe, Zona Rural - Pesqueira		Pesqueira	LAP 1	-8,32474	-36,748116

SECRETARIA DE EDUCAÇÃO E ESPORTES	26106353 EREM SENADOR JOSE ERMIRIO DE MORAES GRE 03	Rua L, Agrovila de Botafogo, S/N	Centro	Itapissuma	LAP 2	-7,749328	-34,936048
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090406 EREM CREUSA DE FREITAS CAVALCANTI GRE 05	Av. José Leitão De Melo, 535	Centro	Macaparana	LAP 2	-7,556546	-35,444076
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027232 ESCOLA ESTADUAL INDÍGENA SÃO FRANCISCO DE ASSIS GRE 11	Sítio Pereiros, S/N	Zona Rural	Ibimirim	LAP 1	-8,534383	-37,695221
SECRETARIA DE EDUCAÇÃO E ESPORTES	26095572 ESCOLA OLIVIA CARNEIRO DE CARVALHO GRE 06	Rua Jornalista Ovidio Verçosa Filho, 114	Cidade de Deus	Moreno	LAP 1	-8,108982	-35,297467
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098822 EREM PROFª ABIGAIL GUERRA GRE 07	Largo da Emancipação, S/N	Centro	Cortês	LAP 2	-8,473747	-35,54337
SECRETARIA DE EDUCAÇÃO E ESPORTES	26213800 ESCOLA MANOEL MESSIAS BARBOSA GRE 14	Agrovila Massangana, S/N	Estrada da Tapera	Petrolina	LAP 2	-9,440888	-40,570326
SECRETARIA DE EDUCAÇÃO E ESPORTES	26189526 ESCOLA ESTADUAL INDÍGENA LUIZ PEREIRA LEAL GRE 13	Aldeia Serrote dos Campos - S/N	Território Indígena do Povo Pankará	Itacuruba	LAP 1	-8	-38,7152146
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126230 ESCOLA IRMA MAGNA GRE 01	Vereador Otacílio Azevedo, 288	Beberibe	Recife	LAP 2	-8,00482463	34,91622987
SECRETARIA DE EDUCAÇÃO E ESPORTES	26023334 EREM PEDRO PIRES FERREIRA GRE 12	Rua José Cordeiro da Silva, S/N	Centro	Tabira	LAP 2	-7,59175329	37,54205167
SECRETARIA DE EDUCAÇÃO E ESPORTES	26035502 ESCOLA ANTONIO NUNES DOS SANTOS GRE 14	Projeto de Irrigação Bebedouro, S/N	Vila NS 1	Petrolina	LAP 2	-9,382733	-40,494913
SECRETARIA DE EDUCAÇÃO E ESPORTES	26074923 ESCOLA PROFª CLARICE GODOY GRE 10	Rua Joaquin Nabuco, 183	Centro	Correntes	LAP 1	-9,127585	-36,330164
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525801 ETE JOSE HUMBERTO DE MOURA CAVALCANTI GRE 08	Rodovia Pe 90, S/N	Centro	Limoeiro	LAP 2	-7,857226	-35,44729
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116413 EREM RADIALISTA LUIZ QUEIROGA GRE 03	Rua Noventa E Oito	Jardim Paulista	Paulista	LAP 2	-7,952335	-34,891466
SECRETARIA DE EDUCAÇÃO E ESPORTES	26131528 EREM ALBERTINA DA COSTA SOARES GRE 04	Rua Engenho São Pedro, S/N	Centro	Ipojuca	LAP 1	-8,512106	-35,121913
SECRETARIA DE EDUCAÇÃO E ESPORTES	26071924 EREM AZARIAS SALGADO GRE 10	Rua Mar Augusto Teixeira De Freitas, 105	Centro	Angelim	LAP 2	-8,889735	-36,285127
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130947 ESCOLA DOMINGOS DE ALBUQUERQUE GRE 04	Rua Joao Pessoa, S/N	Centro	Ipojuca	LAP 2	-8,400991	-35,062968
SECRETARIA DE EDUCAÇÃO E ESPORTES	26066181 ESCOLA ESTELITA TIMOTEO GRE 09	Rua Joao Pereira Tabosa, S/N	Centro	Toritama	LAP 2	-8,006956	-36,055391
SECRETARIA DE EDUCAÇÃO E ESPORTES	26182084 ESCOLA ESTADUAL JOSE RODRIGUES DE BARROS - MESTRE ZUZA GRE 07	Rua do Cajueiro, S/N	Várzea do Una	São José da Coroa Grande	LAP 1	-8,838357	-35,142373
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036169 ESCOLA MANOEL MARINHO GRE 14	Rua A, S/N	Projeto Senador Nilo Coelho	Petrolina	LAP 1	-9,32434	-40,617202
SECRETARIA DE EDUCAÇÃO E ESPORTES	26187566 ESCOLA ESTADUAL CLAUDIO RODRIGUES GALINDO GRE 14	POVOADO DE CACHOEIRA DO ROBERTO, S/N	Cachoeira do Roberto	Afrânio	LAP 1	-8,638403	-41,147054

SECRETARIA DE EDUCAÇÃO E ESPORTES	26092301 JEREM DR WALFREDO LUIZ PESSOA DE MELO GRE 05	Av. Severino Elio Albuquerque, S/N	Centro	Tracunhaém	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26019370 JEREM SANTA CRUZ GRE 12	Rua José Augusto Santos de Nins, 189	Centro	Santa Cruz da Baixa Verde	LAP 2	-7,820184	-38,153132
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134180 ESCOLA PROFª JOEL PONTES GRE 02	Av. Liberdade S/N	Localizado Dentro Do Presídio Anibal Bruno	Recife	LAP 1	-8,081905	-34,961997
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027577 ESCOLA ESTADUAL INDÍGENA ROZENO VIEIRA GRE 11	SERRA DO PERIQUITO	ZONA RURAL	Ibimirim	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26074079 JEREM AUGUSTA CORDEIRO DE MELO GRE 10	Rua Luiz Inácio Dos Santos, 126	Centro	Calçado	LAP 2	-8,742715	-36,338617
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098504 JEREM TOBIAS BARRETO GRE 07	Rua da Balança, S/N	Centro	Catende	LAP 1	-8,668742	-35,720894
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123240 JEREM MARIA GORETTI GRE 02	Rua Padre Teófilo Tworz	Afogados	Recife	LAP 2	-8,065769	-34,908346
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027658 ESCOLA ESTADUAL INDÍGENA FIRMINO LARANJEIRA GRE 11	ALDEIA QUIRIDALHO	ZONA RURAL	Ibimirim	LAP 1	-8,52732	-37,55345
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001624 JEREM ANIZIO RODRIGUES COELHO GRE 16	Rua Raimundo Cordeiro, S/N	Nascente	Araripina	LAP 1	-7,880512	-40,475605
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109360 JEREM BERNARDO VIEIRA GRE 04	Rua Barão De Lucena, 422	Centro	Jaboatão dos Guararapes	LAP 2	-8,112323	-35,017014
SECRETARIA DE EDUCAÇÃO E ESPORTES	26114607 JEREM JOAO MATOS GUIMARAES GRE 03	Av. Das Garças S/N - 4ª Etapa	Rio Doce	Olinda	LAP 2	-7,962325	-34,85369
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105314 JEREM JOAO PESSOA GUERRA GRE 03	Av. Alfredo Bandeira De Melo, S/N	Cruz de Rebouças	Igarassu	LAP 2	-7,824288	-34,916027
SECRETARIA DE EDUCAÇÃO E ESPORTES	26028506 ESCOLA ESTADUAL INDÍGENA AIMBERE GRE 11	ALDEIA BAIXA DA ALEXANDRA	Zona Rural	Inajá	LAP 1	-8,777899	-37,893666
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107945 JEREM PROFº CARLOS FREDERICO DO REGO MACIEL GRE 04	Rua Oscar André Albuquerque, 118	Timbi	Camaragibe	LAP 1	-8,025656	-34,997366
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126133 JEREM DOM VITAL GRE 01	Estrada Arraial, S/N	Casa Amarela	Recife	LAP 2	-8,027308	-34,918196
SECRETARIA DE EDUCAÇÃO E ESPORTES	26154358 JEREM ICO MANDANTES GRE 13	Perímetro Irrigado, S/N	Projeto Icó Mandantes	Petrolândia	LAP 2	-8,913476	-38,274401
SECRETARIA DE EDUCAÇÃO E ESPORTES	16999999 GRE 16 - Sertão do Araripe / Araripina Secret	Rodovia Br-316 Km.21	Centro	Araripina	LAP 2	-7,64883	-40,413795
SECRETARIA DE EDUCAÇÃO E ESPORTES	10999999 GRE 10 - Agreste Meridional / Garanhuns Secret	Praça Tavares Correia, 52	Centro	Garanhuns	LAP 1	-8,881051	-36,476311
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040549 ESCOLA ESTADUAL INDIGENA SANTA ANA GRE 13	Aldeia Baixão, S/N	Povo Atikum	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26095335 JEREM SENADOR JOÃO CLEOFAS DE OLIVEIRA GRE 06	Av. Dom Joao Costa, S/N	Livramento	Vitória de Santo Antão	LAP 2	-8,120505	-35,305528
SECRETARIA DE EDUCAÇÃO E ESPORTES	26134857 ESCOLA MEDICO RUY DO REGO BARROS GRE 03	Avenida A, S/N	Caetés II	Abreu e Lima	LAP 1	-7,92764807	34,92165099
SECRETARIA DE EDUCAÇÃO E ESPORTES	26179806 JEREM DE SALGUEIRO GRE 15	Rodovia Br 232, S/N	Loteamento Nossa Sra. da Conceição	Salgueiro	LAP 2	-8,023698	-39,187488

SECRETARIA DE EDUCAÇÃO E ESPORTES	26104920 JEREM DR EURICO CHAVES GRE 07	Rua Marques De Olinda, S/N	Centro	Sirinhaém	LAP 2	-8,595132	-35,112387
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042428 ESCOLA ESTADUAL INDIGENA DOM JOAO BOSCO GRE 13	Aldeia Mundo Novo Entre Serras, s/n	Zona Rural	Petrolândia	LAP 1	-8,97888	-38,21793
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169975 ESCOLA JOSE ANTONIO FAGUNDES GRE 05	Rua Piloto Ayrton Senna, S/N	Chã de Cruz	Abreu e Lima	LAP 2	-7,902974	-35,066309
SECRETARIA DE EDUCAÇÃO E ESPORTES	26055473 ESCOLA PAULINA MONTEIRO GRE 09	Rua Jose Carlos Coutinho, 432	Centro	Caruaru	LAP 2	-8,280523	-35,946965
SECRETARIA DE EDUCAÇÃO E ESPORTES	26109107 JEREM SIMON BOLIVAR GRE 04	Av Leonardo Da Vinci, S/N	Curado II	Jaboatão dos Guararapes	LAP 1	-8,080094	-34,996582
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009315 JEREM PROFº MANOEL JOAQUIM LEITE GRE 15	Rua Tiradentes, 139	Centro	Cedro	LAP 2	-7,720008	-39,236186
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525828 ETE MAXIMIANO ACCIOLY CAMPOS  GRE 04	Avenida General Manoel Rabelo S/N	Jaboatão Centro	Jaboatão dos Guararapes	LAP 2	-8,11202	-35,013048
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124475 JEREM BRIGADEIRO EDUARDO GOMES - RECIFE GRE 02	Rua Barão de Souza Leão S/N	Boa Viagem	Recife	LAP 2	-8,132385	-34,908316
SECRETARIA DE EDUCAÇÃO E ESPORTES	26188040 ETE PROFº ANTÔNIO CARLOS GOMES DA COSTA GRE 01	Rua Mq Pombal	Santo Amaro	Recife	LAP 2	-8,049688	-34,882877
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024551 JEREM CONEGO OLIMPIO TORRES GRE 12	Rua Jacinto Amorim, S/N	Centro	Tuparetama	LAP 2	-7,603756	-37,304962
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105225 JEREM DESEMBARGADOR CARLOS XAVIER PAES BARRETTO GRE 03	Rua Carlos Barreto - Loteamento Redenção S/N		Igarassu	LAP 2	-7,838806	-34,910364
SECRETARIA DE EDUCAÇÃO E ESPORTES	26037700 ESCOLA SANTA MARIA GRE 14	Rua Estudante, 188	Centro	Lagoa Grande	LAP 2	-8,992628	-40,271532
SECRETARIA DE EDUCAÇÃO E ESPORTES	26012081 JEREM AGRICOLA DE UMAS GRE 15	Sítio Varzea Redonda, S/N	Centro	Salgueiro	LAP 1	-8,18027439	-39,29498474
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027828 JEREM PEDRO BEZERRA DE MELO GRE 11	Rua Severino Francisco da Silva, S/N	Centro	Ibimirim	LAP 2	-8,534383	-37,695221
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058650 ESCOLA ESTADUAL INDÍGENA JOSÉ ALVES DE CARVALHO GRE 11	Aldeia Bananeiras, s/n	Zona Rural	Pesqueira	LAP 1	-8,368735	-36,79751
SECRETARIA DE EDUCAÇÃO E ESPORTES	26074362 ESCOLA PE. ANTÔNIO CALLOU DE ALENCAR GRE 10	Rua Alto da Parasita, 208	Centro	Canhotinho	LAP 2	-8,884166	-36,191749
SECRETARIA DE EDUCAÇÃO E ESPORTES	26182629 ESCOLA ESTADUAL NOSSA SENHORA DAS GRACAS - RECIFE GRE 02	Av Liberdade S/N		Recife	LAP 1	-8,081969	-34,961443
SECRETARIA DE EDUCAÇÃO E ESPORTES	26045435 ESCOLA ESTADUAL INDÍGENA PEDRO BEZERRA DA SILVA GRE 11	Sítio Pau Ferro Grosso, 1188	Zona Rural	Buque	LAP 1	-8,67976	-37,16873
SECRETARIA DE EDUCAÇÃO E ESPORTES	26017598 ESCOLA ESTADUAL JOAQUIM ALVES DE FREITAS GRE 12	Rua José Barros Pereira, S/N	Centro	Iguaraci	LAP 1	-7,835155	-37,514085

SECRETARIA DE EDUCAÇÃO E ESPORTES	26022850 JEREM NOSSA SENHORA DE LOURDES GRE 12	Rua Luiz Carolino Siqueira, 128	Centro	Solidão	LAP 2	-7,601454	-37,648395
SECRETARIA DE EDUCAÇÃO E ESPORTES	26133949 JEREM PROFª CARLOTA BRECKENFELD GRE 12	Rua Dr Fausto Campos, 222	Centro	Tabira	LAP 2	-7,590078	-37,540358
SECRETARIA DE EDUCAÇÃO E ESPORTES	26094878 ESCOLA MADRE LUCILA MAGALHAES GRE 06	Rua 3, 94	Vila da Cohab	Vitória de Santo Antão	LAP 2	-8,12398	-35,287988
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075997 ESCOLA SENADOR ADERBAL JUREMA - GARANHUNS GRE 10	Rua Padre Agomar Valença, S/N	Heliópolis	Garanhuns	LAP 2	-8,877936	-36,469372
SECRETARIA DE EDUCAÇÃO E ESPORTES	26071606 JEREM CORONEL JOÃO FRANCISCO GRE 05	Rua Alcedo Marrocos, S/N	Centro	São Vicente Férrer	LAP 2	-7,587872	-35,491154
SECRETARIA DE EDUCAÇÃO E ESPORTES	26067803 JEREM MANOEL GONCALVES DE LIMA GRE 08	Rua Joao De Moura Borba, 306	Centro	Cumaru	LAP 2	-8,008791	-35,70126
SECRETARIA DE EDUCAÇÃO E ESPORTES	26104229 JEREM PROFª CARLOS JOSE DIAS DA SILVA GRE 07	Rua Lúcio Florentino, 51	São José da Coroa Grande	São José da Coroa Grande	LAP 2	-8,889644	-35,151304
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059177 ESCOLA ESTADUAL INDÍGENA JOSÉ NOGUEIRA NETO GRE 11	Aldeia Cabo do Campo - Pesqueira/PE		Pesqueira	LAP 1	-8,361025	-36,918397
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040301 ESCOLA ESTADUAL INDÍGENA ROSILDA SABAS DE SOUZA GRE 13	Aldeia Vila Serra Arapuã, S/N	Território Indígena Pankará	Carnaubeira da Penha	LAP 1	-8,3206	-38,74147
SECRETARIA DE EDUCAÇÃO E ESPORTES	26064006 ESCOLA PROFª MARIA LÚCIA ALVES GRE 09	Rua Professora Ivani Batista Da Silva, 313	Nova Santa Cruz	Santa Cruz do Capibaribe	LAP 2	-7,94642	-36,211545
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027615 ESCOLA IRACEMA MOURA DE MORAES VERAS GRE 11	Rua Projetada, S/N	Centro	Ibimirim	LAP 1	-8,534383	-37,695221
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186985 ESCOLA ESTADUAL PROFª ODETE DE ANDRADA ALVES GRE 11	LOTEAMENTO NOVO PORTAL	Prado	Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036215 ESCOLA NÚCLEO DE MORADORES - 9 GRE 14	Rua E, S/N	N9	Petrolina	LAP 2	-9,334246	-40,508899
SECRETARIA DE EDUCAÇÃO E ESPORTES	26408643 JEREM PROFª BENEDITA DE MORAIS GUERRA GRE 05	Av. José Inácio, S/N	Centro	Macaparana	LAP 2	-7,550037	-35,445811
SECRETARIA DE EDUCAÇÃO E ESPORTES	26190737 ETE CHICO SCIENCE GRE 03	Avenida das Acácias	Rio Doce	Olinda	LAP 2	-7,959149	-34,844384
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088606 JEREM EMILIANO PEREIRA BORGES GRE 05	Av. Agamenon Magalhães, 3535	Centro	Ferreiros	LAP 2	-7,450199	-35,243009
SECRETARIA DE EDUCAÇÃO E ESPORTES	26061724 ESCOLA ELPIDIO BARBOSA MACIEL GRE 10	Av. Bento Crespo, S/N	Centro	São Bento do Una	LAP 2	-8,522382	-36,444074
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107562 JEREM CONSELHEIRO SAMUEL MAC DOWELL GRE 04	Av. Tiradentes Nº 455	Jardim Primavera	Camaragibe	LAP 2	-8,012729	-34,969306
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999911 Centro Esportivo de Petrolina Secret	Av. Monsenhor Angelo Sampaio, S/N	Areia Branca	Petrolina	LAP 1	-9,384546	-40,489025
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106612 ESCOLA MARECHAL COSTA E SILVA GRE 03	Av. Marechal Costa E Silva, Nº 207	Caetés Velho	Abreu e Lima	LAP 2	-7,907768	-34,911687
SECRETARIA DE EDUCAÇÃO E ESPORTES	26093570 JEREM PROFª BARROS GUIMARAES GRE 06	Av. Djalma Dutra, 238	Centro	Glória do Goitá	LAP 2	-8,00164	-35,293905

SECRETARIA DE EDUCAÇÃO E ESPORTES	26117274 EREM MANUEL BASTOS TIGRE GRE 03	Av Palmares, 0	Arthur Lundgren Um	Paulista	LAP 2	-7,934701	-34,888326
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113805 EREM PINTOR MANOEL BANDEIRA GRE 03	Rua Francisco Abrozio Barros Leite, S/N	Bairro Novo	Olinda	LAP 1	-7,997989	-34,839294
SECRETARIA DE EDUCAÇÃO E ESPORTES	26021927 EREM IRNERO IGNACIO GRE 12	Rua Valdemar Ignácio Oliveira, S/N	Boroborema	Serra Talhada	LAP 2	-7,984618	-38,301147
SECRETARIA DE EDUCAÇÃO E ESPORTES	26008181 EREM PRESIDENTE MEDICI - MOREILÂNDIA GRE 15	Rua PEDRO RIBEIRO, 10960	Centro	Moreilândia	LAP 2	-7,626689	-39,553361
SECRETARIA DE EDUCAÇÃO E ESPORTES	26178435 EREM MARIA VIEIRA MULITERNO GRE 03	Rua Alto Bela Vista, S/N	Centro	Abreu e Lima	LAP 2	-7,908553	-34,897462
SECRETARIA DE EDUCAÇÃO E ESPORTES	26041910 EREM PROFª MARIA DE MENEZES GUIMARAES GRE 13	Rua Antonio Cabral Campos, S/N	Centro	Itacuruba	LAP 2	-8,727683	-38,684773
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128586 ESCOLA SAO JUDAS TADEU GRE 01	Rua Marcilio Dias, 591	Agua Fria	Recife	LAP 2	-8,019572	-34,884473
SECRETARIA DE EDUCAÇÃO E ESPORTES	26018977 ESCOLA TOME FRANCISCO DA SILVA GRE 12	Rua Jose Francisco Nunes, 1048	Quixabá	Carnaíba	LAP 1	-7,711078	-37,915698
SECRETARIA DE EDUCAÇÃO E ESPORTES	26061643 EREM RODOLFO PAIVA GRE 10	Rua João Pessoa, S/N	Centro	São Bento do Una	LAP 2	-8,52328272	-36,44340893
SECRETARIA DE EDUCAÇÃO E ESPORTES	99999904 CEE - CONSELHO ESTADUAL DE EDUCACAO Secret	Av Rui Barbosa, 1559	Graças	Recife	LAP 1	-8,051989	-34,896413
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127512 EREM SENADOR NOVAES FILHO GRE 02	Rua Maria Lacerda, S/N	Várzea	Recife	LAP 2	-8,04812	-34,961331
SECRETARIA DE EDUCAÇÃO E ESPORTES	26092298 EREM AGAMENON MAGALHAES GRE 05	Rua Joaquim Pereira Borba, S/N	Centro	Tracunhaém	LAP 2	-8,33024093	-36,14439352
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106337 ESCOLA PROFª GERCINA FERNANDES RODRIGUES GRE 03	Rua São João, 27	Centro	Itapissuma	LAP 2	-7,773591	-34,89218
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054809 EREM PADRE ZACARIAS TAVARES GRE 09	Rua Rocha Pombo, S/N	Salgado	Caruaru	LAP 2	-8,275833	-35,964736
SECRETARIA DE EDUCAÇÃO E ESPORTES	26005115 EREM FERNANDO BEZERRA GRE 16	Rua Major Rufino José Da Cunha, 248	Centro	Ouricuri	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26041570 ESCOLA ESTADUAL INDIGENA TIBURCIO LIMA GRE 13	ALDEIA FAVELEIRA		Floresta	LAP 1	-8,59693	-38,57435
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107546 EREM ANTONIO CORREIA DE ARAUJO GRE 04	Av. Pernambuco, Nº82	Bairro Dos Estados	Camaragibe	LAP 2	-8,025961	-34,980894
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058634 ESCOLA ESTADUAL INDÍGENA JATOBÁ GRE 11	Aldeia Jatobá	Zona Rural	Pesqueira	LAP 1	-8,291442	-36,797433
SECRETARIA DE EDUCAÇÃO E ESPORTES	26100525 EREM GOVERNADOR EDUARDO CAMPOS GRE 07	Trav. Manoel José da Costa Filho, S/N	Zona Rural	Joaquim Nabuco	LAP 2	-8,63027	-35,532118

SECRETARIA DE EDUCAÇÃO E ESPORTES	26146967 ESCOLA BEM-TE-VI GRE 14	Rua Agrovila IV, S/N	Centro	Orocó	LAP 2	-8,506921	-39,586763
SECRETARIA DE EDUCAÇÃO E ESPORTES	26184710 ESCOLA ESTADUAL INDIGENA VO SALU GRE 13	ALDEIA CACHOEIRA I	RURAL	Carnaubeira da Penha	LAP 1	-8,39208	-38,736819
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036010 ESCOLA POETA JOSE RAULINO SAMPAIO GRE 14	Rua 17, S/N	Pedro Raimundo	Petrolina	LAP 2	-9,370737	-40,525454
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097117 EREM ANTONIO ALVES DE ARAUJO GRE 07	Rua Samuel Coelho, S/N	Das Graças	Amaraji	LAP 2	-8,378065	-35,449001
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113872 ESCOLA PROFª DEANA CLARK XAVIER GRE 03	R. Paqueta Sapucaia, S/N		Olinda	LAP 2	-7,993906	-34,890014
SECRETARIA DE EDUCAÇÃO E ESPORTES	26137149 EREM STELA MARIA DOS SANTOS PINTO BARROS GRE 03	RUA LUIZ CARLOS ANASTÁCIO - 30	Centro	Abreu e Lima	LAP 2	-7,907097	-34,902454
SECRETARIA DE EDUCAÇÃO E ESPORTES	26068427 EREM PROFª MARILENE CHAVES DE SANTANA GRE 08	Av. Manoel Almeida, S/N	Centro	Feira Nova	LAP 2	-7,944711	-35,395992
SECRETARIA DE EDUCAÇÃO E ESPORTES	26185660 ETE GOVERNADOR EDUARDO CAMPOS GRE 10	Rua Projetada nº 01, S/N	Parque de exposição eládio porfirio de macedo	São Bento do Una	LAP 2	-7,9940717	-35,3769802
SECRETARIA DE EDUCAÇÃO E ESPORTES	26020963 EREM ANTONIO TIMOTEO GRE 12	Av. Antonio Timoteo De Lima, 334	Bom Jesus	Serra Talhada	LAP 2	-7,986982	-38,307234
SECRETARIA DE EDUCAÇÃO E ESPORTES	26086905 EREM JOAQUINA LIRA GRE 05	Rua Cleto Campelo, S/N	Centro	Aliança	LAP 2	-7,60428	-35,230946
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090899 ESCOLA DOM RICARDO VILELA GRE 05	Rua Odilon Estevão Da Paz, S/N	Centro	Nazaré da Mata	LAP 1	-7,73193811	35,21932513
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124912 ESCOLA ROBERTO SILVEIRA GRE 02	Av. Governador Roberto Silveira, N° 1	Jordão	Recife	LAP 1	-8,136753	-34,936589
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059193 ESCOLA ESTADUAL INDÍGENA SÃO GERALDO GRE 11	Aldeia Pelada, s/n	Zona Rural	Pesqueira	LAP 1	-8,35828683	-36,6981333
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122553 EREM EMBAIXADOR GILBERTO AMADO GRE 01	Rua Gaspar Regueira, 0	Hipodromo	Recife	LAP 2	-8,033092	-34,887967
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054140 EREM MARIA AUXILIADORA LIBERATO GRE 09	Rua 3, 80	Rendeiras	Caruaru	LAP 2	-8,289425	-35,97262
SECRETARIA DE EDUCAÇÃO E ESPORTES	26165783 EREM NOSSA SENHORA DA PENHA GRE 07	Rua Jose Barradas, 124	Centro	Gameleira	LAP 1	-8,584256	-35,387325
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075733 ESCOLA DUQUE DE CAXIAS GRE 10	Rua Caetes, S/N	Heliópolis	Garanhuns	LAP 2	-8,87132662	36,46056668
SECRETARIA DE EDUCAÇÃO E ESPORTES	26116367 ESCOLA PROFª GENEROSA GIL PEREZ GRE 03	Rua Ten Agnaldo De Lima, S/N	Nossa Senhora do O	Paulista	LAP 2	-7,896617	-34,832458
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098270 EREM COSTA AZEVEDO - CATENDE GRE 07	Praça Do Cinquentenário Jardim Diamante, S/N	Centro	Catende	LAP 1	-8,668749	-35,725766

SECRETARIA DE EDUCAÇÃO E ESPORTES	26108038 EREM TITO PEREIRA DE OLIVEIRA GRE 04	Estrada de Aldeia, Km 12, S/N	Araçá	Camaragibe	LAP 2	-7,967126	-35,00421
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106957 EREM LUIZ RODOLFO DE ARAUJO JUNIOR GRE 03	Av. Pastor Amoro De Sena	Caetés 1	Abreu e Lima	LAP 2	-7,91685547	34,91401899
SECRETARIA DE EDUCAÇÃO E ESPORTES	26084317 EREM MANOEL MOREIRA DA COSTA GRE 09	Rua Professor Jose De Alencar, S/N	Centro	Ibirajuba	LAP 1	-8,583871	-36,180825
SECRETARIA DE EDUCAÇÃO E ESPORTES	26186420 ESCOLA ESTADUAL INDIGENA NOSSA SENHORA DA CONCEICAO GRE 13	Aldeia Riacho Olho D'Água Povo Pankará, s/n - Zona Rural		Carnaubeira da Penha	LAP 1	-8,42848	-38,78036
SECRETARIA DE EDUCAÇÃO E ESPORTES	26079593 EREM REGINA PACIS - GARANHUNS GRE 10	Rua João Luis, 150	Centro	Palmeirina	LAP 2	-9,003732	-36,323872
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126192 ESCOLA GABRIELA MISTRAL GRE 01	Ladeira De Pedra	Água Fria	Recife	LAP 2	-8,016375	-34,900404
SECRETARIA DE EDUCAÇÃO E ESPORTES	26072149 EREM CORONEL JOSE ABILIO GRE 10	Av. 15 de Novembro, S/N	Centro	Bom Conselho	LAP 2	-9,16218904	-36,6780686
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106582 EREM GENERAL ABREU E LIMA GRE 03	Av. Dq Caxias, 660	Centro	Abreu e Lima	LAP 2	-7,906391	-34,901254
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040646 ESCOLA ESTADUAL INDIGENA EMILIANO QUIRINO DE SÁ GRE 13	Aldeia Cachoeira I	Povo Atikum	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26132001 EREM ARQUIPELAGO FERNANDO DE NORONHA GRE 01	Floresta Nova, S/N	Rocas	Fernando de Noronha	LAP 1	-3,84695651	32,41460138
SECRETARIA DE EDUCAÇÃO E ESPORTES	26070260 EREM ABILIO DE SOUZA BARBOSA GRE 08	Rua Do Cruzeiro, S/N	Centro	Orobó	LAP 2	-7,75117542	35,60365786
SECRETARIA DE EDUCAÇÃO E ESPORTES	26095289 ETE JOSE JOAQUIM DA SILVA FILHO GRE 06	Rua Demócrito Cavalcanti, S/N	Livramento	Vitória de Santo Antão	LAP 2	-8,117325	-35,297635
SECRETARIA DE EDUCAÇÃO E ESPORTES	08999999 GRE 08 - Vale do Capibaribe / Limoeiro Secret	Av. Jerônimo Heráclio, 234	Centro	Limoeiro	LAP 1	-7,874219	-35,445098
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040808 ESCOLA ESTADUAL INDIGENA ANA NUNES DA SILVA GRE 13	Aldeia Lajes, S/N	Povo Pankara	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024780 ESCOLA LIONS ANTONIO MORENO GRE 11	Rua L Cohab I, N 19 - Boa Vista	Boa Vista	Arcoverde	LAP 2	-8,415947	-37,036857
SECRETARIA DE EDUCAÇÃO E ESPORTES	26009544 ESCOLA ESTADUAL INDIGENA ANTONIO HONORIO SOBRINHO GRE 13	Aldeia Quixabá, s/n	Território Indígena Atikun	Carnaubeira da Penha	LAP 1	-8,3011272	-38,7099573
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089505 EREM FREI ORLANDO GRE 05	Av. Tenente Fontoura, 226	Centro	Itambé	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011948 ESCOLA ESTADUAL INDIGENA PROFESSOR ANTONIO PEDRO DOS SANTOS GRE 15	ALDEIA RODEADOR, ZONA RURAL		Salgueiro	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26010100 EREM ANDRE NUNES GRE 15	Rua Eliseu Campos, S/N	Joaquim Bezerra de Carvalho	Mirandiba	LAP 2	-8,121832	-38,729856
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111195 ESCOLA PEDRO BARROS FILHO GRE 04	Rua Rocine Roosevelt De Albuquerque, S/N		Jaboatão dos Guararapes	LAP 2	-8,178535	-34,920967
SECRETARIA DE EDUCAÇÃO E ESPORTES	26031884 ESCOLA ESTADUAL INDIGENA MARTILIANO RIBEIRO DE SOUZA GRE 14	Aldeia Umbuzeiro, S/N	Ilha da Assunção	Cabrobó	LAP 1		

SECRETARIA DE EDUCAÇÃO E ESPORTES	26091542 ESCOLA JOAO CAVALCANTI PETRIBU GRE 05	Travessa Dois Irmãos (A) , 68	Alto do Cruzeiro	Paudalho	LAP 2	-7,899057	-35,18062
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058782 ESCOLA ESTADUAL INDÍGENA NOSSA SENHORA DO CARMO GRE 11	Aldeia Afetos	Zona Rural	Pesqueira	LAP 1	-8,321425	-36,766196
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107678 ESCOLA MINISTRO JARBAS PASSARINHO GRE 04	Rua Jasmin, 20	Centro	Camaragibe	LAP 2	-8,018088	-34,984707
SECRETARIA DE EDUCAÇÃO E ESPORTES	26091267 EREM HERCULANO BANDEIRA GRE 05	Av. Marechal Deodoro, 780	Centro	Paudalho	LAP 2	-7,89497571	-35,18006016
SECRETARIA DE EDUCAÇÃO E ESPORTES	26075385 EREM FRANCISCO MADEIROS GRE 10	Rua Juliao Cavalcante, S/N	Magano	Garanhuns	LAP 2	-8,88601	-36,50336
SECRETARIA DE EDUCAÇÃO E ESPORTES	26027917 EREM ANTONIO GUILHERME DIAS LIMA GRE 11	Rua Cicero Torres, 152	Centro	Inajá	LAP 2	-8,90168626	-37,82433292
SECRETARIA DE EDUCAÇÃO E ESPORTES	26056550 ESCOLA AARAO LINS DE ANDRADE GRE 06	Rua Marechal Deodoro Da Fonseca, S/N	Centro	Gravatá	LAP 2	-8,202607	-35,572894
SECRETARIA DE EDUCAÇÃO E ESPORTES	26105250 EREM EURICO PFISTERER GRE 03	R. Jacob Pinto De Freitas N°209		Igarassu	LAP 2	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106388 EREM EURIDICE CADAVAL GRE 03	Frei Serafim, N°262	Centro	Itapissuma	LAP 2	-7,773832	-34,898773
SECRETARIA DE EDUCAÇÃO E ESPORTES	26008505 ESCOLA MARIA LUIZA DE BRITO FERREIRA GRE 16	Rua Santa Luzia, 121	Vila de Caririmirim	Moreilândia	LAP 1	-7,55520697	-39,49868881
SECRETARIA DE EDUCAÇÃO E ESPORTES	26025280 ESCOLA SANTA CECILIA GRE 11	Av. Pinto De Campos, 850	São Miguel	Arcoverde	LAP 1	-8,425295	-37,060116
SECRETARIA DE EDUCAÇÃO E ESPORTES	26045745 EREM DUQUE DE CAXIAS GRE 11	Rua São João, 100	Centro	Buíque	LAP 2	-8,621863	-37,149179
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090910 EREM MACIEL MONTEIRO GRE 05	Rua Bom Jesus, S/N	Centro	Nazaré da Mata	LAP 2	-7,741215	-35,22537
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040344 ESCOLA ESTADUAL INDIGENA MANOEL VICENTE DA SILVA GRE 13	ALDEIA MASSAPÉ - TERRITÓRIO INDÍGENA PANKARÁ	ZONA RURAL	Carnaubeira da Penha	LAP 1	-8,22078	-38,39495
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115883 EREM DE PAULISTA GRE 03	Rua Frei Caneca, S/N	Vila Torres Galvão	Paulista	LAP 2	-7,952574	-34,873553
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124831 ESCOLA PADRE LEBRET GRE 02	Av. Angra Dos Reis S/N	Ur2 - Cohab	Recife	LAP 2	-8,12043	-34,956097
SECRETARIA DE EDUCAÇÃO E ESPORTES	26037599 ESCOLA PROFª JUDITH GOMES DE BARROS GRE 14	Av. Nino Coelho, 509	Cohab	Santa Maria da Boa Vista	LAP 2	-8,803893	-39,824095
SECRETARIA DE EDUCAÇÃO E ESPORTES	26090759 EREM BRIGADEIRO EDUARDO GOMES GRE 05	Av. João Francisco, 301	Centro	Macaparana	LAP 2	-7,552688	-35,448724
SECRETARIA DE EDUCAÇÃO E ESPORTES	26126605 ESCOLA TOME GIBSON GRE 01	Av Ver Otacilio Azevedo, 0	Brejo De Beberibe	Recife	LAP 2	-7,99206886	-34,93541377

SECRETARIA DE EDUCAÇÃO E ESPORTES	26181665 ESCOLA ESTADUAL PADRE ANDRE ALBERT COOPMAN GRE 07	PRESIDIO DR RORENILDO DA ROCHA LEAO, S/N	Zona Rural	Palmares	LAP 1	-8,683215	-35,570313
SECRETARIA DE EDUCAÇÃO E ESPORTES	26181320 ESCOLA ESTADUAL DR. MIGUEL ARRAES DE ALENCAR GRE 07	Rua CARDOZO DA FONTE, S/N	Centro	Sirinhaém	LAP 1	-8,615283	-35,110877
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123533 ESCOLA MONSENHOR ALVARO NEGROMONTE GRE 02	R. 11 de Agosto, S/N	Totó	Recife	LAP 2	-8,077821	-34,971469
SECRETARIA DE EDUCAÇÃO E ESPORTES	26181657 ESCOLA ESTADUAL DIRCELIO FERREIRA DE PAIVA JUNIOR GRE 11	Rua ILDA PACHECO S/N	Novo Arcoverde	Arcoverde	LAP 1	-8,400064	-37,069996
SECRETARIA DE EDUCAÇÃO E ESPORTES	26084201 EREM PROFª MARIA DE LOURDES TEMPORAL GRE 09	Av. Agamenon Magalhães, 70	Centro	Cupira	LAP 2	-8,611831	-35,949608
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113830 EREM PROFª CÂNDIDO PESSOA GRE 03	Rua Lauro Diniz, S/N	Peixinhos	Olinda	LAP 2	-8,015315	-34,868851
SECRETARIA DE EDUCAÇÃO E ESPORTES	26103745 EREM WILSON DE ANDRADE BARRETO GRE 07	Praca Des. Carlos Chavier Paz Barreto, S/N	Campo	Rio Formoso	LAP 2	-8,659736	-35,153827
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033836 CENTRO EJA JOAO BARRACAO GRE 14	Av. Integração, S/N	Gercino Coelho	Petrolina	LAP 2	-9,391794	-40,485922
SECRETARIA DE EDUCAÇÃO E ESPORTES	26036118 EREM JESUINO ANTONIO DAVILA GRE 14	Rua 12, S/N	João de Deus	Petrolina	LAP 2	-9,364671	-40,541823
SECRETARIA DE EDUCAÇÃO E ESPORTES	26127300 EREM DIARIO DE PERNAMBUCO GRE 02	Rua Costa Sepulveda, 0	Engenho Do Meio	Recife	LAP 2	-8,053766	-34,942635
SECRETARIA DE EDUCAÇÃO E ESPORTES	26437724 ESCOLA DOM HELDER CÂMARA GRE 03	Br 101 Norte Km 32.4, S/N	Tabatinga	Igarassu	LAP 1	-7,810976	-34,920146
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125943 EREM MONSENHOR MANOEL MARQUES GRE 01	RUA DESEMBARGADOR ERÁCLITO CAVALCANTE, S/N	ALTO JOSE DO PINHO	Recife	LAP 2	-8,023078	-34,90793
SECRETARIA DE EDUCAÇÃO E ESPORTES	26087375 EREM JAIME COELHO GRE 05	Av. João Teobaldo De Azevedo, S/N	Centro	Buenos Aires	LAP 2	-7,718034	-35,32724
SECRETARIA DE EDUCAÇÃO E ESPORTES	26074311 EREM JERONIMO GUEIROS GRE 10	Rua Quintino Bocaiuva, S/N	Centro	Canhotinho	LAP 2	-8,874747	-36,197422
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113392 EREM DESEMBARGADOR RENATO FONSECA GRE 03	Rua Parana, Sn	Jardim Brasil	Olinda	LAP 1	-8,007703	-34,866139
SECRETARIA DE EDUCAÇÃO E ESPORTES	26083639 EREM QUINTINO BOCAIUVA GRE 06	Rua Oscar Eugenio, 57	Centro	Camocim de São Félix	LAP 2	-8,361739	-35,764268
SECRETARIA DE EDUCAÇÃO E ESPORTES	26125048 ETE JOAO BEZERRA GRE 02	Rua Francisco Valpasso, 0	Brasília Teimosa	Recife	LAP 2	-8,085063	-34,883072
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111012 EREM FELIPE CAMARAO GRE 04	Rua Maria Do Carmo S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,162639	-34,928943
SECRETARIA DE EDUCAÇÃO E ESPORTES	26082020 EREM JOSE LINS DE FIGUEIREDO GRE 09	Rua Siqueira Campos, 166	Centro	Altinho	LAP 1	-8,491533	-36,059034

SECRETARIA DE EDUCAÇÃO E ESPORTES	26188538 ETE ARIANO VILAR SUASSUNA - GARANHUNS GRE 10	Av. Bom Pastor, S/N	Boa Vista	Garanhuns	LAP 2	-8,905708	-36,495047
SECRETARIA DE EDUCAÇÃO E ESPORTES	26028018 ESCOLA ESTADUAL INDIGENA EMIDIO PEREIRA LIMA GRE 11	Sítio Tear		Inajá	LAP 1	-8,81024	-37,760233
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059231 ESCOLA ESTADUAL INDIGENA NOSSA SENHORA APARECIDA - PESQUEIRA GRE 11	ALDEIA PAU FERRO	ZONA RURAL	Pesqueira	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042479 ESCOLA ESTADUAL INDIGENA PANKARARUS GRE 13	ALDEIA SACO DOS BARROS, SN	Zona Rural	Jatobá	LAP 1	-9,12677297	-38,21146469
SECRETARIA DE EDUCAÇÃO E ESPORTES	26169746 ESCOLA ESTADUAL INDIGENA CACHOEIRA II GRE 13	Aldeia Tupan, S/N	Povo Atikum	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26128594 EREM SAO MIGUEL GRE 01	Segunda Travessa Sirigi S/N	Alto Do Mandu	Recife	LAP 1	-8,023768	-34,929328
SECRETARIA DE EDUCAÇÃO E ESPORTES	26172712 EREM GINASIO PERNAMBUCANO - AURORA GRE 01	Rua da Aurora, 703	Boa Vista	Recife	LAP 2	-8,05803239	-34,87918434
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063999 EREM PADRE ZUZINHA GRE 09	Av. Vinte E Nove De Dezembro, 258	São Cristóvão	Santa Cruz do Capibaribe	LAP 2	-7,957193	-36,204858
SECRETARIA DE EDUCAÇÃO E ESPORTES	26133753 CENTRO DE REABILITAÇÃO E EDUCAÇÃO ESPECIAL LIONS CLUBE GRE 10	Rua Manoel Borba, 168	Centro	Garanhuns	LAP 2	-8,890121	-36,495424
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123770 ESCOLA HEROIS DA RESTAURACAO GRE 02	Rua Oiticiça Lins S/N - M Vila Cardeal	Areias	Recife	LAP 2	-8,097719	-34,93511
SECRETARIA DE EDUCAÇÃO E ESPORTES	26115999 EREM JOSE MANUEL DE QUEIROZ GRE 03	Rua Rui Barbosa, 558	Janga	Paulista	LAP 1	-7,946435	-34,828336
SECRETARIA DE EDUCAÇÃO E ESPORTES	26158990 ESCOLA ESTADUAL INDIGENA ALDEIA ESTREITO GRE 13	Aldeia Estreito, s/n		Carnaubeira da Penha	LAP 1	-8,3206	-38,74147
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058561 ESCOLA ESTADUAL INDIGENA CANA BRAVA GRE 11	ALDEIA CANA BRAVA, ZONA RURAL, Pesqueira, PE		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129817 EREM DESEMBARGADOR ANTONIO DA SILVA GUIMARÃES GRE 04	Avenida Enestina Batista S/N	Pontezinha	Jaboatão dos Guararapes	LAP 2	-8,21893	-34,963342
SECRETARIA DE EDUCAÇÃO E ESPORTES	26081849 EREM PROFº JOSE CONSTANTINO GRE 09	Rua Cel. João Guilherme, 200	Centro	Agrestina	LAP 2	-8,455258	-35,947951
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107597 EREM FRANCISCO DE PAULA CORRÊA DE ARAÚJO GRE 04	R. Teodoro Borges, 150	Timbí	Camaragibe	LAP 2	-8,020742	-34,990898
SECRETARIA DE EDUCAÇÃO E ESPORTES	26033607 ESCOLA ESTADUAL INDIGENA SAO FELIX GRE 14	ILHA DE SAO FELIX		Orocó	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26135387 ESCOLA ESTADUAL INDIGENA NOSSA SENHORA DAS GRAÇAS - PESQUEIRA GRE 11	Aldeia Guarda	Zona Rural	Pesqueira	LAP 1	-8,358391	-36,700303
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034441 EREM MARECHAL ANTONIO ALVES FILHO GRE 14	Rua Barão do Amazonas, S/N	Jessino Coelho	Petrolina	LAP 2	-9,390518	-40,515958
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111403 EREM ADELAIDE PESSOA CAMARA GRE 04	Av. Barreto de Menezes, S/N	Conj Marcos Freire Muribeca II	Jaboatão dos Guararapes	LAP 2	-8,158544	-34,930092
SECRETARIA DE EDUCAÇÃO E ESPORTES	26097370 ESCOLA HELIO SANTIAGO RAMOS GRE 07	Av. Presidente Kennedy, 192	Centro	Barreiros	LAP 2	-8,813114	-35,189364
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059088 EREM PROFª MARGARIDA DE LIMA FALCAO GRE 11	Av. Paulo Pires, S/N	Centro	Pesqueira	LAP 2	-8,36521044	-36,70949515

SECRETARIA DE EDUCAÇÃO E ESPORTES	26128721 JEREM PROFº MARDONIO DE ANDRADE LIMA COELHO GRE 01	Rua Chan De Alegria	Bomba do Hemetério	Recife	LAP 2	-8,02086	-34,904707
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130203 JEREM SENADOR FRANCISCO PESSOA DE QUEIROZ GRE 04	Rua 27, S/N	Cohab	Cabo de Santo Agostinho	LAP 1	-8,237827	-34,992396
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058430 JEREM JOSE DE ALMEIDA MACIEL GRE 11	Rua Esio Araujo, S/N	Centro	Pesqueira	LAP 2	-8,352987	-36,683615

SECRETARIA DE EDUCAÇÃO E ESPORTES	26117290 EREM PADRE OSMAR NOVAES GRE 03	Rua Dr Jose Mariano, 0	Paratibe	Paulista	LAP 2	-7,932703	-34,898494
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042045 EREM DELMIRO GOUVEIA-PETROLANDIA GRE 13	Rua Valqueiro Barros, 335	Centro	Petrolândia	LAP 2	-8,9777572	-38,21902641
SECRETARIA DE EDUCAÇÃO E ESPORTES	26088053 EREM LIONS CLUBE DE CARPINA GRE 05	Rua Jose Machado Ferreira, S/N	Santo Antônio	Carpina	LAP 1	-7,841171	-35,261145
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040824 ESCOLA ESTADUAL INDIGENA ESPECIOSA BENIGNA DE BARROS GRE 13	Aldeia Brejinho	Povo Pankara	Carnaubeira da Penha	LAP 1	-8,320596	-38,7436607
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054850 EREM PROFº MARIO SETTE GRE 09	Av. Ruy Limeira Rosal, 30	Vassoural	Caruaru	LAP 2	-8,292912	-35,970218
SECRETARIA DE EDUCAÇÃO E ESPORTES	26063905 EREM LUIZ ALVES DA SILVA GRE 09	Av. Vinte E Nove De Dezembro, Nº 145	Centro	Santa Cruz do Capibaribe	LAP 2	-7,957211	-36,205183
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058758 ESCOLA ESTADUAL INDÍGENA SANTA RITA GRE 11	Aldeia Pe de Serra	Zona Rural	Pesqueira	LAP 1	-8,277201	-36,691557
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059479 ESCOLA ESTADUAL INDÍGENA JOSÉ TIMÓTEO DE LIMA GRE 11	ALDEIA COURO DANTAS	ZONA RURAL	Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111357 ESCOLA ZEQUINHA BARRETO GRE 04	RUA JOÃO FRAGOSO DE MEDEIROS, S/N	Piedade	Jaboatão dos Guararapes	LAP 1	-8,194845	-34,929101
SECRETARIA DE EDUCAÇÃO E ESPORTES	26018020 EREM ARISTAQUE JOSE DE VERAS GRE 12	Av. 20 de Dezembro, S/N	Centro	Ingazeira	LAP 1	-7,677776	-37,460096
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024667 CENTRO EJA CÍCERO FRANKLIN CORDEIRO GRE 11	Av. Gumercindo Cavalcante, S/N	São Cristóvão	Arcoverde	LAP 2	-8,412382	-37,068985
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058863 ESCOLA ESTADUAL INDÍGENA VICÊNCIA DE SOUZA LIMA GRE 11	Fazenda Santa Clara, Zona Rural - Pesqueira/PE		Pesqueira	LAP 1	-8,356804	-36,696867
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042525 ESCOLA NOSSA SENHORA APARECIDA - JATOBA GRE 13	Rua Buique, S/N	Centro	Jatobá	LAP 1	-9,184689	-38,268955
SECRETARIA DE EDUCAÇÃO E ESPORTES	26130521 EREM ZUMBI DOS PALMARES GRE 04	Rua Dezessete, S/N, Loteamento Ilha	Ponte Dos Carvalhos	Cabo de Santo Agostinho	LAP 2	-8,235772	-34,987477
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124777 EREM OTHON BEZERRA DE MELO GRE 02	Rua Virgínia Heráclio, S/N	Ipsep	Recife	LAP 2	-8,108847	-34,923044
SECRETARIA DE EDUCAÇÃO E ESPORTES	26061112 EREM DR BENJAMIN CARACIOLO GRE 11	Rua 18 de Copacabana, 121	Centro	Sanharó	LAP 2	-8,363305	-36,559204
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058960 EREM CRISTO REI GRE 11	Rua Luiz Wilson De Sá Ferraz, 27	Prado	Pesqueira	LAP 2	-8,357421	-36,683804

SECRETARIA DE EDUCAÇÃO E ESPORTES	26042452 ESCOLA ESTADUAL INDIGENA LAGOINHA GRE 13	Aldeia Lagoinha	Área Rural	Petrolândia	LAP 1	-8,96186	-38,2237687
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110237 EREM SENADOR PETRONIO PORTELA GRE 04	Av Cd Pereira Carneiro	Sucupira	Jaboatão dos Guararapes	LAP 2	-8,1044	-34,96402
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129590 ESCOLA VARZEA FRIA GRE 04	Rua Tabelaio João Lago, S/N	Varzea Fria	São Lourenço da Mata	LAP 2	-7,999916	-35,027212
SECRETARIA DE EDUCAÇÃO E ESPORTES	26052792 EREM PRESIDENTE KENNEDY GRE 09	Praça Presidnete Kennedy, 175	Centro	Cachoeirinha	LAP 2	-8,490291	-36,23693

SECRETARIA DE EDUCAÇÃO E ESPORTES	26107651 EREM MARIA DA CONCEICAO DO REGO B LACERDA GRE 04	Rua Vale Do Jaguaribe, S/N	Teresopolis	Camaragibe	LAP 2	-8,0368387	34,97536147
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042096 ESCOLA ESTADUAL INDIGENA JOSE LUCIANO GRE 13	Aldeia Caldeirão, s/n	Povo Pankararu	Jatobá	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054043 EREM DOM MIGUEL DE LIMA VALVERDE GRE 09	Rua Do Vassoural, 175	Vassoural	Caruaru	LAP 2	-8,294699	-35,969054
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107961 ESCOLA PROFª NELSON CHAVES GRE 04	Av Luíza De Medeiros, 600	Tabatinga	Camaragibe	LAP 2	-7,999152	-34,977402
SECRETARIA DE EDUCAÇÃO E ESPORTES	26024730 EREM CARLOS RIOS GRE 11	Rua Maria José dos Santos Moreno, S/N	Centro	Arcoverde	LAP 2	-8,418157	-37,05847
SECRETARIA DE EDUCAÇÃO E ESPORTES	26012014 ESCOLA ESTADUAL INDIGENA SANTA LUZIA GRE 15	Aldeia Poço da Pedr, s/n - Zona Rural		Salgueiro	LAP 1		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26131684 EREM FREI OTTO GRE 04	Rua Secundino Herminio, S/N,	Centro	Ipojuca	LAP 1	-8,056457	-34,923414
SECRETARIA DE EDUCAÇÃO E ESPORTES	26110229 EREM ODETE ANTUNES GRE 04	Rua Lagoa Do Abrigo Nº 01	Cavaleiro	Jaboatão dos Guararapes	LAP 1	-8,082182	-34,978285
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011395 ESCOLA ESTADUAL INDIGENA LUCIO QUIRINO DE FARIAS GRE 15	Aldeia Angico dos Lúcios, s/n	Zona Rural	Salgueiro	LAP 1	-8,04756	-34,876961
SECRETARIA DE EDUCAÇÃO E ESPORTES	26055368 ESCOLA IRMA SONIA GRE 09	Rua Prof José Leão, 567	Maurício de Nassau	Caruaru	LAP 1	-8,277383	-35,96836
SECRETARIA DE EDUCAÇÃO E ESPORTES	26014670 EREM MONSENHOR ANTONIO DE PADUA SANTOS GRE 12	Rua Antônio Alves Dos Santos, 220	Centro	Afogados da Ingazeira	LAP 2	-7,754137	-37,6356
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123576 EREM PRESIDENTE HUMBERTO CASTELO BRANCO GRE 02	Av. Dr. José Rufino, 2993	Tejipió	Recife	LAP 2	-8,09139	-34,949422
SECRETARIA DE EDUCAÇÃO E ESPORTES	26155516 ESCOLA ESTADUAL INDIGENA APINAGE GRE 13	ALDEIA CARRAPATEIRA, S/N	AREA INDIGENA	Jatobá	LAP 1	-9,19301	-38,21109
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040786 ESCOLA ESTADUAL INDIGENA MANOEL MIGUEL DO NASCIMENTO GRE 13	Quilombo Indígena Tiririca, s/n - Zona Rural		Carnaubeira da Penha	LAP 1	-8,45508	-38,78585
SECRETARIA DE EDUCAÇÃO E ESPORTES	26177013 EREM DE BEZERROS GRE 06	Av. Juca Soares Cardoso, Br 232 - Km 98, S/N	Distrito Industrial	Bezerros	LAP 2	-8,234903	-35,722682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26111411 ESCOLA AMOR DIVINO GRE 04	Endereço Rua S Bento, 835	Jardim Jordao	Jaboatão dos Guararapes	LAP 1	-8,14549	-34,932701

SECRETARIA DE EDUCAÇÃO E ESPORTES	26124670 EREM MARECHAL EURICO GASPAR DUTRA GRE 02	Rua Sergio Buarque De Holanda, 279	Ibura	Jaboatão dos Guararapes	LAP 1	-8,131653	-34,965089
SECRETARIA DE EDUCAÇÃO E ESPORTES	26058952 EREM ELIZEU ARAUJO GRE 11	Rua Gleicerio, S/N	Centenário	Pesqueira	LAP 1	-8,364558	-36,694948
SECRETARIA DE EDUCAÇÃO E ESPORTES	26011069 EREM AURA SAMPAIO PARENTE MUNIZ GRE 15	Rua Perpetuo Socorro Ns, 1810	Nossa Sra. Aparecida	Salgueiro	LAP 2	-8,07233	-39,126417
SECRETARIA DE EDUCAÇÃO E ESPORTES	26015625 EREM ANTONIO GOMES DE LIMA GRE 12	Rua Manoel Belarmino de Souza, S/N	Centro	Calumbi	LAP 2	-7,941876	-38,152826

SECRETARIA DE EDUCAÇÃO E ESPORTES	26113562 EREM JERONIMO DE ALBUQUERQUE GRE 03	Av. Nápoles, S/N	Rio Doce Quarta Etapa	Olinda	LAP 2	-7,967575	-34,851237
SECRETARIA DE EDUCAÇÃO E ESPORTES	26123282 EREM JOAQUIM TAVORA GRE 02	Rua Real Da Torre	Madalena	Recife	LAP 2	-8,055562	-34,908835
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089424 EREM FREI CAMPO MAYOR GRE 05	Rua Projetada, 15	Loteamento Goulardi	Goiana	LAP 2	-7,55892948	-35,804186
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034832 EREM MONTEIRO LOBATO GRE 14	Rua Monteiro Lobato, S/N	Povoado de Izacolandia	Petrolina	LAP 2		
SECRETARIA DE EDUCAÇÃO E ESPORTES	26040506 ESCOLA ESTADUAL INDIGENA QUINTINO DE MENEZES GRE 13	Aldeia Casa Nova, S/N	Povo Pankará	Carnaubeira da Penha	LAP 1	-8,39208	-38,73682
SECRETARIA DE EDUCAÇÃO E ESPORTES	26124920 EREM SAO FRANCISCO DE ASSIS GRE 02	Rua Sargento Silvio D. Hollenbach, S/N	Imbiribeira	Recife	LAP 2	-8,103545	-34,909157
SECRETARIA DE EDUCAÇÃO E ESPORTES	26089238 ESCOLA CEL JOSE PINTO DE ABREU GRE 05	Av. Nunes Machado, S/N	Centro	Goiana	LAP 2	-7,558522	-34,996276
SECRETARIA DE EDUCAÇÃO E ESPORTES	26099489 EREM MONSENHOR JOAO RODRIGUES DE CARVALHO GRE 06	Rua Antonio Ramiro, S/N	Escada	Escada	LAP 2	-8,363091	-35,228912
SECRETARIA DE EDUCAÇÃO E ESPORTES	26119730 ESCOLA DE APLICACAO DO RECIFE GRE 02	Av. sport club do recife, 252	Madalena	Recife	LAP 2	-8,0606521	-34,90339536
SECRETARIA DE EDUCAÇÃO E ESPORTES	26098210 EREM ATHAYDE ACCIOLY LINS GRE 07	Rua Jucelino Cubchek de Oliveira, S/N	Centro	Catende	LAP 1	-8,667973	-35,721818
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122880 EREM PRESIDENTE ARTHUR DA COSTA E SILVA GRE 02	Rua Tejucupapo, N536	San Martin	Recife	LAP 2	-8,072383	-34,9227
SECRETARIA DE EDUCAÇÃO E ESPORTES	26525836 ETE ANTONIO ARRUDA DE FARIAS  GRE 08	Rua Antonio Heraclito Do Rego, S/N	Centro	Surubim	LAP 1	-7,83420305	-35,76322104
SECRETARIA DE EDUCAÇÃO E ESPORTES	26082861 EREM LEOBALDO SOARES DA SILVA GRE 06	Av. Joao Ferreira Junior, S/N	Nova Esperança	Barra de Guabiraba	LAP 2	-8,41864	-35,661852
SECRETARIA DE EDUCAÇÃO E ESPORTES	26122839 EREM OTHON PARAISO GRE 02	Av Manoel Gonçalves Da Luz - 140	Mustardinha	Recife	LAP 1	-8,066186	-34,917138
SECRETARIA DE EDUCAÇÃO E ESPORTES	26059398 ESCOLA ESTADUAL INDÍGENA ANTONIO ZUMBA GRE 11	Aldeia Viração, s/n	Zona Rural	Pesqueira	LAP 1	-8,36273	-36,73885
SECRETARIA DE EDUCAÇÃO E ESPORTES	26006499 ESCOLA PROFº TELESFORO SIQUEIRA GRE 16	Rua Coronel Aluisio Coelho, 88	Centro	Ouricuri	LAP 2	-7,884496	-40,081529
SECRETARIA DE EDUCAÇÃO E ESPORTES	26113279 ESCOLA CEL VALERIANO EUGENIO DE MELO GRE 03	Rua Francisco Gomes - S/N	Caixa D'água	Olinda	LAP 1	-7,996765	-34,901504

SECRETARIA DE EDUCAÇÃO E ESPORTES	26123517 EREM JOSE MARIANO GRE 02	Rua Dr Jose Rufino, 892	Areias	Recife	LAP 2	-8,087951	-34,932367
SECRETARIA DE EDUCAÇÃO E ESPORTES	26001900 ESCOLA JOAO CARLOS LOCIO DE ALMEIDA GRE 16	Rua Alvaro Campos, S/N	Centro	Bodocó	LAP 2	-7,780401	-39,942237
SECRETARIA DE EDUCAÇÃO E ESPORTES	26129086 EREM CONDE CORREA DE ARAUJO GRE 04	José De Alencar, Nº 20	Vila Do Reinado	São Lourenço da Mata	LAP 2	-7,991764	-35,044525

SECRETARIA DE EDUCAÇÃO E ESPORTES	26115050 ESCOLA JOAQUIM NABUCO - OLINDA GRE 03	Av Pres Kennedy, 55	Peixinhos	Olinda	LAP 2	-7,999532	-34,894426
SECRETARIA DE EDUCAÇÃO E ESPORTES	26034328 EREM DOM AVELAR BRANDAO VILELA GRE 14	Rua Projeto Nilo Coelho, S/N	Centro	Petrolina	LAP 1	-9,373415	-40,502658
SECRETARIA DE EDUCAÇÃO E ESPORTES	26050102 EREM JOAO MONTEIRO DE MELO GRE 09	Av. Sto Antonio, S/N	Santo Antônio	Belo Jardim	LAP 2	-8,337335	-36,430544
SECRETARIA DE EDUCAÇÃO E ESPORTES	26419831 ESCOLA ESTADUAL JOSÉ FERREIRA DA SILVA GRE 13	RODOVIA PE360, S/N	Centro	Floresta	LAP 1	-8,600728	-38,577553
SECRETARIA DE EDUCAÇÃO E ESPORTES	26038935 EREM MONSENHOR JOAO PIRES GRE 13	Rua Agamenon Magalhães, S/N	Centro	Belém de São Francisco	LAP 2	-8,751244	-38,963432
SECRETARIA DE EDUCAÇÃO E ESPORTES	26107996 ESCOLA VALE DAS PEDREIRAS GRE 04	Rua Perola, Sn	Jardim Primavera	Camaragibe	LAP 2	-8,007094	-34,965192
SECRETARIA DE EDUCAÇÃO E ESPORTES	26008548 ESCOLA HORTENCIO PEREIRA LIMA GRE 16	Rua Padre Cícero, S/N	Centro	Trindade	LAP 2	-7,76683	-40,269537
SECRETARIA DE EDUCAÇÃO E ESPORTES	26106213 ESCOLA DE JAGUARIBE GRE 03	Rua Ernesto José de Albuquerque Nº 87	Jaguaribe	Ilha de Itamaracá	LAP 1	-7,733396	-34,828186
SECRETARIA DE EDUCAÇÃO E ESPORTES	26025876 EREM OSMAR DE SOUZA FERRAZ GRE 11	Av. Osmar Feraz, S/N	Centro	Betânia	LAP 2	-8,27479	-38,035206
SECRETARIA DE EDUCAÇÃO E ESPORTES	26102552 EREM JOAO LOPES DE SIQUEIRA SANTOS GRE 07	Av. Mario Domingues, S/N	Centro	Ribeirão	LAP 2	-8,521755	-35,376501
SECRETARIA DE EDUCAÇÃO E ESPORTES	26006138 ESCOLA DOM IDILIO JOSE SOARES GRE 16	Av. Fernandes Bezerra, 1152	Centro	Ouricuri	LAP 2	-7,887774	-40,087115
SECRETARIA DE EDUCAÇÃO E ESPORTES	26013436 EREM NAPOLEÃO ARAÚJO GRE 15	Rua Napoleão Alves Araujo, S/N	Centro	São José do Belmonte	LAP 2	-7,99604725	38,62511855
SECRETARIA DE EDUCAÇÃO E ESPORTES	26042339 ESCOLA ESTADUAL INDIGENA SALAO GRE 13	ALDEIA SALAO ENTRE SERRAS	ZONA RURAL	Petrolândia	LAP 1	-8,395683	-39,610514
SECRETARIA DE EDUCAÇÃO E ESPORTES	26081180 EREM MONSENHOR ALFREDO DAMASO GRE 10	Rua Cel. Francisco Martins, S/N	Centro	Terezinha	LAP 1	-9,056624	-36,627493
SECRETARIA DE EDUCAÇÃO E ESPORTES	26054094 EREM FELISBERTO CARVALHO GRE 09	Av. Rui Limeira Rosalvo, S/N	Vassoural	Caruaru	LAP 2	-8,292112	-35,970282
SECRETARIA DE EDUCAÇÃO E ESPORTES	26182173 ESCOLA ESTADUAL MONSENHOR ADELMA DA MOTA VALENÇA GRE 10	FAZENDA NASCIMENTO, S/N	Zona Rural	Altinho	LAP 2	-8,8829776	36,48210632

SECRETARIA DE EDUCAÇÃO E ESPORTES	26111209 EREM PROFº BENEDITO CUNHA MELO GRE 04	Conjunto Praia Do Sol S/N	Barra De Jangada	Jaboatão dos Guararapes	LAP 2	-8,224572	-34,932416
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Petrolina	Av. das Nações, 55	Centro	Petrolina	LAP 1	-9,390835	-40,508391
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Núcleo Governo Presente - Cabo de Santo Agostinho	Segunda Travessa Rodrigues, 13	Gaibu	Cabo de Santo Agostinho	LAP 1	-8,33870342	-34,95636394
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Jaboatão	Rua MARIA HELENA, S/N	Cajueiro Seco	Jaboatão dos Guararapes	LAP 1	-8,169358	-34,932269
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - IBURA	Rua Jornalista Costa Pôrto - S/N	UR-II	Recife	LAP 1	-8,11061	-34,95941

SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	SEDSOH - Gppddh	Rua Floriano Peixoto, 141	São José	Recife	LAP 1	-8,065814	-34,88229
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Núcleo Governo Presente - Peixinhos	Av Presidente Kenedy, Centro da Moda Sala 302, bloco B	Peixinhos	Olinda	LAP 1	-8,011763	-34,874454
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	SEDSOH - Sec. de Justiça e Direitos Humanos	Rua Santo Elias, 535	Espinheiro	Recife	LAP 1	-8,046012	-34,891943
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Afogados	Estrada do Arraial, S/N, Chalé no Sítio da Trindade-Memorial da Democracia de PE	Casa Amarela	Recife	LAP 1	-8,071802	-34,910071
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Núcleo Governo Presente - Vitória	Rua Joaquim Nabuco, 366	Matriz	Vitória de Santo Antão	LAP 1	-8,114525	-35,291877
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Caruaru	Av. Amazonas, 168	Universitário	Caruaru	LAP 1	-8,273708	-35,965689
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Cajueiro	Rua Doutor Waldir Pessoa, S/N	Cajueiro	Recife	LAP 1	-8,089007	-34,905004
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Secretaria de Justiça e Direitos Humanos	PRAÇA DO ARSENAL DA MARINHA, S/N	BAIRRO DO RECIFE	Recife	LAP 1	-8,061026	-34,871269
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Núcleo Governo Presente - Palmares	Rua Ascenso Ferreira, 190	São Sebastião	Palmares	LAP 1	-8,67884	-35,583879
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Núcleo Governo Presente - Iputinga	Av Jornalista Possidônio Cavalcanti Basto, s/n	Iputinga	Recife	LAP 1	-8,030603	-34,931029
SECRETARIA DE JUSTIÇA E DIREITOS HUMANOS	Estação Governo Presente - Paulista	Praça Emílio Russel, S/N	Maranguape I	Paulista	LAP 1	-7,947341	-34,857295
SECRETARIA DE MEIO AMBIENTE E SUSTENTABILIDADE	Parque Dois Irmãos - Sede	Praça Farias Neves, S/N	Dois Irmãos	Recife	LAP 1	-8,013728	-34,944413
SECRETARIA DE MEIO AMBIENTE E SUSTENTABILIDADE	SEMAS - SECRETARIA DO MEIO AMBIENTE	Conselheiro Rosa e Silva, 1339	Aflitos	Recife	LAP 1	-8,039927	-34,899349
SECRETARIA DE MOBILIDADE E INFRAESTRUTURA	SEMOBI - Sede	AV. CRUZ GABUGÁ, 1111	SANTO AMARO	Recife	LAP 2	-8,044797	-34,875308

SECRETARIA DE MOBILIDADE E INFRAESTRUTURA	SEMOBI - Sede	AV. CRUZ GABUGÁ, 1111	SANTO AMARO	Recife	LAP 2	-8,04756	-34,876961
SECRETARIA DE MOBILIDADE E INFRAESTRUTURA	Aeródromo de Caruaru	Rua Oscar Laranjeira, s/n	Centro	Caruaru	LAP 1	-8,28468655	-36,1077796
SECRETARIA DE PLANEJAMENTO E GESTÃO	SEPLAG - Sede	Rua da Aurora, 1377	Santo Amaro	Recife	LAP 2	-8,052749	-34,875996
SECRETARIA DE PLANEJAMENTO E GESTÃO	Seplag - Nova Sede	Rua da Aurora, 1337	Santo Amaro	Recife	LAP 2		
SECRETARIA DE PROJETOS ESTRATÉGICOS	Secretaria de Projetos Estratégicos	Av. Rio Branco, 104	Bairro do Recife	Recife	LAP 1	-8,062653	-34,87238

SECRETARIA DE PROJETOS ESTRATÉGICOS	Anexo - SEPE	Rua Vinte e Quatro de Agosto	Centro - Recife	Recife	LAP 2		
SECRETARIA DE PROJETOS ESTRATÉGICOS	Anexo - SEPE	Rua Vinte e Quatro de Agosto	Centro - Recife	Recife	LAP 2		
SECRETARIA DE RECURSOS HÍDRICOS E DE SANEAMENTO	Secretaria de Recursos Hídricos e de Saneamento	Avenida Dr. Jayme da Fonte, 64 - 6º andar	Santo Amaro	Recife	LAP 1	-8,043492	-34,874702
SECRETARIA DE TURISMO	CENTRO DE CONVENÇÕES (SECRETARIA DE TURISMO)	AV COMPLEXO DE SALGADINHO, S/N	Cais do Apolo	Recife	LAP 2	-8,028741	-34,86821
SECRETARIA DE TURISMO	SETUR - Sede	Av. Agamenon Magalhães, 200	Salgadinho	Olinda	LAP 1	-8,032864	-34,870216
SECRETARIA ESTADUAL DE SAÚDE	Hospital Monsenhor Angelo Sampaio	Rua DOUTOR MARBACK, 760	Centro	Santa Maria da Boa Vista	LAP 1	-8,807059	-39,820763
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Agrestina	Rua Coronel Manoel Alves, S/N	Centro	Agrestina	LAP 1	-8,456852	-35,948963
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Tipo III - Barra de Jangada	Rua Cruz Alta - S/N	Barra de Jangada	Jaboatão dos Guararapes	LAP 2	-8,219104	-34,934078
SECRETARIA ESTADUAL DE SAÚDE	UNIDADE DE PRONTO ATENDIMENTO DE GOIANA	Rua Engenho Boa Vista, S/N	Freicheiras	Goiana	LAP 2	-7,569918	-35,023371
SECRETARIA ESTADUAL DE SAÚDE	HOSPITAL OTAVIO DE FREITAS - LINK BACKUP	RUA APRIGIO GUIMARÃES SN	TEJIPIO	Recife	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Santa Terezinha	Rua Bernado Nunes S/N	Centro	Santa Terezinha	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	Pemd V Geres Gerencia Regional Anexo	Rua Pedro Rocha, S/N	Heliópolis	Garanhuns	LAP 2	-8,88308	-36,486376
SECRETARIA ESTADUAL DE SAÚDE	Unidade Pernambucana de Atenção Especializada - UPAES Ouricuri	Av. Manoel Irineu de Araujo, S/N	Centro	Ouricuri	LAP 2	-7,8806635	-40,8925476
SECRETARIA ESTADUAL DE SAÚDE	SES-PE - SEDE	Rua Vinte e Quatro de Agosto, 209	Santo Amaro, Recife	Recife	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	SES-PE - SEDE	Rua Vinte e Quatro de Agosto, 209	Santo Amaro, Recife	Recife	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Condado	Rua Hermínio Mendonça, 175	Centro	Condado	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	Conselho Estadual de Saúde	Rua João Fernandes Vieira, N.º 518	Boa Vista	Recife	LAP 1	-8,052221	-34,892426
SECRETARIA ESTADUAL DE SAÚDE	Escola de Saúde de Pernambuco - ESPE	Rua 48, nº 224	Espinheiro	Recife	LAP 2	-8,04313	-34,891429
SECRETARIA ESTADUAL DE SAÚDE	HOSPITAL DA MULHER DO AGRESTE	JOSÉ RODRIGUES DE JESUS	INDIANÁPOLIS	Caruaru	LAP 1	-8,302713	-35,96274
SECRETARIA ESTADUAL DE SAÚDE	6º Geres - Ambulatorio - Farmacia	Rua das Acacias, SN	Centro	Arcoverde	LAP 2	-8,412498	-37,071132
SECRETARIA ESTADUAL DE SAÚDE	Hospital Metropolitano Oeste Pelopidas Silveira	Rodovia Br 232, S/N	Curado	Recife	LAP 2	-8,07233753	-34,95015801
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Triunfo	Avenida José Veríssimo dos Santos - 365	Guanabara	Triunfo	LAP 1	-7,835977	-38,106503

SECRETARIA ESTADUAL DE SAÚDE	UPA - Tipo III - Lagoa Encantada	Rua Vale do Itajai, S/N	Ibura	Recife	LAP 2	-8,128801	-34,949641
SECRETARIA ESTADUAL DE SAÚDE	UPAE-R (UNIDADE DE PRONTO ATENDIMENTO DE REABILITAÇÃO)	Av. Recife 801	Estância	Caruaru	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Ferreiros	Rua Travessa Oliveira Bezerra Cunha, 8	Centro	Ferreiros	LAP 1	-7,448812	-35,243085
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Lajedo	Rua João da Mata, 55	Centro	Lajedo	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	Hospital Geral do Sertão Gov. Eduardo Campos	BR 232, S/N	BR-232 - Serra Talhada, PE	Serra Talhada	LAP 1	-7,981335	-38,304978

SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Tipo III - São Lourenço da Mata	Avenida Dr. Francisco Correia, 2009	Pixete	São Lourenço da Mata	LAP 2	-7,991229	-35,049055
SECRETARIA ESTADUAL DE SAÚDE	8ª Geres - Petrolina	Av. Doutor Fernando Menezes De Góes, S/N	Centro	Petrolina	LAP 1	-9,395338	-40,501041
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Garanhuns	Av. CARUARU, 228	Heliópolis	Garanhuns	LAP 1	-8,884513	-36,488843
SECRETARIA ESTADUAL DE SAÚDE	Geres - Serra Talhada	Rua Antônio Alves De Oliveira, 2380	Ipsep	Serra Talhada	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	IX GERES ANEXO1	Praça VOLUNTARIO DA PATRIA, 350	Centro	Ouricuri	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Belo Jardim	Rua Coronel Antonio Marinho, 335	Ayrton Maciel	Belo Jardim	LAP 1	-8,332252	-36,415191
SECRETARIA ESTADUAL DE SAÚDE	Hospital São Sebastião	Av. Agamenon Magalhães, 1351	Maurício de Nassau	Caruaru	LAP 2	-8,269545	-35,976343
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Exu	Rua João Ribeiro, 95	Centro	Exu	LAP 1	-7,514421	-39,723011
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional Fernando Bezerra - Ouricuri	Rua Teobaldo Gomes Torres, 510	Centro	Ouricuri	LAP 2	-7,883332	-40,085005
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional de Palmares	Engenho Quilombo Dos Palmares - Br 101 - Sul, S/N	Km 185	Palmares	LAP 2	-8,669523	-35,574749
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Itapetim	Rua JOVINO LEITE, 100	Centro	Itapetim	LAP 1	-7,379097	-37,191308
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Caxanga	Av. Joaquim Ribeiro, S/N	Caxanga	Recife	LAP 2	-8,029815	-34,957759
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Jataúba	Rua Expedicionário Inácio Aleixo de Araújo - 33, Centro, Jataúba - PE	Centro	Jataúba	LAP 1	-8,04756	-34,876961
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Palmares	Avenida Miguel Jasseli	bairro do centro	Palmares	LAP 1	-8,684976	-35,596379
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Cumaru	Rua João de Moura Borba, S/N	Centro	Cumaru	LAP 1	-8,007555	-35,700148
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Itacuruba	Rua Cícero Delgado, 6	Centro	Itacuruba	LAP 1	-8,727978	-38,685232
SECRETARIA ESTADUAL DE SAÚDE	Hospital Belarmino Correia - Goiana	Praça Correia Picanço, S/N	Centro	Goiana	LAP 2	-7,558268	-35,002279
SECRETARIA ESTADUAL DE SAÚDE	Sec. Saude - Sede Bongi - LINK 2	Rua Vinte e Quatro de Agosto, 209	Santo Amaro	Recife	LAP 2	-8,0652047	-34,9230847
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional do Agreste - Waldomiro Ferreira	Br 232 - Km 130, S/N	Indianópolis	Caruaru	LAP 2	-8,307584	-35,968147
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Tipo III - Igarassu	Rodovia Br-101 Norte, S/N, Km-47	Cruz de Rebouças	Igarassu	LAP 1	-7,878806	-34,905346

SECRETARIA ESTADUAL DE SAÚDE	Hospital Getúlio Vargas - Cpl	Av . Gen. San Martins S/N	Cordeiro	Recife	LAP 1	-8,051784	-34,921264
SECRETARIA ESTADUAL DE SAÚDE	Hospital Getúlio Vargas - Backup	Av. General San Martin, S/N,	Cordeiro	Recife	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Hospital Getúlio Vargas - Backup	Av. General San Martin, S/N,	Cordeiro	Recife	LAP 1	-8,066978	-34,927393
SECRETARIA ESTADUAL DE SAÚDE	Hospital Otávio de Freitas	Rua Aprigio Guimarães, Sn	Tejipió	Recife	LAP 1	-8,087748	-34,960679
SECRETARIA ESTADUAL DE SAÚDE	9ª Geres - Ouricuri	Rua Hidelbrando Coelho, S/N	Centro	Ouricuri	LAP 2	-7,881701	-40,085353
SECRETARIA ESTADUAL DE SAÚDE	SES - UNIDADE PERNAMBUCANA DE ATENÇÃO ESPECIALIZADA - UPAES	Av. JOSÉ MARQUES FONTES, S/N	Indianópolis	Caruaru	LAP 2	-8,30074	-35,960519

SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Betânia	Rua Rufino Passos Jardim, S/N	Centro	Betânia	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	UNIDADE PERNAMBUCANA DE ATENÇÃO ESPECIALIZADA - SERRA TALHADA - UPAES	Rua 14 de julho, S/N	Centro	Serra Talhada	LAP 2	-7,980585	-38,294629
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Afrânio	Rua Afranio de Melo Franco, 57	Centro	Afrânio	LAP 1	-8,515442	-41,007362
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional Agamenon Magalhaes - Serra Talhada	Rua Comandante Superior, 955	Centro	Serra Talhada	LAP 1	-7,988515	-38,298727
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Bodocó	Av. Marechal Floriano Peixeira, 206	Centro	Bodocó	LAP 1	-7,781661	-39,94094
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Custódia	Rua Major Experidião de Sá, 320	Centro	Custódia	LAP 1	-8,660266	-35,15272
SECRETARIA ESTADUAL DE SAÚDE	Fusam - Sede (Link Principal)	Pca Oswaldo Cruz, 359	Soledade	Recife	LAP 2	-8,055234	-34,891508
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional do Agreste - Waldomiro Ferreira - Link Backup 2	BR 232 - KM 130 - Indianópolis, S/N	Indianópolis	Caruaru	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Brejão	Rua Capitão Francisco Furtado, 46	Centro	Brejão	LAP 1	-9,028654	-36,565732
SECRETARIA ESTADUAL DE SAÚDE	Hospital Agamenon Magalhães	Estrada Do Arraial, 2723	Estrada Do Arraial, Nº 2723 - Casa Amarela	Recife	LAP 2	-8,030216	-34,906933
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Flores	Rua Cleto Campelo, 180	Centro	Flores	LAP 1	-7,863523	-37,972763
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento -Tipo III - Jaboatão	Rua Leonardo da Vinci Nº 68	Curado li	Jaboatão dos Guararapes	LAP 1	-8,077964	-34,997979
SECRETARIA ESTADUAL DE SAÚDE	HOSPITAL MESTRE VITALINO - CARUARU	RODOVIA BR 104 KM 62,5 S/N	Caruaru	Caruaru	LAP 2	-8,2451792	-35,97425018
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Itaíba	Rua Constantino Lavrador, S/N	Centro	Itaíba	LAP 1	-8,94961109	-37,42314723
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional Inácio de Sá	Rua Antônio De Alencar Sampaio, 346	Planalto	Salgueiro	LAP 2	-8,057935	-39,113656
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Tipo III Engenho Velho	Avenida General Manoel Rabelo, S/N	Engenho Velho	Jaboatão dos Guararapes	LAP 2	-8,110909	-35,006673
SECRETARIA ESTADUAL DE SAÚDE	6ª Geres - Arcoverde	Rua Das Acácias, S/N	Centro	Arcoverde	LAP 1	-8,412498	-37,071132
SECRETARIA ESTADUAL DE SAÚDE	UPAES - UNIDADE DE PRONTO ATENDIMENTO DE SALGUEIRO	Rua JOÃO VERAS DE SIQUEIRA, S/N	Jardim Primavera	Salgueiro	LAP 1	-8,081273	-39,128888
SECRETARIA ESTADUAL DE SAÚDE	UPA - GARANHUS	RODOVIA BR 423, S/N	Centro	Garanhuns	LAP 2	-8,879388	-36,479578
SECRETARIA ESTADUAL DE SAÚDE	3ª Geres - Palmares	Av. LUIZ DE FRANÇA, 1320	Centro	Palmares	LAP 2	-8,68393743	-35,58823652

SECRETARIA ESTADUAL DE SAÚDE	Farmácia de Medicamentos Excepcionais - Caruaru	Rua Padre Félix Barreto, 20	Centro	Caruaru	LAP 2	-8,282131	-35,969672
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Catende	Rua Esmael Silva, 49	Centro	Catende	LAP 1	-8,66961	-35,719813
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Riacho das Almas	1ª Travessa José lima figueroa - 50	Centro	Riacho das Almas	LAP 1	-8,139817	-35,855924
SECRETARIA ESTADUAL DE SAÚDE	Unidade de Pronto Atendimento - Tipo - III - Paulista	Estrada Do Frio, N° 1000	Centro	Paulista	LAP 2	-7,948181	-34,890305
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Joaquim Nabuco	Rua da Aurora, 98	Centro	Joaquim Nabuco	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento- Tipoiii - Caruaru	Av. José Marques Ponte, S/N	Indianópolis	Caruaru	LAP 1	-8,301128	-35,960567
SECRETARIA ESTADUAL DE SAÚDE	Hospital da Restauração - Informática	Av. Prof. Agamenon Magalhães, S/N	Derby	Recife	LAP 2	-8,054264	-34,898019

SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Sanharó	Rua Benjamim Caraciolo, 135	Centro	Sanharó	LAP 1	-8,36032	-36,564052
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Mirandiba	Rua Francisco Carvalho Barros - 3	Centro	Mirandiba	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	Hospital Dom Helder Câmara	Rodovia Br 101 Sul - Km 28	Centro - Cabo	Cabo de Santo Agostinho	LAP 2	-8,3289	-35,106843
SECRETARIA ESTADUAL DE SAÚDE	2ª Geres - Limoeiro	Rua Santa Terezinha, S/N	Centro	Limoeiro	LAP 2	-7,888745	-35,45354
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Santa Cruz	Rua Manuel Siqueira Campos, 13	Centro	Santa Cruz	LAP 1	-8,04756	-34,876961
SECRETARIA ESTADUAL DE SAÚDE	4ª Geres - Caruaru	Rua Estilague Leal, S/N	Salgado	Caruaru	LAP 2	-8,269462	-35,958445
SECRETARIA ESTADUAL DE SAÚDE	Secretaria de Saúde - Sede	Rua Dona Maria Augusta Nogueira, 519	San Martin	Recife	LAP 2	-8,065053	-34,922306
SECRETARIA ESTADUAL DE SAÚDE	Hospital e Policlínica de Prazeres - Jaboatão	Rua Recife, S/N	Prazeres	Jaboatão dos Guararapes	LAP 2	-8,167179	-34,924823
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Sairé	Rua Vereador Amaro Henrique de Freitas, S/N	Centro	Sairé	LAP 1	-8,326243	-35,708639
SECRETARIA ESTADUAL DE SAÚDE	7ª Geres - Salgueiro	Br 232 Km 520, S/N	Cohab	Salgueiro	LAP 2	-8,067458	-39,137695
SECRETARIA ESTADUAL DE SAÚDE	Maternidade Padre Geraldo Leite Bastos	Rodovia Br 101 Sul Km 23, S/N	Ponte Dos Carvalhos	Cabo de Santo Agostinho	LAP 2	-8,258138	-35,020554
SECRETARIA ESTADUAL DE SAÚDE	UPAES - ARCOVERDE	Endereço - Av.Conselheiro João Alfredo, 491	Santa Luzia	Arcoverde	LAP 2	-8,418796	-37,038403
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Santa Filomena	Rua Germino Pereira da Cruz, S/N	Centro	Santa Filomena	LAP 1	-8,159801	-40,614352
SECRETARIA ESTADUAL DE SAÚDE	Hospital Metropolitano Miguel Arraes	Rodovia Br-101 Norte, S/N		Paulista	LAP 2	-7,936198	-34,894078
SECRETARIA ESTADUAL DE SAÚDE	Saúde - Programa Nacional de Imunização - Pni	Av. Norte, 6485	Casa Amarela	Recife	LAP 2	-8,02118	-34,923871
SECRETARIA ESTADUAL DE SAÚDE	5ª Geres - Garanhuns	Rua Joaquim Távora, 240	Heliópolis	Garanhuns	LAP 2	-8,885571	-36,487106
SECRETARIA ESTADUAL DE SAÚDE	10ª Geres - Afogados da Ingazeira	Av. Júlio Câmara, 625	Centro	Afogados da Ingazeira	LAP 1	-7,752426	-37,635959
SECRETARIA ESTADUAL DE SAÚDE	Hospital João Murilo - Vitória	Br - 232 - Km 49, S/N	Centro	Vitória de Santo Antão	LAP 1	-8,109279	-35,105653
SECRETARIA ESTADUAL DE SAÚDE	Hospital Padre Antônio Miguel - Mirueira	Estrada da Mirueira, S/N		Paulista	LAP 2	-7,971448	-34,90468
SECRETARIA ESTADUAL DE SAÚDE	UNIDADE PERNAMBUCANA DE ATENÇÃO ESPECIALIZADA - UPAES - PETROLINA	Av. ONORATO VIANA, S/N	Palhinhas	Petrolina	LAP 2	-9,389781	-40,521696
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Solidão	Rua Luis Carolino Ciqueira, S/N	Centro	Solidão	LAP 1	-7,601436	-37,64849

SECRETARIA ESTADUAL DE SAÚDE	Labend - Laboratório da Mulher	Av. Conde Da Boa Vista, 1570	Boa Vista	Recife	LAP 2	-8,05572	-34,894528
SECRETARIA ESTADUAL DE SAÚDE	Unidade Pernambucana de Atenção Especializada - UPAES - Belo Jardim	BR 232, KM 185, S/N	São Pedro	Belo Jardim	LAP 1	-8,343616	-36,423824
SECRETARIA ESTADUAL DE SAÚDE	Hospital Ulisses Pernambucano	Av. Rosa E Silva, Sn	Tamarineira	Recife	LAP 2	-8,035619	-34,902192
SECRETARIA ESTADUAL DE SAÚDE	UPAES - UNIDADE DE PRONTO ATENDIMENTO DE LIMOEIRO	Rodovia PE-90, S/N	Centro	Limoeiro	LAP 2	-7,877229	-35,445088
SECRETARIA ESTADUAL DE SAÚDE	Hospital Emilia Câmara	Rua São Paulo, S/N	Padre Pedro Pereira	Afogados da Ingazeira	LAP 2	-7,737538	-37,650741
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Caetés	Rua Melchiades Borrego, 26	Centro	Caetés	LAP 1	-8,770776	-36,624075

SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Moreilandia	Rua Coronel Romão Sampaio, S/N	Centro	Moreilândia	LAP 1	-7,620659	-39,555064
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Floresta	Rua Alcina Torres de Araujo, S/N	Centro	Floresta	LAP 1	-8,59794762	-38,57053504
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Tacaimbó	Av. João Clemente, 111	Centro	Tacaimbó	LAP 1	-8,315014	-36,290753
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento Tipo 3 - Cabo	Rua 27 - Cohab	Centro	Cabo de Santo Agostinho	LAP 2	-8,296746	-35,027268
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Bonito	Rua Misael Galindo, S/N	Centro	Bonito	LAP 1	-8,472512	-35,732225
SECRETARIA ESTADUAL DE SAÚDE	SECRETARIA DE SAUDE - PRAÇA OSWALDO CRUZ	Praça OSWALDO CRUZ, S/N	Joana bezerra	Recife	LAP 2	-8,055234	-34,891508
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Lagoa Grande	Rua dos estudantes, S/N	Centro	Lagoa Grande	LAP 1	-8,997437	-40,27133
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Carnaubeira da Penha	Rua Manoel Freire da Silva, 125	Centro	Carnaubeira da Penha	LAP 1	-8,321607	-38,743563
SECRETARIA ESTADUAL DE SAÚDE	UPA E - ABREU E LIMA	BR 101 NORTE	MATINHA	Abreu e Lima	LAP 2	-7,88852	-34,904348
SECRETARIA ESTADUAL DE SAÚDE	UPA - Tipo III - Brejo de Beberibe	Av. Otacilio de Azevedo, S/N	Brejo de Beberibe	Recife	LAP 2	-8,00223	-34,919724
SECRETARIA ESTADUAL DE SAÚDE	Hospital Correia Picanço	Rua Padre Roma, 149	Tamarineira	Recife	LAP 1	-8,033789	-34,904635
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Paranatama	Rua Tancredo Neves - S/N	Centro	Paranatama	LAP 1	-8,919474	-36,65655
SECRETARIA ESTADUAL DE SAÚDE	HOSPITAL BARÃO DE LUCENA - LINK DE BACKUP	Av. Caxangá, 3860	Iputinga	Recife	LAP 1	-8,039955	-34,939661
SECRETARIA ESTADUAL DE SAÚDE	HOSPITAL BARÃO DE LUCENA - LINK DE BACKUP	Av. Caxangá, 3860	Iputinga	Recife	LAP 2		
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Casinhas	Rua Coronel Periandro, S/N	Centro	Casinhas	LAP 1	-7,744447	-35,724392
SECRETARIA ESTADUAL DE SAÚDE	VIII Geres Anexo Endemias	Rua Projetada Parque Josefa Coelho, S/N	Centro	Petrolina	LAP 2	-9,388648	-40,498555
SECRETARIA ESTADUAL DE SAÚDE	Hospital Geral de Areias	Av. Recife, 801	Areias	Recife	LAP 2	-8,086127	-34,931636
SECRETARIA ESTADUAL DE SAÚDE	Hospital Ermírio Coutinho - Nazaré da Mata	Travessa Pancário Leopoldino Vieira De Melo, 1	Centro	Nazaré da Mata	LAP 2	-7,744136	-35,228774
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional José Fernandes Salsa - Limoeiro	Rua Santa Terezinha, S/N	Centro	Limoeiro	LAP 2	-7,869967	-35,440072
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional Rui de Barros Correia - Arcoverde	Av. Agamenon Magalhães, S/N	Centro	Arcoverde	LAP 1	-8,422865	-37,055045
SECRETARIA ESTADUAL DE SAÚDE	Setor de Epdemologia e Vigilância Sanitária - Salgueiro	Rua José Alves De Lira, S/N	Nossa Sra. Aparecida	Salgueiro	LAP 2	-8,07519033	-39,13046239
SECRETARIA ESTADUAL DE SAÚDE	Central de Regulação de Leitos	Estrada do Bongí	Bongi	Recife	LAP 2	-8,065895	-34,914413

SECRETARIA ESTADUAL DE SAÚDE	Central de Regulação de Leitos	Estrada do Bongi	Bongi	Recife	LAP 2	-8,065895	-34,914413
SECRETARIA ESTADUAL DE SAÚDE	Hospital da Restauração - Informática - Backup	Av. Prof. Agamenon Magalhães, S/N		Recife	LAP 1	-8,054264	-34,898019
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Ouricuri	Av. Fernando Bezerra, 239	Centro	Ouricuri	LAP 1	-7,89319695	-40,9025852
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Aliança	Rua Domingos Braga, 196	Centro	Aliança	LAP 1	-7,601369	-35,230148
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Bom Conselho	Av. 15 de Novembro, 174	Centro	Bom Conselho	LAP 1	-9,166769	-36,679776
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Terezinha	Rua MARECHAL RONDON, S/N	Centro	Terezinha	LAP 1	-7,377024	-37,48038

SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Vertentes	Rua PEDRO FERREIRA, S/N	Goiabeira I e II	Vertentes	LAP 1	-8,04756	-34,876961
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - São Caetano	Rua Olímpico Vieira Ramos, 1008	Centro	São Caetano	LAP 1		
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento Tipo - III Olinda	Av. Br 101 - PE-15	Jardim Fragoso	Olinda	LAP 2	-7,979501	-34,859544
SECRETARIA ESTADUAL DE SAÚDE	Hospital Agamenon Magalhães	Estrada Do Arraial, 2723	Casa Amarela	Recife	LAP 2	-8,030216	-34,906933
SECRETARIA ESTADUAL DE SAÚDE	Saúdelog - Logística de Saúde	Rod. Empresário João Santos Filho, 732	Muribeca	Jaboatão dos Guararapes	LAP 1	-8,157315	-34,96996
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Trindade	Rua Presidente Dutra, 446	Centro	Trindade	LAP 1	-7,762474	-40,267408
SECRETARIA ESTADUAL DE SAÚDE	Projeto Mae Coruja - Amaraji	Rua Francisco Teixeira, 169	Centro	Amaraji	LAP 1	-8,37882041	-35,4504747
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Jupi	Rua Jessina Pereira, 39	Centro	Jupi	LAP 1	-8,710455	-36,41719
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Ibirajuba	Av. Tenente Xavier de Araujo, S/N	Centro	Ibirajuba	LAP 1	-8,57888	-36,177887
SECRETARIA ESTADUAL DE SAÚDE	Hospital Barão de Lucena - Informática	Av. Caxangá, Número, 3860	Iputinga	Recife	LAP 2	-8,039955	-34,939661
SECRETARIA ESTADUAL DE SAÚDE	Hospital Regional Dom Moura - Garanhuns	Av. Simoa Gomes, 417	Heliópolis	Garanhuns	LAP 2	-8,890876	-36,496461
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - São Vicente Férrer	Rua 24 DE OUTUBRO, 22	Centro	São Vicente Férrer	LAP 1	-7,58926029	-35,49096999
SECRETARIA ESTADUAL DE SAÚDE	UPA - UNIDADE DE PRONTO ATENDIMENTO DE AFOGADOS DA INGAZEIRA	Rua Antonio Alves dos Santos, S/N	Centro	Afogados da Ingazeira	LAP 2	-7,754634	-37,637293
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Panelas	Praça Coronel João Rufino, 6	Centro	Panelas	LAP 1	-8,663912	-36,005071
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento - Tipo III - Imbiribeira	Av. Mal. Mascarenhas de Morais, S/N	Imbiribeira	Recife	LAP 2	-8,1209	-34,913864
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Parnamirim	Rua Coronel Jambo, 35	Centro	Parnamirim	LAP 1	-8,091281	-39,577816
SECRETARIA ESTADUAL DE SAÚDE	UPA - Unidade de Pronto Atendimento -Tipo Iii- Torrões	Av. Abdias de Carvalho, S/N	Torrões	Recife	LAP 2	-8,063169	-34,934113
SECRETARIA ESTADUAL DE SAÚDE	Programa Mãe Coruja - Jurema	Rua Julio Cordeiro Santos, 126	Centro	Jurema	LAP 1	-8,721509	-36,135363
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Arcoverde	Rua João Isidoro Da Silva, 20	Sucupira	Arcoverde	LAP 1	-8,42620708	-37,5504601
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Sede	Rua Da Aurora, 885	Boa Vista	Recife	LAP 1	-8,060758	-34,880801
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Bezerros	Av. Otavio Pessoa S Maior, S/N	Centro	Bezerros	LAP 1	-8,233137	-35,744304
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Palmares	Rod Br 101 Sul, Km 117, S/N	Newton carneiro	Palmares	LAP 1	-8,68263047	-35,58473971

TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Garanhuns	Av. Amaury De Medeiros, 195	Heliópolis	Garanhuns	LAP 1	-8,885038	-36,487911
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Surubim	Rua Antônio Medeiros Sobrinho, S/N	Centro	Surubim	LAP 1	-7,841357	-35,756738
TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO	TCE - Petrolina	Avenida Fernando Goes - 875	Centro	Petrolina	LAP 1	-9,395946	-40,496004

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TRACUNHAÉM - FÓRUM JUIZ VALDIR BARBOSA	Loteamento Santa Cruz, Br 408, S/N	Santa Cruz	Tracunhaém	LAP 1	-7,805176	-35,239848
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - CASA DA JUSTIÇA (BONGI)	Rua Acajutiba, 43	Bongi	Recife	LAP 1	-8,063304	-34,922212
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PAULISTA - FÓRUM DOUTOR IRAJÁ D'ALMEIDA LINS	Av. Senador Salgado Filho, S/N	Centro	Paulista	LAP 1	-7,93849	-34,881128
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - GRAVATÁ - FÓRUM DESEMBARGADOR PEDRO RIBEIRO MALTA	Rua Quintino Bocaiuva, S/N	Centro	Gravatá	LAP 1	-8,199089	-35,567239
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PANELAS - FÓRUM DE PANELAS	Av. Dom Moura, S/N	Centro	Panelas	LAP 1	-8,6692303	-36,1478427
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JABOATÃO DOS GUARARAPES - FÓRUM DESEMBARGADOR HENRIQUE CAPITULINO	Rodovia Br 101	Prazeres	Jaboatão dos Guararapes	LAP 1	-8,15189985	-34,94172477
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - LAGOA GRANDE - FÓRUM DESEMBARGADOR BENILDES DE SOUZA RIBEIRO	Rua Olimpio Avelim, S/N	Estátua	Lagoa Grande	LAP 1	-8,991767	-40,272598
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VENTUROSA - FÓRUM FRANCISCO PEREIRA DE CARVALHO BARROS	Rua Tenente Wanderleii, S/N	centro	Venturosa	LAP 1	-8,57804098	-36,87367369
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TUPARETAMA - FÓRUM JOSÉ PERAZZO LEITE	Rua Tereza Menezes, S/N	Centro	Tuparetama	LAP 1	-7,599055	-37,308
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PESQUEIRA - FÓRUM SÉRGIO HIGINO DIAS	Rua Largo Bernado Vieira De Mela, S/N	Centro	Pesqueira	LAP 1	-8,360148	-36,702134
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TRINDADE - FÓRUM DE TRINDADE	Rua Vinte E Cinco De Abril, 226	Centro	Trindade	LAP 1	-7,760165	-40,267697
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO BENTO DO UNA - FÓRUM DOUTOR GERALDO DE SOUZA VALENÇA	Av. Manoel Candido, S/N	Centro	São Bento do Una	LAP 1		
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PALMARES - FÓRUM DE PALMARES PROFESSOR ANÍBAL BRUNO	ROD BR 101 SUL KM 188, S/N	Quilombo II	Palmares	LAP 1	-8,662212	-35,567327
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CARUARU - VARA VIOLÊNCIA CONTRA MULHER	Av. Portugal, S/N	Universitário	Caruaru	LAP 1	-8,268117	-35,966944
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - INAJÁ - FÓRUM DE INAJÁ	Av. Cristo Rei, S/N	Centro	Inajá	LAP 1	-8,90330647	-37,8289723
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JOÃO ALFREDO - FÓRUM DESEMBARGADOR CUNHA BARRETO	Av. Presidente Kenedy, S/N	Boa Vista	João Alfredo	LAP 1	-7,86152	-35,589827

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SALOÁ - FÓRUM DOUTOR JOAQUIM CIRILLO DE ARAÚJO PEREIRA	Rua 21 de Abril, S/N	Ipsep	Saloá	LAP 1	-8,97579683	-36,6899499
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JABOATÃO DOS GUARARAPES - VARA DA VIOLÊNCIA DOMÉSTICA E FAMILIAR CONTRA A MULHER DE JABOATÃO	Rua JANGADEIRO, 127	Candeias	Jaboatão dos Guararapes	LAP 1	-8,19358	-34,919671
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO JOÃO - FÓRUM DOUTOR LITO D'AZEVEDO E SILVA FILHO	Av. José Clemente da Rocha, S/N	Centro	São João	LAP 1	-8,871303	-36,368768
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PARNAMIRIM - FÓRUM JUIZ JOSÉ RAMOS ANGELIM	Rua Corenel Janbo, 39	Centro	Parnamirim	LAP 1	-8,088908	-39,577183

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IPUBI - FÓRUM HELI LEITÃO DE MELO	Praça Siqueira Campos, S/N	Centro	Ipupi	LAP 1	-7,650011	-40,147665
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TACAIBÓ - FÓRUM JUIZ JOSÉ FERREIRA LIMA	Praça Francelino Araújo, 80 A	Centro	Tacaibó	LAP 1	-8,315632	-36,289718
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO JOSÉ DA COROA GRANDE - FÓRUM ESCRIVÃO ANTÔNIO FÉLIX DA SILVA	Rua Inaldo Moraes Acioli, 2020	Centro	São José da Coroa Grande	LAP 1	-8,89640649	-35,14534797
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - FÓRUM DESEMBARGADOR BENILDES DE SOUZA RIBEIRO	Av Marechal Mascarenhas de Moraes. Nº1919	Imbiribeira	Recife	LAP 1	-8,09770105	-34,90490886
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ARARIPINA - FÓRUM DOUTOR FRANCISCO MUNIZ ARRAES	Rua Ramos Larcada, S/N	Centro	Araripina	LAP 1	-7,57455242	-40,49530743
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAQUITINGA - FÓRUM JUIZ NICANOR MUNIZ DA SILVA BORGES	Rua Agrovila, S/N	Centro	Itaquitinga	LAP 1	-7,660056	-35,103633
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - PORTO DIGITAL	Cais do Apolo, 222	Recife Antigo	Recife	LAP 1	-8,058836	-34,87249
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SANTA CRUZ DO CAPIBARIBE - FÓRUM DOUTOR NAÉRCIO CIRENO GONÇALVES	ROD. PE-160, S/N	Lídia queiroz	Santa Cruz do Capibaribe	LAP 1	-7,949494	-36,223357
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PEDRA - FÓRUM ARTHUR TENÓRIO LIMA	Rua Joao Bezerra Galindo, S/N	Centro	Pedra	LAP 1	-8,5000591	-36,94235763
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - ESCOLA JUDICIAL	Rua DESEMBARGADOR GUERRA BARRETO, S/N	Joana Bezerra	Recife	LAP 1	-8,0708	-34,891798
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - FORUM THOMAZ DE AQUINO CYRILLO WANDERLEY	Av. Martins De Barros, 593	Santo Antônio	Recife	LAP 1	-8,065489	-34,876431
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JUPI - FÓRUM DESEMBARGADOR RODOLFO AURELIANO	Rua Antonio Pereira Braga, S/N	Centro	Jupi	LAP 1	-8,708968	-36,417243
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BOM JARDIM - FÓRUM DOUTOR OSWALDO DE LIMA	R Tabelaão Manoel Arnóbio Souto Maior, S/N	Centro	Bom Jardim	LAP 1	-7,79699314	-35,58840796
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TAQUARITINGA DO NORTE - FÓRUM DEFENSORA PÚBLICA MARLIETE ARAGÃO DE FARIAS	RODOVIA PE-130, S/N	Centro	Taquaritinga do Norte	LAP 1	-7,896956	-36,059528
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - MORENO - FÓRUM DESEMBARGADOR AGAMENON DUARTE LIMA	Rua CLETO CAMPELO, 3189	Centro	Moreno	LAP 1	-8,117918	-35,096639

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO CAETANO - FÓRUM DESEMBARGADOR ALCEBIADES MEDEIROS DE SIQUEIRA CAMPOS	Av. Pedro Almeida Do Nascimento, S/N	Centro	São Caetano	LAP 1	-8,326476	-36,142318
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BODOCÓ - FÓRUM DOUTOR JOSÉ FERNANDES MENDONÇA DE SOUSA	Rua Teodosio Leandro Horas, S/N	Centro	Bodocó	LAP 1	-7,780141	-39,935644
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - AGRESTINA - FÓRUM DEPUTADO ELIAS LIBÂNIO RIBEIRO	Rodovia BR 104, S/N	Cordeiro	Agrestina	LAP 1	-	-
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RIO FORMOSO - FÓRUM GOVERNADOR AGAMENON MAGALHÃES	Rua São José, 147	Centro	Rio Formoso	LAP 1	-8,66008	-35,152614
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - LIMOEIRO - FÓRUM DESEMBARGADOR JOÃO BATISTA GUERRA BARRETO	Rodovia PE 090 - KM 22, s/n	Centro	Limoeiro	LAP 1	-7,852152	-35,454985

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - FÓRUM DESEMBARGADOR RODOLFO AURELIANO	Rua Desembargador Guerra, S/N	Joana Bezerra	Recife	LAP 1	-8,070691	-34,896802
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CABO DE SANTO AGOSTINHO - FÓRUM DR. HUMBERTO DA COSTA SOARES	Av. Pres Getulio Vargas, 482	Centro	Cabo de Santo Agostinho	LAP 1	-8,285228	-35,036558
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ALTINHO - FÓRUM DOUTOR JOSÉ FERREIRA DE LIMA	Av. João Cassiano, 170	Centro	Altinho	LAP 1	-8,48519	-36,05915
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VERTENTES - FÓRUM DESEMBARGADOR JOÃO AURELIANO CORREIA DE ARAÚJO	Praça Agamenon Magalhaes, 300	Centro	Vertentes	LAP 1	-7,90300939	-35,98666734
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - DIRETORIA DE SAUDE	Abdias de Carvalho, S/N	Prado	Recife	LAP 1	-8,062966	-34,903923
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BARREIROS - FÓRUM DESEMBARGADOR ORLANDO AGUIAR	Rua Dom Luis, 346	Centro	Barreiros	LAP 1	-8,812755	-35,200189
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAPOEIRAS - FÓRUM ADALBERTO BEZERRA DE MELO	Rua Aprigio Inacio Cordeiro, S/N	Santa tereza	Capoeiras	LAP 1	-8,73625	-36,626367
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ALIANÇA - FÓRUM JUIZ JOSÉ ALBINO LATACHE PIMENTEL	Rua 2, Nº79, Coab	Centro	Aliança	LAP 1	-7,59484962	-35,23421919
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - AFOGADOS DA INGAZEIRA - FÓRUM LAURINDO LEANDRO LEMOS	Av. Padre Luis de Goes, S/N	Manoela Valadares	Afogados da Ingazeira	LAP 1	-7,754102	-37,632212
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - AEROPORTO DOS GUARARAPES	Av. MASCARENHAS DE MORAES, S/N- AEROPORTO , INTERNACIONAL DOS GUARARAPES - PISO	Imbiribeira	Recife	LAP 1	-8,125932	-34,924015
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAMARAGIBE - DATA CENTER	Rua Tenente Arnaldo	Timbi	Camaragibe	LAP 1	-8,025409	-34,988856
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VITÓRIA DE SANTO ANTÃO - VARA DA INFÂNCIA E DA JUVENTUDE DE VITÓRIA DE SANTO ANTÃO	Rua Versoça, 350	Centro	Vitória de Santo Antão	LAP 1	-8,116044	-35,294379
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - GLÓRIA DO GOITÁ - FÓRUM DOUTOR MANOEL PESSOA DE LUNA FILHO	Av. Rui Barbosa, 896	Centro	Glória do Goitá	LAP 1	-8,002896	-35,300152
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PETROLINA - VARA DA INFÂNCIA E JUVENTUDE DA COMARCA DE PETROLINA	Av. Fernando de Menezes Goes, 696	Centro	Petrolina	LAP 1	-9,39502	-40,502171
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ÁGUAS BELAS - FÓRUM JOSÉ MARIA FLORENTINO DE LIMA	Praça Padre Nelson, S/N	Comonaty	Águas Belas	LAP 1	-9,107397	-37,125972
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAMARAGIBE - FÓRUM DESEMBARGADOR AGENOR FERREIRA DE LIMA	Rua Belmiro Gouveia, 144	Centro	Camaragibe	LAP 1	-8,024061	-35,000516

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SANTA MARIA DA BOA VISTA - FÓRUM DA COMARCA DE SANTA MARIA DA BOA VISTA	Rua Projetada 8, S/N	Centro	Santa Maria da Boa Vista	LAP 1	-8,78817842	39,87646481
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAÍBA - FÓRUM DESEMBARGADOR JEOVÁ DA ROCHA WANDERLEY	Rua Constantino lavrador, S/N	Centro	Itaíba	LAP 1	-8,949724	-37,423188
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - DIRIEST - GERÊNCIA DE TRANSPORTES	RUA FRANCISCO SILVEIRA, s/n	Cabanga	Recife	LAP 1	-8,082371	-34,905064

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - CENTRO INTEGRADO DA CRIANÇA E DO ADOLESCENTE	Av. Dr. João Fernandes Vieira, 405	Boa Vista	Recife	LAP 1	-8,052986	-34,892395
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PASSIRA - FÓRUM FRANCISCO LIMA BEZERRA	Praça Severino Ferreira, 59	Centro	Passira	LAP 1	-7,979532	-35,58052
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAPISSUMA - FÓRUM JUIZ ANTÔNIO DE PÁDUA COUTO CARACIOLO	Rua Manuel Lourenço, 201	Centro	Itapissuma	LAP 1	-7,776181	-34,891145
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - FÓRUM PAULA BAPTISTA	Rua Do Imperador Dom Pedro, 207	Santo Antônio	Recife	LAP 1	-8,062249	-34,876945
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CUSTÓDIA - FÓRUM DOUTOR JOSUÉ CUSTÓDIO DE ALBUQUERQUE	Av. Inocência Lima, S/N	Nossa Senhora de Lourdes	Custódia	LAP 1	-8,088165	-37,647355
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - OROCO - FÓRUM DE OROCO	Rua Quirino Do Nascimento, 667	Centro	Orocó	LAP 1	-8,616651	-39,602233
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - EXU - FÓRUM JUIZ VALDIR BARBOSA	Av. Edmundo Dantas, S/N	Centro	Exu	LAP 1	-7,51304409	-39,72112576
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CARPINA - FÓRUM DOUTOR JOSÉ GONÇALVES GUERRA	Av. Conselheiro João Alfredo, 820	São José	Carpina	LAP 1	-7,845739	-35,249681
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - PALÁCIO DA JUSTIÇA	Praça Da República, S/N	Santo Antônio	Recife	LAP 1	-8,061642	-34,877673
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ÁGUA PRETA - FÓRUM EURICO CHAVES	Praça Dos Três Poderes, 3156	Centro	Água Preta	LAP 1	-8,703245	-35,527942
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CABROBÓ - FÓRUM DOUTOR ANTÔNIO DE NOVAES MELLO E AVELLINS	Rua Vereador João Gonçalves Dos Santos, S/N	Centro	Cabrobó	LAP 1	-8,511591	-39,309541
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - QUIPAPÁ - FÓRUM DESEMBARGADOR JOSÉ NEVES	Rua Edson Lira de Paula, S/N	Vila Canarinho	Quipapá	LAP 1	-8,824603	-36,009248
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAETÉS - FÓRUM DE CAETÉS	Fazenda Pau Ferro, S/N		Caetés	LAP 1	-8,772483	-36,619715
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PETROLINA - JUIZADO CÍVEL DA COMARCA DE PETROLINA	Rua JONAS BRANDÃO, 1465	Centro	Petrolina	LAP 1	-9,394472	-40,482411
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - LAJEDO - FÓRUM JOSÉ FIRMINO BURGOS	Rua Mucio Monteiro, S/N	Centro	Lajedo	LAP 1		
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ABREU E LIMA - FÓRUM SERVENTUÁRIO ANTÔNIO CAMAROTTI	Av. Brasil, 635	Timbó	Abreu e Lima	LAP 1	-7,909286	-34,90199

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - OROBÓ - FÓRUM DOUTOR OTÍLIO GUEDES DE FREITAS MONTENEGRO	Rua João Pessoa, S/N	Centro	Orobó	LAP 1	-7,749417	-35,604358
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAMARACÁ - FÓRUM SANDOVAL MALTA DE ALMEIDA	Rua Brumado, Quadra N, Loteamento Recreio II, S/N	Jaguaribe	Ilha de Itamaracá	LAP 1	-7,749637	-34,825081
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - LAGOA DOS GATOS - FÓRUM FREI CANECA	Rua Dom Luiz, S/N	Centro	Lagoa dos Gatos	LAP 1	-8,65844	-35,905436
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TABIRA - FÓRUM JOSÉ VERÍSSIMO MONTEIRO	RODOVIA PE, 320	Centro	Tabira	LAP 1	-7,591174	-37,539827

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - FLORES - FÓRUM DESEMBARGADOR ADAUTO MAIA	Rua Pedro Santos Estima, 87	Centro	Flores	LAP 1	-7,864001	-37,975542
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CARNAÍBA - FÓRUM ANTÔNIO DE SOUZA DANTAS	Rua José Fernandes de Andrade, S/N	José Dantas	Carnaíba	LAP 1	-7,8063919	-37,79942671
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BELO JARDIM - FÓRUM DESEMBARGADOR JOÃO PAES	Praça Joao Torres Galindo, S/N	Centro	Belo Jardim	LAP 1	-8,3380019	-36,4242423
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - CENTRO INTEGRADO DO CIDADÃO	Rua Da Glória, 301	Boa Vista	Recife	LAP 1	-8,064277	-34,887223
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BOM CONSELHO - FÓRUM DOUTOR ORLANDO CAVALCANTE DE ALBUQUERQUE	Praça Dom Pedro II, 34	Centro	Bom Conselho	LAP 1	-9,16791	-36,678588
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - GOIANA - FÓRUM DESEMBARGADOR NUNES MACHADO	Estrada da Boa Vista, S/N	Jardim Novo Mundo	Goiana	LAP 1	-7,555594	-35,011913
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PETROLINA - FÓRUM DOUTOR MANOEL FRANCISCO DE SOUZA FILHO	Praça Santos Dummont, S/N	Centro	Petrolina	LAP 1	-9,394586	-40,497703
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - EDIFÍCIO SANTO ANTÔNIO	Av. Dantas Barreto, 191	São Jose	Recife	LAP 1	-8,061942	-34,877978
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JUREMA - FÓRUM CLÁUDIO AMÉRICO DE MIRANDA	Praça Da Bandeira, S/N	Centro	Jurema	LAP 1	-8,719215	-36,136464
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VITÓRIA DE SANTO ANTÃO - JUIZADO DE VITÓRIA DE SANTO ANTÃO	Rua Dr. José Rufino Bezerra, 223	Cajá	Vitória de Santo Antão	LAP 1	-8,112919	-35,291164
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IGARASSU - FÓRUM DOM PEDRO II	Av. 27 De Setembro, S/N	Centro	Igarassu	LAP 1	-7,839051	-34,906468
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CACHOEIRINHA - FÓRUM FRANCISCO LEITE MARTINS	Rua Diva Valença de Melo, 118	Centro	Cachoeirinha	LAP 1	-8,488221	-36,240308
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - FEIRA NOVA - FÓRUM JESUÍNO ALVES FERREIRA	Rua Sebastião Da Rocha, S/N	Centro	Feira Nova	LAP 1	-7,950544	-35,38542
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SAIRÉ - FÓRUM DOUTOR ALUIZIO DE MELO XAVIER	Rua Sete de Setembro, 1		Sairé	LAP 1	-8,18498616	-36,706766
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BONITO - FÓRUM DOUTOR PLÁCIDO DE SOUZA	Loteamento Jardim América, S/N	Boa Vista	Bonito	LAP 1	-8,47861194	-35,75241466

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CABO DE SANTO AGOSTINHO - VARA DA VIOLÊNCIA DOMÉSTICA CONTRA A MULHER DO CABO DE SANTO AGOSTI	Rua DOUTOR MANOEL CLEMENTINO CAVALCANTE, 96	Centro	Cabo de Santo Agostinho	LAP 1	-8,282931	-35,031771
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO LOURENÇO DA MATA - FÓRUM DESEMBARGADOR PAULO ANDRÉ DIAS DA SILVA	Rua Tito Pereira, 267	Centro	São Lourenço da Mata	LAP 1	-7,992663	-35,042968
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - CASA DA JUSTIÇA (COQUE)	Rua Cabo Eutropico, 178	Joana Bezerra	Recife	LAP 1	-8,075153	-34,900042
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CUMARU - FÓRUM MANOEL GONÇALVES DE LIMA	Rua Eumenia de Oliveira Gonçalves, S/N	Centro	Cumaru	LAP 1	-8,009469	-35,700948
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - AMARAJO - FÓRUM DESEMBARGADOR JOSÉ SIRONE DE VASCONCELOS	Rua Adnaldo Correia, S/N	Centro	Amaraji	LAP 1	-8,377827	-35,450986

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CARUARU - FÓRUM JUIZ DEMÓSTENES BATISTA VERAS	Av. Jose Florencio Filho, S/N	Maurício de nassau	Caruaru	LAP 1	-8,258728	-35,967626
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAMARAGIBE - JECÍVEL DA COMARCA DE CAMARAGIBE	Av. Dr. Belmiro Correia, 1533B	Centro	Camaragibe	LAP 1	-8,02038275	-34,98052818
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO LOURENÇO DA MATA - TJPE - CASA CIVIL DE SÃO LOURENÇO DA MATA	Rua OLIVIO COSTA, S/N	Centro	São Lourenço da Mata	LAP 1	-7,996492	-35,036639
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CORRENTES - FÓRUM DOUTOR EURICO CANTALICE DE MELO	Praça Agamenon Magalhaes, S/N	Casa amarela	Correntes	LAP 1	-9,129516	-36,328053
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VICÊNCIA - FÓRUM DOUTOR CLÁUDIO GUEIROS LEITE	Rua Delclides de Andrade Lima, 5	Centro	Vicência	LAP 1	-7,658069	-35,319542
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SALGUEIRO - FÓRUM CORNÉLIO DE BARROS MUNIZ E SÁ	Rua Manoel Francisco Santiago, 300	Augusto alencar sampaio	Salgueiro	LAP 1	-8,07112142	-39,13808886
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TRIUNFO - FÓRUM DOUTOR CAETÊS DE MEDEIROS	RUA JOSÉ LOPES TOMAS, s/n	Encruzilhada	Triunfo	LAP 1	-7,840314	-38,094923
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - OURICURI - FÓRUM JOSUÉ CUSTÓDIO DE ALBUQUERQUE	Av. Antonio Pedro, S/N	Centro	Ouricuri	LAP 1	-7,884861	-40,08474
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - LAGOA DE ITAENGA - FÓRUM DA COMARCA DE LAGOA DE ITAENGA	Rua Maria Aurora, 12	Centro	Lagoa do Itaenga	LAP 1	-7,92724429	-35,29586853
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SERRITA - FÓRUM DESEMBARGADOR RODOLFO AURELIANO	Rua Rogerio Camelo Na Vila Do Ceac, S/N	Centro	Serrita	LAP 1	-7,94306	-39,297717
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ARCOVERDE - FÓRUM CLÓVIS DE CARVALHO PADILHA	Rua Antônio de Moura Cavalcante, S/N	São Miguel	Arcoverde	LAP 1	-8,423262	-37,066333
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO JOSÉ DO EGITO - FÓRUM DESEMBARGADOR FAUSTO CAMPOS	Av. 25 de Agosto, S/N	Bela Vista	São José do Egito	LAP 1	-7,468483	-37,274647
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IATI - FÓRUM DOUTOR MAURÍCIO LINS GALVÃO	Rua Francisco Pereira da Costa, S/N	Centro	Iati	LAP 1	-8,04756	-34,876961
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - NAZARÉ DA MATA - FÓRUM MINISTRO DJALMA TAVARES DA CUNHA MELO	Rua Bom Jesus, S/N	Centro	Nazaré da Mata	LAP 1	-7,742212	-35,227375
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CORTÊS - FÓRUM JUIZ ANÍBAL BALTAR SOUTO MAIOR	Rodovia Pe 85, S/N		Cortês	LAP 1	-8,473053	-35,548195
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VITÓRIA DE SANTO ANTÃO - FÓRUM SEVERINO JOAQUIM KRAUSE GONÇALVES	Rua Joaquim Nabuco, 256	Centro	Vitória de Santo Antão	LAP 1	-8,114963	-35,292417
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - ARQUIVO GERAL E GEMAN	Rua Santa Edvrigens, 390	Afogados	Recife	LAP 1	-8,06420553	-34,91252089

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CARUARU - FÓRUM UNIVERSITÁRIO DE CARUARU	Av. Portugal, S/N	Universitário	Caruaru	LAP 1	-8,25830236	-35,9668783
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - MARAIAL - FÓRUM DE MARAIAL	Av. Nova Maraial, S/N	Centro	Maraial	LAP 1	-8,77842197	-35,80914355
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - GAMELEIRA - FÓRUM DOUTOR ONOFRE DE BARROS	Av. Jose Barradas, 81	Centro	Gameleira	LAP 1	-8,585437	-35,387132

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SÃO JOAQUIM DO MONTE - FÓRUM JOSÉ ANDRADE GUEDES	Praça Alberto de Oliveira, S/N	Centro	São Joaquim do Monte	LAP 1	-8,43356642	-35,80536836
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ESCADA - FÓRUM EZEQUIEL DE BARROS	Rua Dr. Ezequiel De Barros, S/N	Jaguaribe	Escada	LAP 1	-8,369618	-35,237908
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SANTA MARIA DO CAMBUCÁ - FÓRUM JOÃO DAVID DE SOUZA	Rua David Souza, S/N	Centro	Santa Maria do Cambucá	LAP 1	-7,83029	-35,885053
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CAMOCIM DE SÃO FÉLIX - FÓRUM DOUTOR JOSÉ ARTUR DE LIMA	Rua Manoel Serafim Santos, S/N	Centro	Camocim de São Félix	LAP 1	-8,3609	-35,762205
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RIBEIRÃO - FÓRUM ABOLICIONISTA JOSÉ MARIANO	Praça Eliseu Lins de Andrade, S/N	Centro	Ribeirão	LAP 1	-8,50817357	-35,37322532
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAPETIM - FÓRUM DESEMBARGADOR ED-EK GONÇALVES LOPES	Rua Francisco Santos, 37	Centro	Itapetim	LAP 1	-7,37906923	-37,1869766
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - AFRÂNIO - FÓRUM FRANCISCO JUBELINO CAVALCANTI	Rua Francisco Rodrigues, 241	Centro	Afrânio	LAP 1	-8,516364	-41,006554
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IBIMIRIM - FÓRUM DE IBIMIRIM	Av. Emanuel Vicente, S/N	Centro	Ibimirim	LAP 1	-8,535252	-37,692686
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CANHOTINHO - FÓRUM DOUTOR ANTÔNIO LUIZ LINS DE BARROS	Rua PROJETADA Nº 02 DA QUADRA - 25, s/n	Centro	Canhotinho	LAP 1	-8,881442	-36,192364
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CONDADO - FÓRUM DESEMBARGADOR LUIS TAVARES GOUVEIA MARINHO	Av. Olegario da Fonseca, S/N	Centro	Condado	LAP 1	-7,586183	-35,099913
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ALAGOINHA - FÓRUM DOUTOR JOSÉ VITAL BEZERRA GALINDO	Av. Gonsalo Antunes Bezerra, S/N	Centro	Alagoinha	LAP 1	-8,46881069	-36,77227821
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TORITAMA - FÓRUM ERNESTO HERCULINO CORDEIRO	Av. Projetada, 1	Loteamento monte Verde	Toritama	LAP 1	-8,00937956	-36,07811915
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PAUDALHO - FÓRUM MINISTRO PETRÔNIO PORTELA	Praça Pedro Continho, Nº97, Centro	Centro	Paudalho	LAP 1	-7,896766	-35,17627
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SERRA TALHADA - FÓRUM DOUTOR CLODOALDO BEZERRA DE SOUZA E SILVA	Rua Cabo Joaquim da Mata, S/N	Tancredo neves	Serra Talhada	LAP 1	-7,9776112	-38,28112977
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - MACAPARANA - FÓRUM FRANCISCO SALUSTIANO CORREIA	Rua João Francisco Queiroz, 327	Centro	Macaparana	LAP 1	-7,552619	-35,448696
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SERTÂNIA - FÓRUM DOUTOR ULISSES LINS DE ALBUQUERQUE	Rua Padre Atanasio, S/N	Centro	Sertânia	LAP 1	-8,07517237	-37,26698691

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - JABOATÃO DOS GUARARAPES - JUIZADO ESPECIAL CRIMINAL	Rua ARÃO LINS DE ANDRADE, 82	Floriano	Jaboatão dos Guararapes	LAP 1	-8,098185	-34,996971
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - MIRANDIBA - FÓRUM ALCINDO TORRES DE CARVALHO LOPES	Rua Josefa Magalhães, S/N	Centro	Mirandiba	LAP 1	-8,117499	-38,728541
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - FLORESTA - FÓRUM DESEMBARGADOR EUCLIDES FERRAZ	Av. Odomar Ferraz, 52	Centro	Floresta	LAP 1	-8,599618	-38,571052
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - GARANHUNS - FÓRUM MINISTRO ERALDO GUEIROS LEITE	Av. Rui Barbosa, 479	Heliópolis	Garanhuns	LAP 1	-8,88452818	-36,48339719

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CATENDE - FÓRUM EDMUNDO JORDÃO DE VASCONCELOS	Praça Costa Azevedo, 120	Centro	Catende	LAP 1	-8,67017839	-35,71993918
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BUIQUE - FÓRUM DOUTOR JOÃO CARLOS RIBEIRO ROMA	Av. Jonas Camelo De Almeida, S/N	Centro	Buíque	LAP 1	-8,62139831	-37,15562852
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BEZERROS - FÓRUM ALÍPIO CAVALCANTI	Av. Francisca de Araújo Moraes - S/N- , São Sebastião	São Sebastião	Bezerros	LAP 1	-8,244225	-35,754705
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TAMANDARÉ - FÓRUM DOUTOR CLEMENCEAU DUTRA DE ALMEIDA LYRA	LOTE 1 - SÍTIO JONICO - A 100M PREFEITURA DE TAMANDARÉ	Centro	Tamandaré	LAP 1	-8,746351	-35,094028
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - TIMBAÚBA - FÓRUM IRAJÁ D' ALMEIDA LINS	R. Floriano Peixoto - 91	Barro	Timbaúba	LAP 1	-7,51173	-35,321153
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PETROLINA - JUIZADO ESPECIAL CRIMINAL DE PETROLINA	Rua SÃO FRANCISCO, 549	Atrás da Banca	Petrolina	LAP 1	-9,398732	-40,506891
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - RECIFE - MEMORIAL DA JUSTIÇA	Av. Alfredo Lisboa, S/N	Bairro do recife	Recife	LAP 1	-8,06229	-34,87065
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SIRINHAÉM - FÓRUM DESEMBARGADOR MEDEIROS CORREIA	Rua Sebastião Chaves, 215	Centro	Sirinhaém	LAP 1	-8,591227	-35,1166
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - ITAMBÉ - FÓRUM JUIZ ROBERTO GUIMARÃES	Pe 75, S/N	Centro	Itambé	LAP 1	-7,40497448	-35,12067356
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - PETROLÂNDIA - FÓRUM PROFESSOR JOSÉ DA COSTA PORTO	Av. Dos Três Poderes, 75	Centro	Petrolândia	LAP 1	-8,979704	-38,218474
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - VERDEJANTE - FÓRUM DOUTOR JONAS PEREIRA NETO	Praça Raimundo Tagino, S/N	Tagino	Verdejante	LAP 1	-7,927013	-38,969897
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SANHARÓ - FÓRUM DOUTOR JOSÉ FOERSTER	Av. Vice Prefeito Iraldemir de Freitas, S/N	Centro	Sanharó	LAP 1	-8,361511	-36,562978
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - OLINDA - FÓRUM LOURENÇO JOSÉ RIBEIRO	Av. Pam Nordestina, S/N	Vila Popular	Olinda	LAP 1	-8,012563	-34,859636
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IPOJUCA - FÓRUM THOMAZ DE AQUINO CYRILLO WANDERLEY	Av. Francisco Alves De Souza, S/N	Centro	Ipojuca	LAP 1	-8,399898	-35,058694
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CABO DE SANTO AGOSTINHO - EMPRESARIAL CABO CORPORATE CENTER	Rua CENTO E SESSENTA E TRES, 1	Garapu	Cabo de Santo Agostinho	LAP 1	-8,300604	-35,030264
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - BELÉM DE SÃO FRANCISCO - FÓRUM JOAQUIM CRISPINIANO COELHO BRANDÃO	Av. Coronel Geronimo Pires, 820	Centro	Belém de São Francisco	LAP 1	-8,75374	-38,968117
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - SURUBIM - FÓRUM BACHAREL DÍDIMO GONÇALVES GUERRA	Rua Conego Benigeno Lira, S/N	Centro	Surubim	LAP 1	-7,837838	-35,758068

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - POMBOS - FÓRUM DOUTOR RONALDO DE BARROS NOTARO	Rua I, S/N	Centro	Pombos	LAP 1	-8,14356	-35,402841
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - IGARASSU - VARA DA VIOLENCIA DOMÉSTICA E FAMILIAR CONTRA A MULHER DE IGARASSU	Av. Mário de Melo, 425	Centro	Igarassu	LAP 1	-7,826609	-34,909524
TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO	TJPE - CUPIRA - FÓRUM ANTÔNIO IZÍDIO DE ARRUDA	Rua José Luiz Silveira Barros, 146	Centro	Cupira	LAP 1	-8,611842	-35,955778
UPE - CAMPUS MATA NORTE	UPE - Campus Mata Norte	Rua Professor Amaro Maltez, 201	Centro	Nazaré da Mata	LAP 2	-7,747092	-35,222665
UPE - CAMPUS MATA SUL	UPE - Campus Mata Sul	Av. Doutor Homero de França Limeira, S/N	Centro	Palmares	LAP 1	-8,672685	-35,576296

## ANEXO D – QUANTITATIVO DE TRAFÉGO EXTRARREDE E ESPECIFICAÇÕES TÉCNICAS PARA DIMENSIONAMENTO DE SOLUÇÃO DE VOZ EM CLOUD

1. Este anexo fornece dados relacionados à quantidade de Pontos de Voz Fixo (PVFs) por município que necessitam ser portados, além de informações sobre o tráfego consumido pelos serviços 0800 Estadual e Solução de Tráfego Extrarrede ao longo do ano de 2024 de operação. Essas informações são disponibilizadas para subsidiar os LICITANTES na avaliação da capacidade de suas redes, permitindo que atendam adequadamente às especificações técnicas e aos requisitos operacionais estabelecidos no Termo de Referência e seus Adendos.

2. A infraestrutura a ser implantada pela CONTRATADA deverá ser flexível e escalável, garantindo condições para assumir eventuais crescimentos no número de PVFs ou demandas adicionais em qualquer município do Estado de Pernambuco, sem que isso implique em limitação operacional ou técnica para o cumprimento das obrigações contratuais.

3. As tabelas abaixo fornecem dados que refletem as localidades atualmente instaladas e os volumes médio de consumo de tráfego registrados na rede atual. Esses valores poderão ser substituídos, acrescidos ou diminuídos a critério da CONTRATANTE, antes ou durante a execução do contrato, sem que isso represente qualquer ônus adicional para esta.

4. A CONTRATADA será responsável pelo dimensionamento da rede e da infraestrutura necessária para os serviços de Portabilidade Numérica, Serviço 0800 Estadual e Solução de Tráfego Extrarrede, garantindo plena conformidade com os Níveis Mínimos de Serviço (NMS) e os requisitos técnicos estabelecidos neste Termo de Referência. O dimensionamento deve contemplar tanto a capacidade atual quanto eventuais expansões futuras, assegurando flexibilidade, escalabilidade e desempenho contínuo, mesmo em cenários de alta demanda.

5. A infraestrutura e os serviços propostos devem atender aos padrões normativos vigentes e regulamentações aplicáveis, com monitoramento contínuo de desempenho e qualidade. A CONTRATADA será integralmente responsável por ajustes necessários na infraestrutura proposta, sem ônus adicional à CONTRATANTE, em caso de inadequações que comprometam a operação ou os indicadores de qualidade exigidos.

6. Portabilidade numérica: Quantidade de Pontos de Voz Fixo (PVF) por município

6.1. A tabela abaixo apresenta a distribuição dos Pontos de Voz Fixo (PVFs) da Rede Corporativa do Estado de Pernambuco por município. Esses números devem ser considerados para a execução da portabilidade, conforme especificado no Termo de Referência e seus Adendos.

6.1.1. Os LICITANTES devem assegurar a capacidade de realizar a portabilidade integral desses PVFs, com o mínimo impacto nos serviços, conforme os requisitos operacionais descritos no Termo de Referência.

6.1.2. O dimensionamento da rede e a infraestrutura proposta devem estar alinhados com os requisitos estabelecidos no Termo de Referência e os padrões normativos vigentes.

Ordem	Município	Quantidade de PVFs
1	Recife	12579
2	Caruaru	845
3	Petrolina	506
4	Garanhuns	360
5	Olinda	352
6	Jaboatão dos Guararapes	352
7	Arcoverde	284
8	Paulista	277
9	Serra Talhada	276
10	Cabo de Santo Agostinho	253
11	Salgueiro	245
12	Palmares	243
13	Ipojuca	193
14	Vitória de Santo Antão	179
15	Limoeiro	176
16	Afogados da Ingazeira	175
17	Goiana	153
18	Ouricuri	132
19	Camaragibe	124
20	Nazaré da Mata	101
21	Pesqueira	100
22	Fernando de Noronha	93
23	Belo Jardim	90
24	Abreu e Lima	82
25	Araripina	81
26	Santa Cruz do Capibaribe	77
27	Igarassu	75
28	Surubim	69
29	São Lourenço da Mata	65
30	Carpina	65
31	Bezerros	60
32	Floresta	55
33	Ilha de Itamaracá	50
34	Gravatá	49
35	Carnaubeira da Penha	48
36	Timbaúba	40
37	Belém de São Francisco	38
38	Petrolândia	37
39	Cabrobó	35
40	Paudalho	34
41	Buíque	33
42	Ribeirão	33
43	Itaquitinga	29

44	São Bento do Una	28
45	Sertânia	28
46	Ibimirim	26
47	Custódia	24
48	Tacaratu	23
49	Escada	23
50	Santa Maria da Boa Vista	22
51	Canhotinho	22
52	Tabira	21
53	Jatobá	21
54	Exu	21
55	Inajá	20
56	São Caetano	20
57	Itambé	20
58	Ipubi	18
59	São José do Belmonte	18
60	Bom Conselho	18
61	Barreiros	18
62	Lajedo	18
63	Agrestina	17
64	Brejinho	17
65	Carnaíba	17
66	Mirandiba	17
67	Águas Belas	17
68	Pedra	17
69	Xexéu	16
70	Parnamirim	16
71	Glória do Goitá	16
72	Altinho	15
73	Brejo da Madre de Deus	15
74	Macaparana	15
75	Catende	15
76	Gameleira	15
77	São José da Coroa Grande	15
78	Tacaimbó	15
79	Bom Jardim	15
80	Taquaritinga do Norte	15
81	Itapetim	15
82	Bonito	15
83	Afrânio	15
84	Tuparetama	14
85	Sirinhaém	14
86	Itapissuma	14
87	Alagoinha	14

88	Toritama	13
89	Cupira	13
90	Venturosa	13
91	Rio Formoso	13
92	Pombos	13
93	Serrita	13
94	Triunfo	13
95	Sanharó	13
96	Lagoa Grande	13
97	Aliança	13
98	Água Preta	12
99	Tamandaré	12
100	Flores	12
101	Saloá	12
102	Jurema	12
103	Verdejante	12
104	Panelas	12
105	João Alfredo	12
106	Vertentes	11
107	Bodocó	11
108	Correntes	11
109	Moreno	11
110	Caetés	11
111	Orobó	11
112	São Joaquim do Monte	11
113	Orocó	11
114	Cumaru	11
115	Passira	11
116	Tracunhaém	11
117	Cachoeirinha	11
118	Vicência	11
119	Trindade	10
120	Iguaraci	10
121	Camocim de São Félix	10
122	Itaíba	10
123	Sairé	10
124	Santa Maria do Cambucá	10
125	Moreilândia	10
126	Quipapá	10
127	Amaraji	9
128	Maraial	9
129	São José do Egito	9
130	Lagoa do Itaenga	9
131	Santa Cruz da Baixa Verde	9

132	Poção	8
133	Tupanatinga	8
134	Jupi	8
135	São João	8
136	Dormentes	8
137	Capoeiras	8
138	Itacuruba	8
139	Cedro	8
140	Ferreiros	7
141	Granito	7
142	Camutanga	7
143	Brejão	7
144	São Vicente Férrer	7
145	Iati	7
146	Santa Terezinha	7
147	Angelim	7
148	Paranatama	7
149	Manari	7
150	Ingazeira	7
151	Ibirajuba	7
152	Terra Nova	7
153	Santa Filomena	7
154	Terezinha	6
155	São Benedito do Sul	6
156	Lagoa dos Gatos	6
157	Jataúba	6
158	Lagoa do Carro	6
159	Betânia	6
160	Lagoa do Ouro	6
161	Solidão	6
162	Riacho das Almas	6
163	Frei Miguelinho	6
164	Chã Grande	6
165	Palmeirina	6
166	Primavera	6
167	Calçado	5
168	Calumbi	5
169	Cortês	5
170	Araçoiaba	5
171	Santa Cruz	5
172	Jucati	5
173	Vertente do Lério	5
174	Salgadinho	5
175	Buenos Aires	5

176	Quixabá	5
177	Casinhas	4
178	Machados	4
179	Barra de Guabiraba	4
180	Condado	4
181	Feira Nova	4
182	Jaqueira	4
183	Chã de Alegria	3
184	Belém de Maria	3
185	Joaquim Nabuco	2
<b>Total Geral</b>		<b>20754</b>

## 7. Tráfego consumido - Solução de Tráfego Extrarrede

7.1. A tabela abaixo apresenta a minutagem consumida de operação real do serviço no ano de 2024 pela Solução de Tráfego Extrarrede, segmentada por tipo de ligação. Esses dados foram extraídos do bilhetador do contrato atual do Governo (coluna "Tipo da Ligação") e têm como objetivo auxiliar as LICITANTES na elaboração de propostas técnicas e comerciais, fornecendo uma base para a estimativa de custos. Todas as informações abaixo estão apresentadas na unidade de medida de minutos.

PRODUTO	jan/24	fev/24	mar/24	abr/24	mai/24	jun/24	jul/24	ago/24	set/24	out/24	nov/24	dez/24
CHAMADA DE LONGA DISTÂNCIA PARA FIXO	176,9	149,50	151,00	216,90	133,60	99,90	97,40	133,40	329,40	582,20	730,60	185,50
CHAMADA DE LONGA DISTÂNCIA PARA FIXO - D01	515,1	530,10	738,00	529,20	599,40	371,80	553,70	163,20	207,10	121,20	148,70	143,30
CHAMADA DE LONGA DISTÂNCIA PARA FIXO - D02	388,9	315,90	456,70	430,80	479,70	374,40	235,30	198,90	138,30	201,10	116,70	56,90
CHAMADA DE LONGA DISTÂNCIA PARA FIXO - D03	1.198,00	1.090,70	1.023,70	067,00	935,50	985,30	815,50	664,40	487,20	471,10	1.851,20	223,60
CHAMADA DE LONGA DISTÂNCIA PARA FIXO - D04	1.036,10	1.115,60	1.226,60	1.491,30	1.343,90	1.175,80	1.665,40	679,80	695,60	609,60	756,60	503,80
CHAMADA DE LONGA DISTÂNCIA PARA MOVEL (VC2)	2.222,70	2.090,10	2.432,70	2.105,80	1.005,70	1.529,80	1.509,80	1.093,10	879,30	970,90	1.111,60	096,50
CHAMADA DE LONGA DISTÂNCIA PARA MOVEL (VC3)	1.830,60	1.440,40	1.063,00	1.489,60	1.103,80	994,30	1.567,60	1.045,90	1.026,40	1.351,80	986,70	974,30
CHAMADA DESTINO MOVEL GRUPO GOV-PE	7.233,80	10.255,70	11.358,80	8.682,60	7.787,30	7.210,60	5.196,50	5.997,10	5.470,90	9.694,10	7.368,10	5.673,00
CHAMADA ENTRANTE	1.313.422,60	1.260.798,90	1.334.342,70	1.455.934,70	1.419.205,40	1.156.448,80	1.676.092,00	1.379.364,60	1.104.438,80	1.187.040,10	1.144.109,30	656.697,60
CHAMADA LOCAL PARA FIXO	47.485,40	41.817,80	49.800,90	52.824,20	48.520,40	39.589,10	46.166,60	37.032,60	34.953,00	41.835,00	39.430,50	30.352,10
CHAMADA LOCAL PARA MOVEL (VC1)	130.234,20	127.399,00	112.054,60	116.127,20	123.915,00	94.528,70	89.201,10	79.085,80	91.059,30	90.479,30	80.435,20	70.043,00
CHAMADA PARA 0800	42.274,90	36.816,30	34.675,30	32.067,70	31.553,10	29.604,70	25.300,80	21.836,00	23.157,00	23.254,10	20.028,90	19.092,50
CHAMADA PARA 3000 - NÚMERO UNICO NACIONAL	0,1	0,70	0,30	8,80	0,10	0,50	0,20	0,10	0,10	2,60	0,00	0,10
CHAMADA PARA 4000 - NÚMERO UNICO NACIONAL	31,1	76,10	14,60	40,70	5,60	2,20	0,20	8,50	0,00	12,16	134,30	34,00
CHAMADA PARA NÚMERO UNICO NACIONAL	14.208,60	11.017,10	13.289,50	17.693,10	14.923,00	11.757,50	12.226,10	10.252,00	9.480,80	9.770,80	11.184,30	7.813,00
CHAMADA PARA SERVICOS	2.132,70	1.317,70	1.665,10	1.585,30	1.547,70	1.205,00	976,50	629,00	1.043,00	700,70	926,50	671,10
DDI - CHAMADA INTERNACIONAL	1,2	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,30	0,00	0,00
CHAMADA INTRA-REDE	257.852,50	247.514,70	270.458,00	298.493,30	266.664,90	221.842,30	246.017,80	249.829,00	219.318,20	235.156,80	208.703,50	177.683,10

7.2. Destacam-se alguns tipos de tráfego relevantes para a identificação/dimensionamento da capacidade da solução:

- CHAMADA ENTRANTE: Representa o volume total de chamadas recebidas pelos terminais do Governo. Estas chamadas são tarifadas diretamente às operadoras originadoras, seguindo as tarifas reguladas pela ANATEL (TU-RL, TU-RIU1, TU-RIU2).
- CHAMADA PARA 0800: Refere-se a chamadas destinadas a serviços do tipo 0800.
- CHAMADA PARA SERVIÇOS: Tráfego relacionado a serviços como números Trídígito (por exemplo, números de emergência).
- CHAMADA INTRA-REDE: Refere-se às ligações VoIP realizadas dentro da rede, sem a necessidade de passar por uma rede externa.

7.3. Esses tipos de ligação devem ser considerados para o correto dimensionamento do link SIP da solução, garantindo a capacidade de escoar adequadamente todo o tráfego gerado.

7.4. As colunas identificadas com os meses detalham o consumo mensal em minutos durante todo ano de 2024. Esses dados são fornecidos para auxiliar no planejamento da capacidade técnica e na estrutura de custos. Ressalta-se que os valores apresentados são históricos e não configuram garantia de consumo futuro. Cabe à LICITANTE analisar e considerar essas informações como base para a elaboração de suas estimativas.

7.5. Devido à natureza variável do tráfego, cabe às LICITANTES realizar estimativas próprias para elaboração das propostas técnicas e comerciais. A CONTRATANTE não se responsabiliza por variações nos perfis de consumo e reitera que a tabela apresentada serve como base exemplificativa para análise e não substitui a necessidade de avaliação detalhada por parte das LICITANTES.

7.6. A LICITANTE deverá garantir que a infraestrutura e os recursos propostos sejam dimensionados para suportar adequadamente o escoamento do tráfego extrarrede, atendendo plenamente aos requisitos técnicos e operacionais estabelecidos no Termo de Referência e seus Adendos.

7.7. A CONTRATADA deverá assegurar que o dimensionamento da solução permita expansões automáticas e dinâmicas em caso de incremento de demanda, sem comprometer os Níveis Mínimos de Serviço (NMS) estabelecidos.

8. Tráfego consumido – ADENDO XV - Serviço tráfego telefônico extrarrede reverso, do tipo Discagem Direta Gratuita (DDG)) - Serviço 0800

8.1. A tabela a seguir apresenta a minutagem total consumida no ano de 2024 pelo Serviço 0800, segmentada por tipo de ligação tarifada. Esses dados devem ser utilizados pelos LICITANTES para ajudar dimensionar a capacidade da rede e os recursos necessários para atender à demanda.

ITEM SERVIÇO E-FISCO	UNID.	jan/24	fev/24	mar/24	abr/24	mai/24	jun/24	jul/24	ago/24	set/24	out/24	nov/24	dez/24
Serviço fixo interestadual	MIN	182,9	177,90	350,80	235,70	187,20	213,50	154,60	252,50	299,80	201,30	182,90	207,90
Serviço longa inter regional fixo	MIN	269,5	333,80	445,40	267,00	344,60	447,20	393,30	410,90	178,80	314,20	206,50	184,90
Serviço fixo intraestadual	MIN	14.186,40	12.569,00	12.681,50	10.135,70	11.524,20	10.952,30	8.961,50	7.330,30	8.012,90	7.714,70	6.367,00	7.677,00
Serviço fixo local	MIN	67.052,40	58.294,10	83.804,80	57.663,40	54.321,80	56.864,30	59.764,80	46.698,70	49.887,50	51.355,20	47.262,40	58.518,30
Serviço móvel local	MIN	478.936,70	417.494,60	556.676,70	435.376,30	488.938,40	435.496,90	303.540,30	328.002,00	303.594,40	333.641,80	304.107,20	371.260,40
Serviço móvel VC2	MIN	56,7	57,3	75,1	80	105,5	49,3	52,2	404,10	420,20	588,50	329,50	604,70
Serviço móvel intraestadual	MIN	91547	90472	110159,3	97807,6	117662	86342,1	75797,4	71.853,40	81.944,10	86.560,90	77.679,20	109.963,90
Serviço móvel VC3	MIN	121,50	80,50	75,90	107,00	79,90	97,70	56,40	338,30	641,20	474,50	496,50	432,20

9. Ainda com o objetivo de auxiliar as Proponentes no dimensionamento da solução de voz a ser contratada, apresentamos abaixo as informações adicionais para embasar as estimativas dos recursos de cloud e canais de comunicação:

#### 9.1. Quantidade de Canais Utilizados

9.1.1. **Total de sessões:** O sistema conta atualmente com 600 sessões simultâneas para originar e receber chamadas, sem distinção entre chamadas internas (entre extensões da mesma rede) e externas (para fora da rede).

#### 9.2. Taxa de Ocupação dos Canais

9.2.1. **Taxa máxima de ocupação:** A máxima utilização registrada no último ano foi de 300 sessões simultâneas. No entanto, as proponentes devem considerar adicionalmente, que solução proposta deve ser escalável e capaz de gerenciar picos de utilização, assegurando a continuidade do serviço.

#### 9.3. Tempo Médio de Duração das Ligações

9.3.1. **Duração média das chamadas:** A duração média das chamadas é de 2,22 minutos, tanto para chamadas internas quanto para externas.

#### 9.4. Tráfego em Erlangs

9.4.1. **Histórico de tráfego:** Com base nos cálculos atuais, a carga de tráfego registrada é de aproximadamente 9,17 Erlangs, considerando chamadas com duração média de 2,2 minutos cada.

10. A solução proposta pela Proponente deve suportar eficientemente este tráfego, além de apresentar capacidade de expansão, caso seja necessário elevar os recursos e sem custos adicionais para CONTRATANTE.

### ANEXO E - MATRIZ DE RISCOS

Segundo o art. 14 do Decreto Estadual nº 53.384, de 22 de agosto de 2022, a matriz de riscos é o instrumento que permite a identificação das situações futuras e incertas que possam impactar o equilíbrio econômico-

financeiro do contrato, bem como a definição das medidas necessárias para tratar os riscos e as responsabilidades entre as partes.

Objeto da contratação: 1.1.O objeto da presente licitação é a contratação de prestações de serviços de rede corporativa segura com acesso à Internet, envolvendo implantação, operacionalização e melhoria contínua de serviços de acesso à Internet, conectividade de rede local e datacenter, voz, comunicação unificada, contact center, segurança e operação integrada de redes de computadores, visando atender as necessidades dos órgãos da Administração Direta, Indireta, Fundos Especiais, Autarquias e Fundações Públicas integrantes do Poder Executivo do Estado de Pernambuco, conforme as condições, especificações, quantidades e exigências contidas neste Termo de Referência e seus adendos.

MATRIZ DE RISCOS			
EVENTO DE RISCO	NÍVEL DE RISCO	MEDIDA PROPOSTA	ALOCÇÃO
Ocorrência de eventos fortuitos ou de força maior, como fenômenos climáticos e ambientais excepcionais (ex.: chuvas intensas, vendavais, descargas atmosféricas), causando danos a equipamentos e infraestruturas disponibilizados pela CONTRATADA para a execução do contrato.	RB - RISCO BAIXO	<p><b>Medida Preventiva:</b></p> <p><b>Contratada:</b> Tomar todas as providências necessárias para proteger os equipamentos dos efeitos climáticos e instalar equipamentos com rigorosa atenção aos procedimentos e normas de segurança vigentes.</p> <p><b>Contratada:</b> Implementar planos de contingência, incluindo o uso de equipamentos e recursos sobressalentes para rápida substituição em caso de danos.</p> <p><b>Contratada:</b> Avaliar a contratação de seguro abrangente para equipamentos e infraestruturas, cobrindo danos causados por eventos fortuitos ou de força maior.</p> <p><b>Contratante:</b> Garantir que as especificações contratuais definam claramente a responsabilidade da CONTRATADA pela segurança física de equipamentos e materiais localizados fora dos sites governamentais.</p> <p><b>Medida Corretiva:</b></p> <p><b>Contratada:</b> Repor ou reparar os equipamentos danificados na maior brevidade possível, sem custos adicionais para a CONTRATANTE.</p> <p><b>Contratada:</b> Apresentar à CONTRATANTE relatórios dos danos ocorridos</p>	CONTRATADA

		<p>e das ações corretivas adotadas.</p> <p><b>Contratada:</b> Revisar os protocolos de prevenção para mitigar os riscos em áreas com maior exposição a fenômenos naturais.</p>	
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<p>Ocorrência de furto, roubo, dano ou extravio de cabos, equipamentos, peças, componentes e periféricos em ambientes fora do site do governo (PCS).</p>	<p>RM - RISCO MÉDIO</p>	<p><b>Medida Preventiva:</b></p> <p><b>Contratante:</b> Garantir que as especificações contratuais definam claramente a responsabilidade da CONTRATADA pela segurança física de equipamentos e materiais localizados fora dos sites governamentais.</p> <p><b>Contratada:</b> Avaliar a implementação de seguros contra furto, roubo e danos de materiais sensíveis localizados fora do site, mitigando prejuízos financeiros.</p> <p><b>Contratada:</b> Instalar equipamentos com rigorosa atenção aos procedimentos de segurança, visando maximizar a eficiência na proteção e dificultar a ocorrência de furtos.</p> <p><b>Contratada:</b> Implementar planos de contingência, incluindo o uso de equipamentos e recursos sobressalentes para rápida substituição em caso de danos.</p> <p><b>Medidas Corretivas:</b></p> <p><b>Contratada:</b> Substituir ou reparar imediatamente os itens danifica-</p>	<p>CONTRATADA</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------

		<p>dos, furtados ou extraviados, garantindo a continuidade dos serviços contratados, sem custos adicionais para a CONTRATANTE.</p> <p><b>Contratada:</b> Apresentar relatórios detalhados do incidente à CONTRATANTE, incluindo evidências de acionamento do seguro (caso contratado) e prazos para reposição dos itens.</p>	
<p>Ocorrência de furto, roubo, dano ou extravio de cabos, equipamentos, peças, componentes e periféricos em ambientes internos e sob controle do site do governo (PCS).</p>	<p>RMB - RISCO MUITO BAIXO</p>	<p><b>Medida Preventiva:</b></p> <p><b>CONTRATANTE:</b> Avaliar a implementação de medidas de segurança adequadas para proteger os equipamentos alocados em suas propriedades, incluindo vigilância, controle de acesso e monitoramento.</p> <p><b>CONTRATANTE:</b> Estabelecer cláusulas contratuais que definam de forma clara as responsabilidades da CONTRATANTE Aderente em caso de furto, roubo ou danos por mau uso, assegurando que os prejuízos sejam ressarcidos à CONTRATADA.</p> <p><b>Medidas Corretivas:</b></p> <p><b>Contratante:</b> Ressarcir à CONTRATADA os prejuízos causados, com base em cotações de preços de mercado obtidas junto a três empresas para itens iguais ou similares, acompanhadas da Nota Fiscal de compra efetuada pela CONTRATADA.</p> <p><b>Contratada:</b> Apresentar documentação detalhada à CONTRATANTE, incluindo as cotações ob-</p>	<p>CONTRATANTE</p>

		<p>tidas e a Nota Fiscal da compra realizada, para garantir transparência no processo.</p> <p><b>Contratante:</b> Monitorar a execução do processo de reposição para assegurar que os valores ressarcidos sejam adequados e cumpram o estabelecido em contrato.</p>	
<p>Aumento do dólar comercial de até 50% durante o período contratual, considerando como referência a taxa PTAX de venda</p> <p>divulgada pelo Banco Central na data de ocorrência do certame, impactando a aquisição de insumos importados.</p>	RM - RISCO MÉDIO	<p><b>Medida Preventiva:</b></p> <p><b>Contratante:</b> Inserir cláusulas contratuais que definam explicitamente que os riscos associados à oscilação cambial são de responsabilidade exclusiva da CONTRATADA, estabelecendo a taxa de referência como PTAX de venda na data do certame.</p> <p><b>Contratante:</b> Garantir ampla divulgação do edital e das condições contratuais para que os licitantes possam precificar adequadamente os impactos cambiais.</p> <p><b>Contratada:</b> Avaliar aquisições com estratégias de hedge cambial ou similares, para mitigar os impactos financeiros da oscilação do dólar.</p> <p><b>Medida Corretiva:</b></p> <p><b>Contratada:</b> Assumir os custos adicionais derivados da oscilação cambial dentro do limite estabelecido no contrato, sem repasse ou pedido de reequilíbrio.</p> <p><b>Contratante:</b> Monitorar o cum-</p>	CONTRATADA

		<p>primento contratual e aplicar as sanções previstas em caso de não execução por parte da CONTRATADA.</p>	
<p>Aumento do dólar superior a 50% durante o período contratual, considerando como</p> <p>referência a taxa PTAX de venda divulgada</p> <p>pelo Banco Central na data de ocorrência do certame, aplicando-se o impacto</p> <p>exclusivamente ao excedente superior a 50% da variação cambial.</p>	<p>RB - RISCO BAIXO</p>	<p><b>Medida Preventiva:</b></p> <p><b>Contratante:</b> Inserir cláusulas contratuais que prevejam a responsabilidade da CONTRATANTE sobre o impacto cambial para variações superiores a 50%, exclusivamente no excedente, tomando como referência a taxa PTAX de venda do Banco Central.</p> <p><b>Contratante:</b> Definir procedimentos e prazos para solicitação de reequilíbrio econômico-financeiro, incluindo a obrigatoriedade de comprovação documental da variação e dos custos impactados.</p> <p><b>Contratada:</b> Manter registros detalhados de aquisição de insumos e serviços afetados pela variação cambial, vinculados ao contrato, para justificar formalmente a solicitação de reequilíbrio. <b>Medida Corretiva:</b></p> <p><b>Contratada:</b> Disponibilizar à CONTRATANTE os seguintes documentos como condição para análise do reequilíbrio: notas fiscais e contratos relacionados aos insumos afetados, histórico de taxas cambiais aplicadas, e planilhas detalhadas de impacto financeiro com valores segregados (base e excedente superior a</p>	<p>CONTRATANTE</p>

		<p>50%).</p> <p><b>Contratante:</b> Avaliar a documentação fornecida, realizar auditorias ou consultas a órgãos externos para validação, e formalizar aditivos contratuais para reequilibrar o valor excedente.</p> <p><b>Contratante:</b> Estabelecer prazo de resposta para análise e efetivação do reequilíbrio, garantindo previsibilidade para a CONTRATADA.</p>	
<p>Implantação de serviços próximo ao encerramento do contrato, não gerando ROI (Return Of Investment) suficiente para a contratada</p>	<p>RM - RISCO MÉDIO</p>	<p><b>Medida Preventiva:</b></p> <p><b>Contratante:</b> Estabelecer cláusulas contratuais claras que detalhem a natureza do contrato por demanda, assegurando que os licitantes estejam cientes da inexistência de garantia de volume total de execução.</p> <p><b>Contratada:</b> Elaborar planejamento operacional e financeiro flexível, capaz de ajustar recursos humanos e materiais conforme as variações na demanda.</p> <p><b>Contratada:</b> Precificar os serviços considerando os cenários de execução, incorporando margens para lidar com variações na demanda.</p> <p><b>Medida Corretiva:</b></p> <p><b>Contratada:</b> Garantir a prestação de serviços conforme solicitado pela CONTRATANTE, independentemente da quantidade demandada, dentro dos limites previstos no contrato.</p> <p><b>Contratante:</b> Monitorar a execução e o cumprimento dos serviços demandados, aplicando penalidades contratuais em caso de descumprimento por parte da CONTRATADA.</p> <p><b>Contratada:</b> Manter flexibilidade operacional e ajustar alocações internas de recursos para</p>	<p>CONTRATADA</p>

		atender às variações na demanda sem comprometer a qualidade.	
--	--	--------------------------------------------------------------	--

## ANEXO F - ARQUITETURA DO SISTEMA GESTÃO DE ORDENS - SGOS

### Arquitetura e Topologia do Sistema PECONECTA

Versão do Documento: 2.0

Data: 23 de março de 2026

Ambiente: Produção

Sistema: PE Conecta

2026

## Sumário

INTRODUÇÃO .....	4
VISÃO GERAL .....	4
TOPOLOGIA DO AMBIENTE DE PRODUÇÃO .....	4
1. Infraestrutura .....	4
2. Diagrama de Topologia do Ambiente de Produção .....	5
2.1. Comunicação com Bancos de Dados .....	6
2.2. Integrações Externas .....	6
2.3. Protocolos de Comunicação .....	7
2.4. Considerações de Segurança .....	7
2.5. Conclusão da Topologia .....	7
2.6. Hospedagem no IIS .....	7
3. ARQUITETURA DA APLICAÇÃO .....	8
3.1. Padrão Arquitetural .....	8
3.2. Descrição das Camadas .....	8
4. ADOÇÃO DO PADRÃO CQRS .....	9
4.1. Fluxo de Escrita (Command) .....	9
4.2. Fluxo de Leitura (Query) .....	9
5. PERSISTÊNCIA DE DADOS .....	10
5.1. SQL Server .....	10
5.2. MongoDB .....	10
6. INTEGRAÇÃO EXTERNAS .....	10
6.1. API de Cadastros .....	10
6.2. API de Relatórios .....	10
7. SEGURANÇA .....	10
8. CONSIDERAÇÕES OPERACIONAIS .....	11
9. CONCLUSÃO .....	11
10. ACESSO E CREDENCIAIS .....	11
10.1. Modelo de Controle de Acesso .....	11
10.2. Perfil do Sistema .....	11

10.3.	Perfis Administrativos .....	13
10.4.	Segregação de Funções .....	14
10.5.	Autenticação e Gestão de Credenciais .....	14
11.	INTEGRAÇÃO E DEPENDÊNCIAS CRÍTICAS .....	14
11.1.	Visão Geral .....	14
11.2.	Sistemas Externos Integrados .....	15
11.3.	Dependências de Banco de Dados .....	15
11.4.	Dependências de Infraestrutura .....	16
11.5.	Protocolos e Contratos de Comunicação .....	16
12.	Rede .....	17
12.1.	Topologia .....	17
12.2.	Funcionamento .....	18
13.	Backup .....	18
13.1.	Infraestrutura .....	18
13.2.	Diagrama de Topologia do Ambiente de backup .....	19
13.3.	Agendamento & Retenção de dados .....	19
CONCLUSÃO .....		20

## INTRODUÇÃO

Este documento apresenta a arquitetura técnica do sistema PE Conecta, descrevendo sua estrutura tecnológica, componentes principais, integrações externas e mecanismos de segurança adotados na solução.

A documentação tem como objetivo fornecer uma visão estruturada da aplicação, incluindo aspectos relacionados à infraestrutura, organização arquitetural, fluxos de comunicação entre sistemas e dependências críticas necessárias para o funcionamento da plataforma.

Além de servir como referência técnica para desenvolvimento e manutenção do sistema, este documento também apoia atividades de governança de tecnologia da informação, auditoria, gestão de infraestrutura e planejamento de evolução da solução.

Dessa forma, este documento busca consolidar as principais informações técnicas do sistema PE Conecta, garantindo maior transparência sobre sua arquitetura e facilitando a compreensão de sua estrutura por equipes técnicas, gestores e demais partes interessadas.

## VISÃO GERAL

O presente documento descreve a arquitetura, topologia e fluxos de integração do sistema PE Conecta, desenvolvido com frontend em Angular 15 e backend em .NET 6.

A aplicação adota os princípios de Clean Architecture e o padrão CQRS (Command Query Responsibility Segregation), promovendo separação de responsabilidades, organização estrutural e escalabilidade.

Apersistênciadadosérealizadautilizando:

- SQLServer—armazenamentodedadostransacionais;
- MongoDB—armazenamentocomplementar(ArmazenamentodeOrdensdeServiço “Legado”jáfinalizadanosistema Integra).

Osistemaintegra-seaindacom:

- APIdeCadastros(.NET+SQL Server);
- APIdeRelatórios(.NET +SQL Server).

O sistema opera exclusivamente em **ambiente de Produção**, hospedado em máquina virtual Windows Server com aplicação publicada no IIS (Internet Information Services).

## TOPOLOGIA DO AMBIENTE DE PRODUÇÃO

### 1. Infraestrutura

Oambiente deProduçãoécompotoppor:

- MáquinaVirtual(VM)comsistemaoperacionalWindowsServer;
- IIS(InternetInformationServices)comoservidor web;
- AplicaçãoAngularpublicadacomoaplicaçãowebnoIIS;
- API.NET6publicadanoIIS;
- BancodeDadosSQL Server;
- BancodeDados MongoDB;
- IntegraçãocomAPIsexternas.

### 2. Diagrama de Topologia do Ambiente de Produção

Figura1—DiagramadeArquiteturaeIntegraçãodoAmbiente de Produção

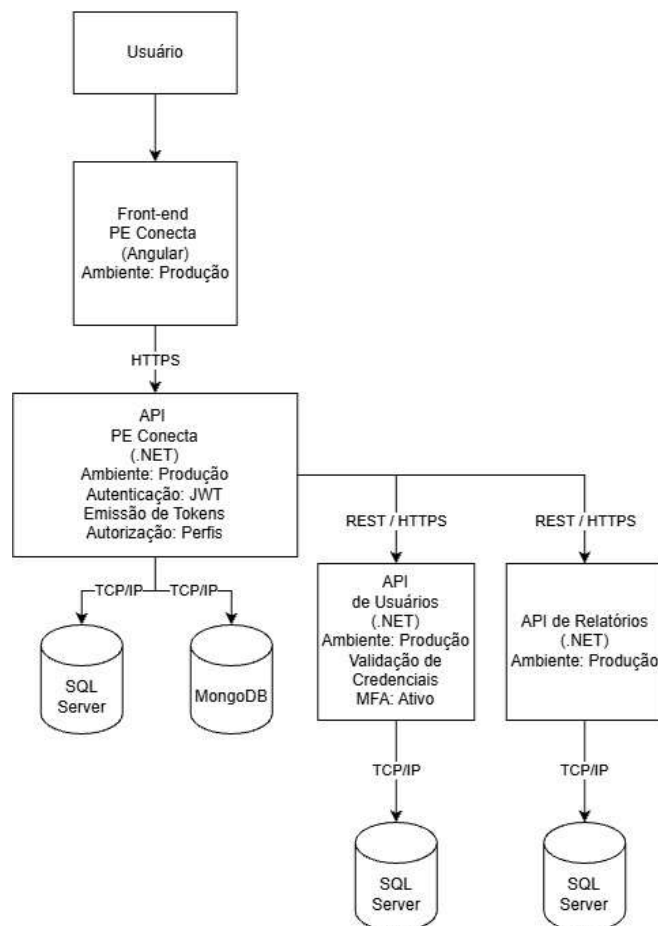


Figura1 Apresenta a topologia completa do ambiente de Produção do sistema, demonstrando os componentes internos, integrações externas, protocolos de comunicação e mecanismos de autenticação adotados.

Conforme ilustrado na Figura1, o fluxo operacional do sistema ocorre da seguinte forma:

1. O **Usuário** acessa o sistema por meio do Front-end da aplicação;

Figura1 Apresenta a topologia completa do ambiente de Produção do sistema, demonstrando os componentes internos, integrações externas, protocolos de comunicação e mecanismos de autenticação adotados.

Conforme ilustrado na Figura 1, o fluxo operacional do sistema ocorreu da seguinte forma:

2. O **Usuário** acessa o sistema por meio do Front-end da aplicação;
3. O **Front-end PE Conecta (Angular)**, hospedado no IIS em ambiente de Produção, realiza comunicação segura via HTTPS com a API principal;
4. A **API PE Conecta (.NET6)** é responsável pelo processamento das requisições, aplicação das regras de negócio e controle de autenticação e autorização.

A API principal implementa:

- Autenticação baseada em JWT (JSON Web Token);
- Emissão e validação de tokens;
- Controle de autorização baseado em perfis (roles).

## 2.1. Comunicação com Bancos de Dados

Conforme demonstrado na Figura 1, a API principal comunica-se diretamente com:

- SQL Server, responsável pelos dados transacionais da aplicação;
- MongoDB, utilizado para armazenamento complementar, de Ordens de Serviço já fechadas no sistema Integra.

A comunicação com os bancos ocorre via protocolo TCP/IP, dentro da rede interna do ambiente de Produção.

## 2.2. Integrações Externas

A Figura 1 demonstra ainda a integração da API principal com sistemas externos por meio de chamadas REST sobre HTTPS:

### a) API de Usuários (.NET)

Responsável por:

- Validação de credenciais;
- Processo de autenticação;
- Suporte a MFA (Multi-Factor Authentication), quando aplicável.

Fluxo:

API Principal → REST/HTTPS → API de Usuários → SQL Server de Usuários

### b) API de Relatórios (.NET)

Responsável por:

- Geração e consultação de relatórios;
- Recuperação de dados consolidados;
- Processamento de informações externas a domínio principal da aplicação.

Fluxo:

API Principal → REST/HTTPS → API de Relatórios → SQL Server de Relatórios

## 2.3. Protocolos de Comunicação

De acordo com a Figura 1, os seguintes protocolos são utilizados:

- HTTPS – Comunicação entre Front-ende API;
- REST/HTTPS – Comunicação entre APIs;
- TCP/IP – Comunicação com bancos de dados.

Essa estrutura garante:

- Segurança na transmissão de dados;
- Isolamento de camadas;
- Separação clara de responsabilidades entre sistemas.

## 2.4. Considerações de Segurança

Conforme ilustrado na Figura 1, o sistema adota as seguintes práticas de segurança:

- Autenticação via JWT;
- Controle de autorização por perfis;
- Validação de credenciais em API dedicada;
- Suporte a MFA na autenticação de usuários;
- Comunicação criptografada via HTTPS;
- Acesso aos bancos restrito à rede interna.

## 2.5. Conclusão da Topologia

A topologia apresentada na Figura 1 demonstra uma arquitetura centralizada, com separação clara entre:

- Camada de apresentação;
- Camada de aplicação;
- Persistência de dados;
- Serviços externos integrados.

Essa organização promove maior controle de segurança, manutenção facilitada e escalabilidade controlada dentro do ambiente único de Produção.

## 2.6. Hospedagem no IIS

O IIS é responsável por:

- Hospedagem da aplicação Angular (arquivos estáticos);
- Hospedagem da API.NET 6;
- Gerenciamento de Application Pools;
- Controle de bindings HTTPS;
- Gerenciamento de certificados digitais;
- Controle de permissões e isolamento da aplicação.

## 3. ARQUITETURA DA APLICAÇÃO

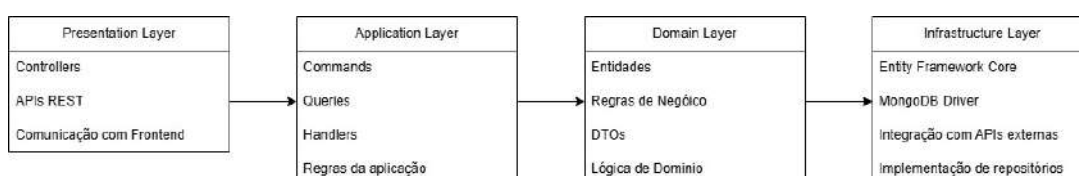
### 3.1. Padrão Arquitetural

A aplicação foi desenvolvida seguindo os princípios de Clean Architecture, garantindo separação entre camadas e independência entre regras de negócio e infraestrutura.

As camadas da aplicação são:

- Presentation Layer;
- Application Layer;
- Domain Layer;
- Infrastructure Layer.

**Figura 2 – Arquitetura em Camadas da Aplicação**



*Figura 2- Apresenta a organização das camadas da aplicação baseada no padrão Clean Architecture.*

Esse modelo estabelece uma separação clara entre responsabilidades, permitindo que as regras de negócio permaneçam independentes de tecnologias de infraestrutura.

A camada **Presentation** é responsável pela exposição dos endpoints e interação com o cliente da aplicação.

A camada **Application** coordena os fluxos da aplicação por meio de Commands, Queries e Handlers, implementando o padrão CQRS.

A camada **Domain** concentra as entidades e regras de negócio centrais do sistema, mantendo independência de frameworks e tecnologias externas.

Por fim, a camada **Infrastructure** implementa os mecanismos de persistência de dados, integrações externas e demais dependências técnicas necessárias para o funcionamento da aplicação.

### 3.2. Descrição das Camadas

#### Presentation Layer

Responsável por:

- Controllers REST;
- Recebimento de requisições HTTP;
- Validação de entrada;
- Autenticação e autorização.

#### Application Layer

Responsável por:

- Commands (operações de escrita);
- Queries (operações de leitura);
- Handlers;
- DTOs;
- Orquestração dos fluxos de negócio.

#### Domain Layer

Responsável por:

- Entidades;
- Regras de negócio;
- Interfaces;
- Lógica central do sistema.

#### Infrastructure Layer

Responsável por:

- Implementação de repositórios;
- Configuração do EF Core (Code First);
- Implementação de acesso ao MongoDB;
- Integração com APIs externas via HttpClient;

- Configuraçãodepersistência.

## 4. ADOÇÃO DOPADRÃO CQRS

Apliação adota CQRS para separação entre leitura e escrita.

### 4.1. Fluxo de Escrita (Command)

Angular → Controller → Command → Handler → EFCore → SQL Server

Responsável por:

- Inclusão de registros;
- Atualização de dados;
- Exclusão de registros.

### 4.2. Fluxo de Leitura (Query)

Angular → Controller → Query → Handler → SQL Server ou MongoDB

Responsável por:

- Consultas;
- Listagens;
- Filtros;
- Recuperação de dados.

## 5. PERSISTÊNCIA DE DADOS

### 5.1. SQL Server

- Banco relacional principal;
- Armazenamento de transacionais;
- Estrutura controlada por EF Core (Code First);
- Versionamento via Migrations.

### 5.2. Mongo DB

- Banco NoSQL complementar;
- Utilizado para armazenamento de Ordens de Serviço Legados do sistema Integra apenas para consulta;
- Acesso realizado via driver oficial do MongoDB para .NET.

## 6. INTEGRAÇÕES EXTERNAS

### 6.1. API de Cadastros

Fluxo:

Usuário → Angular → API Principal → API de Cadastros → SQL Server Cadastros

- Comunicação via HTTPS;
- Troca de dados em JSON;
- Validação e consulta de dados cadastrais.

### 6.2. API de Relatórios

Fluxo:

Usuário → Angular → API Principal → API de Relatórios → SQL Server Relatórios

- Comunicação via HTTPS;
- Geração e recuperação de relatórios.

## 7. SEGURANÇA

O sistema implementa:

- Comunicação segura via HTTPS;
- Autenticação baseada em token (ex.: JWT ou mecanismo institucional);

- Controle de acesso baseado em perfis (Roles);
- Restrição de acesso aos bancos de dados;
- Configuração de permissões no IIS e Application Pool dedicado.

## 8. CONSIDERAÇÕES OPERACIONAIS

- O sistema possui ambiente único de Produção;
- Está hospedado em VM Windows Server;
- Publicação realizada no IIS;
- Versionamento do banco realizado via Migrations do EF Core;
- Backups seguem política institucional vigente;
- Atualizações são realizadas mediante processo controlado de publicação.

## 9. CONCLUSÃO

A arquitetura adotada garante:

- Organização estrutural;
- Separação de responsabilidades;
- Manutenibilidade;
- Escalabilidade controlada;
- Segurança e controle de acesso;
- Integração padronizada com sistemas externos.

O modelo implementado está alinhado com as práticas de arquitetura de software para aplicações corporativas em ambiente Windows Server com IIS.

## 10. ACESSOS E CREDENCIAIS

### 10.1. Modelo de Controle de Acesso

O sistema adota modelo de controle de acesso baseado em perfis (Role-Based Access Control – RBAC), no qual cada usuário possui um ou mais perfis associados que determinam suas permissões dentro da aplicação.

As permissões são validadas na API principal por meio da análise das roles presentes no token JWT emitido após autenticação.

O modelo implementa o princípio do menor privilégio, concedendo aos usuários apenas as permissões necessárias para execução de suas atividades funcionais.

## 10.2. Perfis do Sistema

Os perfis atualmente implementados nos sistemas são:  Gestor

| SAD GETEL (Gestor GETEL)

Permissões:

- Visualização integral do sistema;
- Aprovação de ordens de serviço;
- Acompanhamento de fluxos operacionais.

Perfil com responsabilidade decisória no processo de validação e aprovação de demandas.

 Gestor | SADGCCOR (Gestor GCCOR) Permissões:

- Visualização integral do sistema;
- Gerenciamento de contratos;
- Gerenciamento de termos de adesão.

Perfil responsável pela gestão contratual e acompanhamento administrativo.

 Contratada (Técnico/Executor) (Técnico) Permissões:

- Visualização de dados vinculados ao fornecedor associado;
- Execução de ordens de serviço atribuídas.

Perfil operacional vinculado ao fornecedor específico, com escopo restrito às suas atribuições contratuais.

 Gestor de Telemática (Cliente) Permissões:

- Visualização de informações vinculadas à sua organização;
- Cadastro de ordens de serviço.

Perfil responsável pela abertura e acompanhamento de demandas dentro de sua unidade organizacional.

 Gestor Técnico | ATI (ATI)

Permissões:

- Visualização integral do sistema;

- Fechamentodeordensde serviço.

Perfilcomresponsabilidadetécnicasobreencerramentodedemandas.

 Operação Integrada | NOC/ServiceDesk (Validação) Permissões:

- Visualização integral do sistema;
- Validação da execução das ordens de serviço.

Perfil responsável pela validação operacional das execuções realizadas.

 Gestor Auxiliar (Apoio)

Permissões:

- Visualização dos dados vinculados à sua organização;
- Cadastro e gestão de ordens de serviço.

Perfil de apoio operacional com permissões restritas ao escopo organizacional.

 Administrador (Administrador) Permissões:

- Acesso integral ao sistema;
- Execução de todas as ações disponíveis na aplicação.

Perfil com privilégios máximos, destinado à administração do sistema. O uso deste perfil deve ser restrito e monitorado.

 ServiceDesk (ServiceDesk) Permissões:

- Visualização integral do sistema;
- Cadastro e gerenciamento de usuários;
- Administração de acessos.

Perfil responsável pelo suporte e gestão de usuários.

### 10.3. Perfis Administrativos

São considerados perfis administrativos:

- Administrador;
- Service Desk;
- Gestor SADGETEL;
- Gestor SADGCCOR;

- GestorTécnico | ATI;
- OperaçãoIntegrada | NOC/Service Desk.

Esses perfis possuem acesso ampliado e devem ser atribuídos mediante autorização formal, conforme diretrizes institucionais.

A utilização desses perfis está sujeita a auditoria e a rastreabilidade.

#### 10.4. Segregação de Funções

O modelo implementado promove segregação de funções entre:

- Cadastro de demanda (Gestor SAD GCCOR, Gestor de Telemática, Gestor Auxiliar e Service Desk);
- Execução (Técnico Executor);
- Validação (Operação Integrada);
- Aprovação (Gestor SAD GETEL);
- Fechamento (Gestor Técnico | ATI);
- Administração do sistema (Administradores).

Essa separação reduz riscos operacionais e mitiga conflitos de interesse no fluxo de ordens de serviço.

#### 10.5. Autenticação e Gestão de Credenciais

A autenticação é realizada por meio de API dedicada de usuários, com emissão de token JWT contendo:

- Identificação do usuário;
- Perfis associados;
- Tempo de expiração;
- Claims necessárias para autorização.

O sistema pode utilizar MFA (Multi-Factor Authentication), conforme política institucional vigente.

Credenciais:

- Não são armazenadas na aplicação principal;
- São gerenciadas pela API de Usuários;
- Seguem política institucional de segurança (complexidade, expiração e proteção de senha).

### 11. Integrações e Dependências Críticas

#### 11.1. Visão Geral

O sistema PE Conecta integra-se com serviços externos e depende de componentes de infraestrutura essenciais para seu pleno funcionamento.

As integrações ocorrem por meio de APIs REST sobre HTTPS, com troca de dados no formato JSON.

As dependências listadas nesta seção são consideradas críticas para a operação do sistema.

## 11.2. Sistemas Externos Integrados

### API de Usuários

**Tipo:** API REST (.NET)

**Finalidade:** Autenticação e validação de credenciais

**Banco associado:** SQL Server (Base de Usuários)

Responsabilidades:

- Validação de login e senha;
- Emissão de token JWT;
- Gerenciamento de credenciais;
- Suporte a MFA (quando aplicável).

Dependência crítica: Sem a disponibilidade da API de Usuários, não é possível realizar autenticação no sistema.

### API de Relatórios

**Tipo:** API REST (.NET)

**Finalidade:** Geração e consulta de relatórios

**Banco associado:** SQL Server (Base de Relatórios)

Responsabilidades:

- Processamento de dados consolidados;
- Geração de relatórios;
- Retorno de informações estruturadas para consumo pela API principal.

Dependência crítica: A indisponibilidade da API de Relatórios impacta diretamente funcionalidades relacionadas à geração e consulta de relatórios.

## 11.3. Dependências de Banco de Dados

### SQL Server – Base Principal

- Bancorelacional principal da aplicação;
- Armazenado de transacionais;
- Responsável por ordens de serviço ativas, contratos, usuários internos e demais entidades do domínio;
- Gerenciado via Entity Framework Core (Code First).

Dependência crítica: A indisponibilidade do SQL Server implica interrupção das operações de escrita e leitura da aplicação.

#### MongoDB – Base de Dados Legado (Sistema Integra) O

MongoDB é utilizado especificamente para:

- Armazenamento de Ordens de Serviço Legado;
- Consulta de ordens já encerradas provenientes do sistema Integra;
- Preservação histórica de dados migrados.

Trata-se de base complementar, utilizada para consulta de dados históricos, não sendo responsável por dados transacionais ativos do sistema.

Dependência operacional: A indisponibilidade do MongoDB impacta a consulta de ordens de serviço legadas, porém não compromete o funcionamento das funcionalidades principais relacionadas às ordens de serviço atuais.

### 11.4. Dependências de Infraestrutura

#### 11.4.1 Windows Server (VM de Produção)

- Ambiente operacional onde o sistema está hospedado;
- Responsável pela execução do IIS e serviços associados.

#### IIS (Internet Information Services)

- Hospedagem da aplicação Angular;
- Hospedagem da API.NET 6;
- Gerenciamento de Application Pools;
- Gerenciamento de certificados HTTPS.

Dependência crítica: Falhas no IIS no sistema operacional resultam na indisponibilidade total da aplicação.

### 11.5. Protocolos e Contratos de Comunicação

As integrações utilizam:

- REST sobre HTTPS;
- Comunicação síncrona;
- Formato de dados JSON;
- Autenticação baseada em token JWT quando aplicável.

Os contratos de integração são definidos por meio de:

- Endpoints documentados;
- Estruturas de DTO;

- Regras de autenticação;
- Validação de payload.

Alterações nos contratos das APIs externas podem impactar diretamente o funcionamento do sistema, devendo ser previamente validadas.

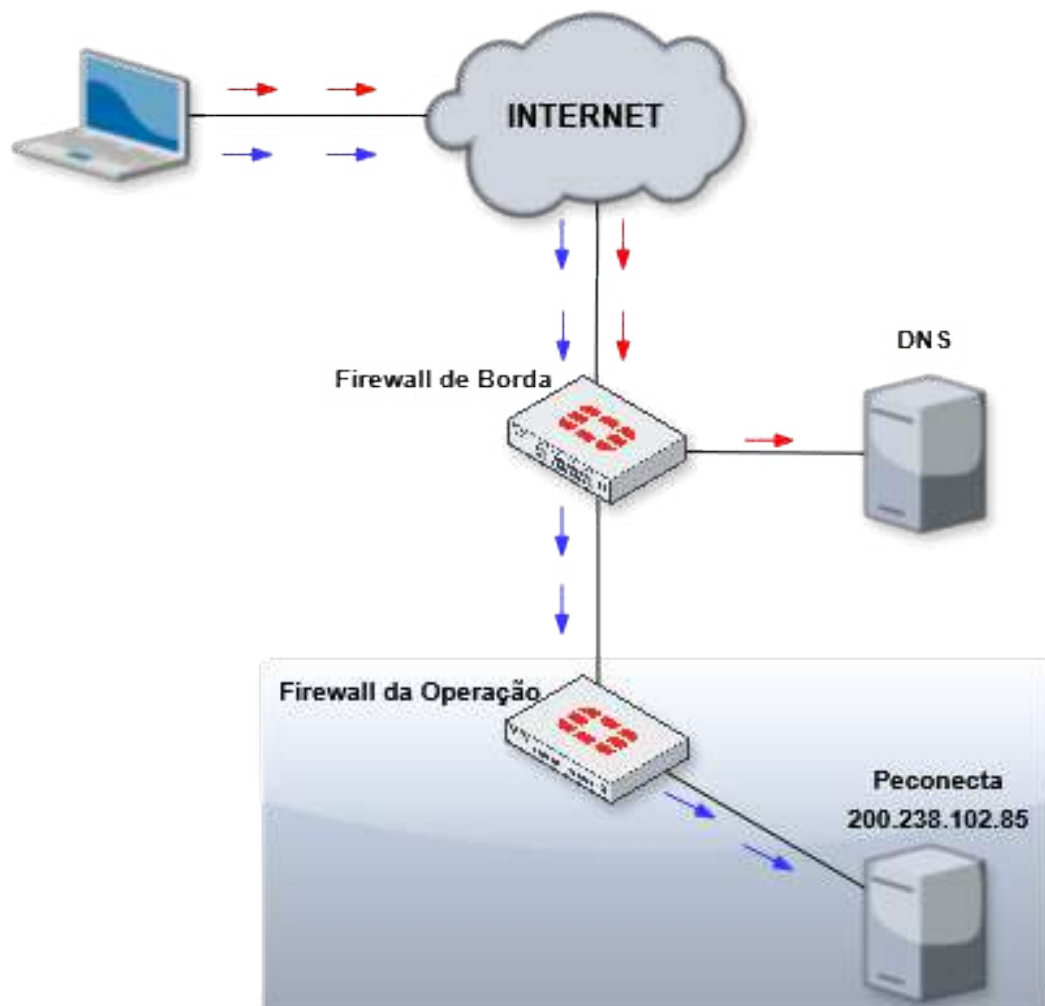
## 12. Rede

A aplicação está disponível na internet e hospedada na rede PEConectado, integrando-se aos serviços de infraestrutura corporativa de tecnologia da informação e comunicação disponibilizados ao governo.

A topologia de serviço acima é estruturada para assegurar proteção dos ativos internos, o controle do tráfego e a adequada segregação dos ambientes:

- Acesso: Internet
- Segurança: Firewall de borda
- Operação: Serviço PECONNECTA

### 12.1. Topologia



## 12.2. Funcionamento

O acesso à aplicação por usuários ocorre conforme o fluxo descrito a seguir:

### Resolução de Nome (DNS)

Ao iniciar o processo de acesso à aplicação, a requisição é inicialmente encaminhada ao serviço de DNS, responsável pela resolução do nome do serviço (FQDN), por meio do firewall de borda. Em seguida, o DNS retorna o endereço IP correspondente à aplicação.

### Encaminhamento de Tráfego (Firewall de Borda)

Após a resolução DNS, o tráfego segue pela internet utilizando o protocolo TCP garantindo a comunicação confiável entre o usuário e a aplicação. O tráfego chega ao firewall de borda que constitui o principal ponto de entrada e saída de todo o tráfego da infraestrutura de rede, atuando como elemento central de segurança perimetral e de integração de conectividade com as redes externas, o qual é inspecionado conforme as políticas de segurança e regras de roteamento do projeto PE Conectado que permite o acesso controlado ao serviço.

### Acesso à Aplicação (Firewall da Operação)

Após o Firewall de Borda tratar a requisição, essa é encaminhada ao Firewall Interno da Operação que atua e encaminha ao servidor da aplicação PECONNECTA. Nesse ponto, o tráfego é novamente inspecionado, sendo aplicado as políticas de segurança específicas definidas para o serviço em questão. Após a validação das regras de acesso, o tráfego autorizado é direcionado

## 13. Backup

### 13.1. Infraestrutura

O ambiente PECONNECTA está hospedado em infraestrutura virtualizada, sendo composto por uma máquina virtual, outra responsável pelo banco de dados relacional e, por fim, um servidor responsável pelo banco de dados NoSQL.

A solução de backup é baseada no Veeam Backup & Replication, implantada dentro do ambiente.

Os backups são armazenados em um repositório externo à infraestrutura de virtualização, garantindo isolamento lógico dos dados e maior resiliência contra falhas ou incidentes no ambiente principal.

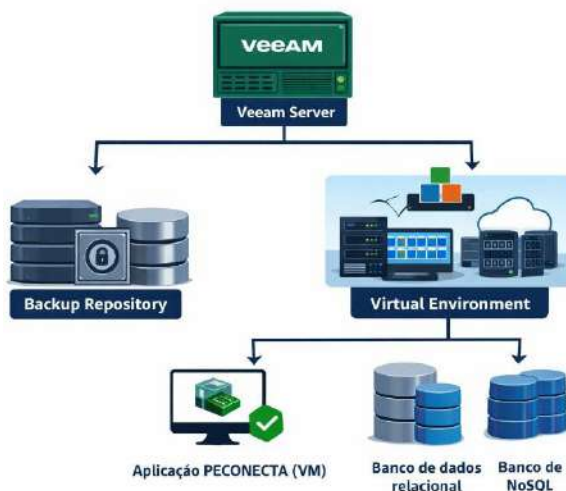
Todos os dados de backup são protegidos por criptografia nativa da solução, assegurando confidencialidade e integridade das informações armazenadas.

O ambiente é composto pelos seguintes elementos:

- Servidor virtual da aplicação PECONNECTA
- Servidor virtual do banco de dados relacional
- Servidor Virtual do banco de dados No SQL
- Servidor de backup com Veeam
- Repositório de backup externo

A comunicação entre os componentes ocorre através da rede interna controlada, respeitando as políticas de segurança e segregação de tráfego da organização.

### 13.2. Diagrama de Topologia do Ambiente de backup



O ambiente de produção do PECONNECTA é composto por camadas distintas de aplicação, banco de dados e backup.

A solução de backup realiza a proteção das máquinas virtuais e do banco de dados através de processamento interno, com envio dos dados para repositório externo, garantindo segregação entre ambiente produtivo e armazenamento de backup.

O diagrama acima ilustra a interação entre os componentes, evidenciando o fluxo de dados entre a aplicação, banco de dados e a infraestrutura de backup.

### 13.3. Agendamento & Retenção de dados

Agendamento

A política de backup do ambiente PECONNECTA foi definida de forma a garantir a proteção contínua dos dados e a possibilidade de recuperação em diferentes pontos no tempo.

#### Backup das Máquinas Virtuais

- Tipo: Incremental diário
- Backup completo(Full): Executado semanalmente aos sábados
- Abrangência: Máquina virtual da aplicação e máquinas virtuais dos bancos de dados
- Retenção
  - A retenção do ambiente é medida em recovery points, todos os backups têm a retenção de 14 restore points.
  - No caso do servidor de banco de dados relacionais, é aplicada a política GFS, onde os backups semanais (sábado) ficam armazenados por 1 mês, os mensais por 1 ano e os anuais por 5 anos.
- Recuperação
  - RPO: 24h
  - RTO: 2h

#### Backup do Banco de Dados Relacional

Para o banco de dados SQL, além do backup em nível de máquina virtual, é utilizada a funcionalidade de backup transacional da solução.

- Backup de logs de transação: Executado a cada 30 minutos
- Objetivo: Minimizar perda de dados em cenários de falha
  - RPO: 30min
  - RTO: 2h

## CONCLUSÃO

O sistema PE Conecta foi desenvolvido seguindo boas práticas de arquitetura de software e padrões consolidados no desenvolvimento de aplicações corporativas, garantindo organização estrutural, segurança e facilidade de manutenção.

A adoção de Clean Architecture e do padrão CQRS proporciona uma separação clara entre responsabilidades da aplicação, permitindo maior controle sobre as regras de negócio e reduzindo o acoplamento entre as camadas do sistema.

A utilização de tecnologias consolidadas, como .NET 6, Angular, SQL Server e MongoDB, contribui para a estabilidade, escalabilidade e confiabilidade da solução, além de facilitar sua integração com outros sistemas institucionais.

O ambiente de execução em Windows Server com IIS garante a hospedagem adequada da aplicação, enquanto os mecanismos de autenticação, controle de acesso e suporte a autenticação multifator contribuem para a segurança das informações e dos processos operacionais do sistema.

As integrações com serviços externos, como a API de Usuários e a API de Relatórios, ampliam as funcionalidades da plataforma e permitem a centralização dos serviços institucionais.

importantes, mantendo o sistema alinhado com a arquitetura tecnológica adotada pela organização.

Por fim, a documentação apresentada neste documento busca registrar de forma estruturada os principais aspectos arquiteturais da solução, servindo como referência para gestão do sistema, suporte técnico, auditorias e futuras evoluções da plataforma.

## ADENDO I - OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE

### 1. OBRIGAÇÕES DA CONTRATADA

#### **1.1. Obrigações aplicáveis a todos os lotes:**

1.1.1. A CONTRATADA obriga-se a executar os serviços na forma e termos reportados neste Termo, especificações técnicas e demais disposições contidas nos seus Adendos e Anexos, bem como, na sua proposta de preço. A CONTRATADA deverá constituir Unidade(s) Gerencial(is) que trate(m) tanto da área Contratual como também da área Técnica, com o objetivo de manter estreita ligação com a CONTRATANTE Principal (Secretaria de Administração - SAD) e a CONTRATANTE aderente Técnica (Agência Estadual de Tecnologia da Informação - ATI), respectivamente, a fim de assegurar a perfeita execução dos serviços contratados.

1.1.2. A CONTRATADA deve, no prazo de até 45 (quarenta e cinco) dias corridos contados a partir da emissão da OS do serviço CIISC, designar formalmente seu(s) representante(s) técnicos e gerenciais, com disponibilidade para atendimento presencial na cidade do Recife, capazes de atender a todas as necessidades administrativas oriundas do contrato, bem como aos assuntos técnicos relacionados à qualidade e quantidade da prestação dos serviços contratados. Além disso, durante toda a vigência do contrato, a CONTRATADA deve disponibilizar, não necessariamente nas dependências da CONTRATANTE Principal, um preposto para atividades técnico-administrativas, devidamente munido das ferramentas necessárias, que atue como interlocutor entre a CONTRATADA e a CONTRATANTE Principal, prestando o suporte necessário para a eficiente execução dos serviços.

1.1.3. A CONTRATADA deve planejar os serviços de forma a não interferir no andamento normal das atividades desenvolvidas no local e em seu entorno.

1.1.4. A CONTRATADA deve responder por todos os ônus e obrigações concernentes às legislações Fiscal, Previdenciária, Trabalhista e Comercial, inclusive os decorrentes de acidentes de trabalho.

1.1.5. A CONTRATADA deve responder financeiramente, sem prejuízo de medidas outras que possam ser adotadas, por quaisquer danos causados à União, Estado, Município ou terceiros, em razão da execução dos serviços.

1.1.6. A CONTRATADA deve manter, durante a prestação dos serviços, seus funcionários e subcontratados devidamente identificados por crachá, sempre que estiverem na execução de suas funções. Deve ainda manter sua equipe técnica sempre provida de veículos, EPI's, ferramental, instrumentos e equipamentos, devidamente aferidos e calibrados, adequados ao trabalho e em perfeitas condições de uso.

1.1.7. A CONTRATADA deve garantir que os prepostos indicados deverão participar da prestação do serviço do objeto contratado, admitindo-se a substituição por profissionais de experiência equivalente ou superior.

1.1.8. A CONTRATADA deve garantir a presença do seu referido preposto nas reuniões gerenciais mensais, realizadas com a CONTRATANTE Principal e com a CONTRATANTE aderente Técnica, para tratar do desempenho e das ocorrências surgidas a cada mês, referentes à Nova Rede Corporativa.

1.1.9. A CONTRATADA deve manter nos locais dos serviços, equipe técnica suficiente, formalmente designada, composta de profissionais habilitados e de capacidade comprovada, com capacidade para assumir perante uma auditoria ou fiscalização a responsabilidade técnica dos mesmos, inclusive com poderes para deliberar sobre qualquer determinação de emergência que se torne necessária.

1.1.10. A CONTRATADA deve manter nos locais dos serviços a serem instalados e/ou operacionalizados, além da equipe técnica retromencionada, auxiliares necessários ao perfeito controle dos padrões exigidos, assim como promover, às suas expensas e segundo as especificações e normas técnicas, o controle tecnológico dos equipamentos e materiais a serem empregados nos serviços.

1.1.11. A CONTRATADA deve facilitar a ação da auditoria a quem competir, atendendo as especificações contidas neste Termo, na inspeção dos serviços, prestando todas as informações e esclarecimentos solicitados, inclusive de ordem administrativa, bem como sobre os documentos relativos ao processo.

1.1.12. A CONTRATADA deve entregar à CONTRATANTE Principal e às CONTRATANTES aderentes, quando da entrega dos serviços por parte da CONTRATADA, o Termo de Recebimento correspondente, registrando todas as alterações e complementações efetuadas, caso houver, no decorrer do prazo contratual, observando, obrigatoriamente, as normas da CONTRATANTE Principal.

1.1.13. A CONTRATADA deve relatar oportunamente à CONTRATANTE Principal e às CONTRATANTES aderentes, ocorrências ou circunstâncias que possam acarretar dificuldades no desenvolvimento dos serviços.

1.1.14. A CONTRATADA deve dar à CONTRATANTE Principal e às CONTRATANTES aderentes, imediata ciência de fatos irregulares que venham a ocorrer durante a execução do Contrato.

1.1.15. A CONTRATADA deve prover os dados necessários para o devido acompanhamento dos processos que se façam necessários durante a execução do objeto desta licitação.

1.1.16. A CONTRATADA deve disponibilizar à CONTRATANTE, através de diversos meios eletrônicos, as informações atualizadas do andamento da execução dos serviços contratados na forma de Relatórios Gerenciais pertinentes, conforme especificados no Termo de Referência.

1.1.17. A CONTRATADA deve responsabilizar-se, em casos fortuitos e força maior, pelos prejuízos causados aos seus equipamentos disponibilizados.

1.1.18. A CONTRATADA deve fornecer os recursos técnicos e humanos, operacionais dentro dos requisitos exigidos neste Termo e seus adendos.

1.1.19. A CONTRATADA deve prover capacidade operacional suficiente para a plena prestação dos serviços de telemática da Nova Rede Corporativa, dentro da sua abrangência.

1.1.20. A CONTRATADA deve arcar com todos os custos relativos aos encargos sociais e obrigações trabalhistas e previdenciárias relativas da equipe empregada na execução dos serviços, bem como, impostos, taxas, emolumentos, seguros ou outros valores que incidam, direta ou indiretamente sobre os serviços ora contratados.

1.1.21. A CONTRATADA deve responder por danos causados à CONTRATANTE, ou a terceiros, decorrentes de falhas ou irregularidades na execução dos serviços.

1.1.22. A CONTRATADA deve manter, durante toda execução do contrato, as mesmas condições de habilitação e qualificação exigidas na licitação.

1.1.23. A CONTRATADA deve facilitar o acompanhamento e fiscalização dos serviços pela CONTRATANTE.

1.1.24. A CONTRATADA é a responsável pelo fornecimento de todos os serviços e recursos especificados nos itens e subitens deste Termo, os quais serão devidamente formalizados a partir de instrumentos contratuais específicos, como Edital e seus Anexos.

1.1.25. A CONTRATADA deve fornecer os recursos técnicos, humanos e operacionais, dentro dos requisitos exigidos neste Termo e seus Adendos.

1.1.26. A CONTRATADA deve atender as Ordens de Serviços emitidas pela CONTRATANTE, dentro dos requisitos e prazos especificados e exigidos neste Termo.

1.1.27. A CONTRATADA deverá realizar a remessa de equipamentos ou componentes, às suas expensas, para a prestação do serviço de manutenção/conserto. Toda e qualquer despesa logística ou operacional será de responsabilidade da CONTRATADA.

1.1.28. A CONTRATADA deve providenciar a substituição temporária e/ou permanente, sem ônus para a CONTRATANTE, de todos os recursos técnicos necessários ao funcionamento da solução do serviço contratado, quando na constatação de uma falha.

1.1.29. A CONTRATADA deve realizar todos as configurações, ajustes, substituições e testes necessários dos recursos da solução adotada, para os serviços contratados da Nova Rede Corporativa, mantendo os mesmos em condições de pleno funcionamento.

1.1.30. A CONTRATADA deve prover, quando solicitado pela CONTRATANTE, laudo técnico identificando a causa da falha na prestação do serviço contratado e, quando for o caso, identificar o uso indevido por parte do usuário.

1.1.31. A CONTRATADA deve manter sempre atualizadas as informações referentes ao funcionamento dos serviços contratados, tais como status, cliente, local, data, hora etc., acessíveis à CONTRATANTE em sistema via Web.

1.1.32. A CONTRATADA deve utilizar ferramentas, equipamentos e recursos adequados, para a realização de análise, diagnóstico e correção de eventuais falhas na prestação dos serviços;

1.1.33. A CONTRATADA deve encaminhar aos CONTRATANTES aderentes, até o quinto dia útil do mês subsequente da efetiva execução dos serviços, as Notas Fiscais/Faturas correspondentes à prestação dos serviços contratados, contendo a descrição detalhada de cada serviço, para os devidos atestados e pagamentos, sendo estas através de Sistema via WEB, com possibilidade de extração no formato de planilha eletrônica, impressas e em meio digital gravadas no formato de arquivo (.txt), conforme modelo elaborado pela FEBRABAN, versão V3R0 ou mais recente, ou, alternativamente, no padrão XML - Nota Fiscal Eletrônica (NF-e), reconhecido nacionalmente para fins de validação fiscal e operacional.

1.1.34. A CONTRATADA deve fornecer ferramentas para controle e gestão de faturas, para o CONTRATANTE aderente, discriminadas e em formato eletrônico de planilha. Os acessos a essa ferramenta devem ser restritos, garantindo que somente cada CONTRATANTE aderente possa recuperar, consultar e manusear os dados do seu Órgão e vinculadas, com exceção da Secretaria de Administração (SAD), que poderá ter os mesmos direitos de acesso para todos os CONTRATANTES aderentes da Administração Pública Estadual.

1.1.35. A CONTRATADA deve responder a contestação, enviando a fatura, que está momentaneamente suspensa, com uma nova data de vencimento, com prazo de no mínimo 20 (vinte) dias, garantindo que os valores divergentes, caso haja, sejam descontados na fatura posterior.

1.1.36. A CONTRATADA deve registrar e atualizar todos os dados do faturamento referente aos serviços prestados, no sistema de informações de faturamento da CONTRATADA, visando e permitindo o acompanhamento por parte do CONTRATANTE aderente.

1.1.37. A CONTRATADA deve ceder à CONTRATANTE, em caráter definitivo, o direito patrimonial das bases de dados, e os respectivos SGBDs (Sistemas Gerenciadores de Banco de Dados), resultantes dos serviços executados durante a vigência do contrato, entendendo-se por resultados quaisquer bases de imagens, áudios, vídeos, estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

1.1.38. A CONTRATADA deve observar o Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014) que fala da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas, da Da Guarda de Registros de Conexão, da Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão, Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações, Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros, Da Requisição Judicial de Registros e da ATUAÇÃO DO PODER PÚBLICO.

1.1.39. A CONTRATADA deve manter processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27002, item 5.12 – Classificação da Informação, processo necessário segundo o Decreto Nº 7.845/2012, Capítulo III, Do Tratamento de Informação Classificada. Esta classificação da informação deve ser acessível à CONTRATANTE.

1.1.40. A CONTRATADA deve manter processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação, item 8.2 - Avaliação do risco

de segurança da informação. Este item fornece diretrizes sobre como identificar, avaliar e tratar riscos relacionados à segurança da informação.

1.1.41. A CONTRATADA deve nomear responsável pela segurança da informação, à semelhança das orientações contidas na ISO/IEC 27002:2022, Controle 5.2 aborda a implementação e gestão de responsabilidades de segurança da informação.

1.1.42. A CONTRATADA deve seguir as políticas de segurança da informação que forem desenvolvidas no item de evolução de maturidade em segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27002 – Política de segurança da informação.

1.1.43. A CONTRATADA deve dar ciência à CONTRATANTE, formal e imediatamente, sobre qualquer anormalidade verificada referente à propriedade, sigilo e segurança das informações durante a prestação dos serviços.

1.1.44. A CONTRATADA deve guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da CONTRATANTE, sendo vedada à sua cessão, locação ou venda a terceiros sem prévia autorização formal da CONTRATANTE Principal.

1.1.45. A CONTRATADA deve zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

1.1.46. A CONTRATADA deve estar cientes de que a estrutura computacional da CONTRATANTE não poderá ser utilizada para fins particulares.

1.1.47. A CONTRATADA deve entregar à CONTRATANTE toda e qualquer documentação produzida decorrente da prestação de serviços, objeto desta licitação, bem como, ceder à CONTRATANTE, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia.

1.1.48. A CONTRATADA deverá disponibilizar à CONTRATANTE, a qualquer tempo, mediante solicitação, de forma imediata ou no prazo máximo definido pela CONTRATANTE, toda e qualquer informação, dado, registro, log, configuração, documentação técnica, inventário, métricas, relatórios, bases de dados e demais elementos relacionados aos serviços contratados e à infraestrutura da Nova Rede Corporativa da CONTRATANTE, independentemente do estado de adimplência contratual, incluindo situações de inadimplemento, suspensão de pagamentos, rescisão ou encerramento contratual;

1.1.48.1. Para fins deste item, todas as informações, dados e registros, ainda que armazenados, processados ou geridos em ambientes, sistemas ou plataformas sob responsabilidade ou domínio da CONTRATADA, serão considerados de propriedade exclusiva da CONTRATANTE, não podendo ser retidos, restringidos, condicionados, indisponibilizados ou utilizados como mecanismo de garantia, pressão ou compensação contratual;

1.1.48.2. Consideram-se abrangidos por esta obrigação quaisquer artefatos informacionais produzidos pela CONTRATADA a partir de dados da CONTRATANTE ou de sua operação, incluindo análises, consolidações, enriquecimentos, correlações, indicadores, inteligência operacional, modelos, scripts, parametrizações e quaisquer outras formas de tratamento ou transformação da informação;

1.1.48.3. A CONTRATADA deverá garantir que tais informações sejam fornecidas em formato aberto, estruturado, legível e passível de reutilização, sem qualquer tipo de bloqueio tecnológico, criptográfico ou dependência de ferramentas proprietárias que impeçam ou dificultem seu acesso e uso pela CONTRATANTE.

1.1.49. A CONTRATADA deve informar à CONTRATANTE sobre qualquer acesso indevido, invasão ou ataque sofrido nos servidores ou serviços onde estejam hospedados cada solução CONTRATADA.

1.1.50. A CONTRATADA deve instalar e operacionalizar todos os serviços referentes ao respectivo Lote, conjuntamente com a CONTRATADA dos serviços ofertados na solução da nova Rede, até a completa finalização da assunção de todos os serviços para Nova Rede Corporativa.

1.1.51. A CONTRATADA, deve fornecer e manter a versão mais recente de todos os componentes (hardware e software) das soluções CONTRATADAS.

1.1.52. A CONTRATADA deve fornecer AS Built com toda documentação técnica completa e original de todos os componentes fornecidos da prestação dos serviços, quando solicitado pela CONTRATANTE, em língua portuguesa, em meio impresso e/ou meio eletrônico. Quaisquer atualizações da documentação devem ser fornecidas, sem ônus para a CONTRATANTE, durante a vigência do contrato.

1.1.53. A CONTRATADA deve realizar a configuração de todos os equipamentos fornecidos nas soluções da Nova Rede Corporativa e a integração ao ambiente atual da nova Rede.

1.1.54. A CONTRATADA deve realizar vistoria no ambiente da CONTRATANTE aderente, quando da instalação de novos serviços, para levantamento de dados do referido ambiente e adequação dos mesmos, conforme exigências deste Termo.

1.1.55. São de responsabilidade da CONTRATADA os custos referentes à energia elétrica para o funcionamento das soluções que eventualmente envolvam serviços instalados em via pública.

1.1.56. A CONTRATADA deve manter os técnicos encarregados dos serviços de manutenção e assistência técnica previamente relacionados, para ter livre acesso aos recursos inerentes à prestação dos serviços da Nova Rede Corporativa, a fim de executar os serviços de manutenção, respeitando as normas de segurança vigentes e as da CONTRATANTE aderente.

1.1.57. A CONTRATADA deve entregar lista dos profissionais, juntamente com as cópias de suas identidades funcionais, com foto, aos gestores de cada CONTRATANTE aderente, de modo que sejam devidamente cadastrados para acesso às suas dependências. Esta lista deverá ser atualizada e redistribuída sempre que houver alteração no quadro funcional da CONTRATADA.

1.1.58. A CONTRATADA deve fornecer relatórios específicos para cada CONTRATANTE, contendo as informações relativas aos serviços contratado, de acordo com as especificações deste Termo.

1.1.59. A CONTRATADA será a responsável pelo fornecimento de todos os serviços e recursos especificados nos itens e subitens deste Termo, o qual será devidamente, formalizado a partir de instrumentos contratuais específicos, conforme Edital e seus anexos.

1.1.60. A CONTRATADA deve atender obrigatoriamente a todos os requisitos, prazos e especificações técnicas, para prestação dos serviços da Nova Rede Corporativa.

1.1.61. As obrigações acima listadas não excluem outras eventualmente listadas no Termo.

## **1.2. Obrigações aplicáveis ao LOTE 01:**

1.2.1. A CONTRATADA deve substituir qualquer integrante da equipe técnica, caso esteja alocado nas instalações da CONTRATANTE, durante a execução dos serviços, somente após a anuência da CONTRATANTE Principal e das CONTRATANTES aderentes, mediante a comprovação de experiência equivalente ou superior do substituto proposto.

1.2.2. A CONTRATADA deve cumprir os prazos e condições contidos no item de Plano de Assunção dos serviços em operação conforme item e subitens correspondentes no Termo.

1.2.3. A CONTRATADA deve apresentar todas as Notas Fiscais de remessa dos equipamentos de Telemática providos para a prestação de todos os serviços da Nova Rede Corporativa, no momento da entrega e aceite, pelos gestores, desses serviços, onde todas as referidas NF de remessa, acima citadas.

1.2.4. A CONTRATADA deve manter processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27002, item 7.1 – Inventário de ativos. A base com estas informações deve ser acessível à CONTRATANTE.

1.2.5. Obrigações Relacionadas a Implementação das Soluções e Suporte junto com os Fabricantes:

1.2.5.1. Suporte Diferenciado do Fabricante para as soluções abaixo mencionadas:

1.2.5.1.1. Solução unificada de segurança de rede;

1.2.5.1.2. Serviço de rede sem fio com segurança (interno, externo e temporário);

1.2.5.1.3. Solução para gerenciamento de acessos à rede;

1.2.5.1.4. Solução de proteção, detecção e resposta para servidores;

1.2.5.1.5. Solução de segurança de confiança zero;

1.2.5.1.6. Solução de proteção, detecção e resposta para dispositivos de tráfego de rede;

1.2.5.1.7. Solução de segurança de identidade privilegiada;

1.2.5.1.8. Solução de filtro de mensagens indesejadas;

1.2.5.1.9. Solução de filtro de aplicações WEB;

1.2.5.1.10. Solução de monitoramento e análise de eventos de segurança;

1.2.5.1.11. Solução de automação de resposta a incidentes de segurança;

1.2.5.1.12. Solução para guarda de LOGs.

1.2.5.2. A CONTRATADA deverá garantir que todas as soluções fornecidas possuam contrato ativo de suporte técnico junto ao fabricante, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), em nível corporativo (enterprise ou equivalente), contemplando, no mínimo:

1.2.5.2.1. Abertura ilimitada de chamados técnicos junto ao fabricante;

1.2.5.2.2. Atendimento em regime ininterrupto (24x7);

1.2.5.2.3. Suporte para diagnóstico, troubleshooting, correção de falhas e orientação técnica especializada;

1.2.5.2.4. Acesso a atualizações, patches, correções de segurança e upgrades de software/firmware;

1.2.5.2.5. Escalonamento para níveis avançados de suporte do fabricante, conforme severidade e criticidade do incidente;

1.2.5.2.6. A CONTRATADA será responsável por registrar, acompanhar, gerenciar e realizar o devido escalonamento dos chamados técnicos junto aos fabricantes;

1.2.5.2.7. Para incidentes críticos, a CONTRATADA deverá disponibilizar relatórios de análise de causa raiz (Root Cause Analysis – RCA), elaborados com base nas informações técnicas disponíveis, incluindo, sempre que aplicável, análise e contribuições do fabricante, contendo, no mínimo:

1.2.5.2.7.1. identificação da causa do incidente;

1.2.5.2.7.2. ações corretivas adotadas;

1.2.5.2.7.3. recomendações para prevenção de recorrência.

1.2.5.2.8. A CONTRATADA deverá garantir comunicação contínua com os fabricantes, assegurando a coleta e a pronta disponibilização à CONTRATANTE de boletins técnicos, notificações de vulnerabilidades, atualizações críticas e demais informações relevantes que possam impactar a segurança, estabilidade ou desempenho das soluções;

1.2.5.2.9. A CONTRATADA deverá garantir que todas as atualizações de software e firmware sejam precedidas de análise técnica quanto ao impacto no ambiente;

1.2.5.2.10. Sempre que demandado pela CONTRATANTE, a CONTRATADA deverá viabilizar a participação do fabricante em reuniões técnicas para apoio na análise de incidentes, esclarecimentos técnicos ou evolução da solução;

1.2.5.2.11. A CONTRATADA deverá assegurar o alinhamento técnico entre CONTRATANTE, CONTRATADA e fabricante para definição do High Level Design (HLD) e implantação da arquitetura, contemplando requisitos de rede, segurança, alta disponibilidade e aderência às melhores práticas;

1.2.5.2.12. A CONTRATADA deverá acionar o suporte especializado do fabricante, inclusive com atuação hands-on, sempre que necessário, durante a fase de implantação ou operação, garantindo a correta configuração e aderência às boas práticas e aos requisitos do projeto.

1.2.6. A CONTRATADA será responsável por toda a infraestrutura interna (física e elétrica) necessária ao PCS, restrita à infraestrutura para a implantação e operação do serviço contratado/solução adotada.

1.2.6.1. A CONTRATADA deve projetar, instalar, manter e atualizar toda a infraestrutura física interna do PCS (endereço/site) necessária para instalar e operar os equipamentos do projeto que atenderão ao serviço contratado. Todas as instalações devem seguir rigorosamente as normas e padrões técnicos aplicáveis, garantindo segurança, confiabilidade e desempenho da rede. As responsabilidades da CONTRATADA incluem assegurar a conformidade com os requisitos estabelecidos para a infraestrutura física, conforme detalhado a seguir:

1.2.6.1.1. Rede Interna (LAN): Fornecimento e organização do cabeamento estruturado, utilizando par trançado Cat 6A ou superior e fibra óptica, conforme a necessidade técnica. O cabeamento deverá suportar conexões de 2,5 Gbps e 10 Gbps, incluindo backhaul da rede sem fio, garantindo compatibilidade por meio de conversores de mídia quando necessário. A infraestrutura deverá incluir patch panels, racks, organizadores de cabos, tampas cegas e demais acessórios seguindo as normas ANSI/TIA-568.2-D e ISO/IEC 11801.

1.2.6.1.2. Conversores de Mídia: A CONTRATADA será responsável pelo fornecimento, instalação e configuração de conversores de mídia sempre que necessário para garantir a integração entre os diferentes meios físicos da infraestrutura de conectividade e da rede sem fio. Os conversores deverão ser compatíveis com interfaces de fibra óptica (monomodo e multimodo) e cabeamento em par trançado (Cat 6A ou superior), suportando velocidades de 2,5 Gbps e 10 Gbps, conforme a necessidade do ambiente. Deverão atender aos padrões IEEE 802.3bz (2,5GBASE-T), IEEE 802.3an (10GBASE-T) e IEEE 802.3ae (10GBASE-SR/LR).

1.2.6.1.3. Conexões e Conectores: Fornecer e instalar conectores RJ45 de alta qualidade, adaptadores ópticos adequados e, quando necessário, módulos ópticos (GBICs/SFP/SFP+/XFP) compatíveis com os equipamentos utilizados na solução. Os módulos fornecidos deverão atender às especificações de velocidade e tipo de fibra exigidos para cada ambiente, incluindo padrões como LC, SC e MPO, conforme necessidade, seguindo as Normas/Padrões: ISO/IEC 11801, ANSI/TIA-568.2-D, IEC 61754.

1.2.6.1.4. Calhas e Canaletas: Para acomodação segura dos cabos, evitando interferências e danos físicos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

1.2.6.1.5. Organizadores de Cabos: Utilização de organizadores de cabos para evitar emaranhados e facilitar a manutenção. Conforme Normas/Padrões: ANSI/TIA-568.2-D.

1.2.6.1.6. Racks e Gabinetes: Racks apropriados para montagem e organização dos equipamentos de rede. Conforme Normas/Padrões: EIA-310-D, IEC 60297.

1.2.6.1.7. Etiquetagem e Documentação: Todos os cabos, conexões e equipamentos devem ser devidamente etiquetados e documentados. Conforme Normas/Padrões: ANSI/TIA-606-C (Administration Standard for Telecommunications Infrastructure).

1.2.6.1.8. Patch Panels: Utilização de patch panels para a terminação de cabos de rede, permitindo fácil gerenciamento e organização das conexões. Conforme Normas/Padrões: ANSI/TIA-568.2-D.

1.2.6.1.9. Testes e Certificações de Cabos: Realização de testes e certificações de todos os cabos instalados para garantir a conformidade com os padrões de desempenho especificados. Conforme Normas/Padrões: ANSI/TIA-1152-A (Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling).

1.2.6.2. A CONTRATADA é responsável pela infraestrutura elétrica necessária para instalar todos os aparelhos e equipamentos do projeto que atenderão ao serviço contratado, devendo projetar, implementar e manter essa infraestrutura de forma a assegurar a segurança e eficiência energética. As instalações elétricas devem seguir as normas e padrões técnicos estabelecidos, garantindo a qualidade e conformidade do serviço. As responsabilidades da CONTRATADA para a infraestrutura elétrica são detalhadas a seguir:

1.2.6.2.1. Tomadas: Instalação de tomadas adequadas para todos os aparelhos e equipamentos, com número suficiente para evitar sobrecarga. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

1.2.6.2.2. Aterramento: Sistema de aterramento adequado para proteger os equipamentos contra surtos e descargas elétricas. Conforme Normas/Padrões: NBR 5419 (Proteção contra Descargas Atmosféricas).

1.2.6.2.3. Estabilizadores: Estabilizadores de tensão para garantir a alimentação elétrica estável dos equipamentos de rede. Conforme Normas/Padrões: IEC 62040 (Uninterruptible power systems – UPS).

1.2.6.2.4. No-Breaks (UPS): Sistemas de alimentação ininterrupta para garantir a continuidade do serviço em caso de falha de energia, com autonomia mínima de 15 minutos. Conforme Normas/Padrões: IEC 62040 (Uninterruptible power systems – UPS).

1.2.6.2.5. Cabos Elétricos: Utilização de cabos elétricos de qualidade, dimensionados corretamente para suportar a carga dos equipamentos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

1.2.6.2.6. Quadro de Distribuição: Instalação de quadros de distribuição elétrica para organizar e proteger os circuitos elétricos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

1.2.6.2.7. Disjuntores: Utilização de disjuntores adequados para proteção contra sobrecorrente e curto-circuito. Conforme Normas/Padrões: NBR 5361 (Disjuntores).

1.2.6.2.8. Proteção contra Interferências Eletromagnéticas (EMI): Adoção de medidas para minimizar as interferências eletromagnéticas que podem afetar o desempenho da rede. Conforme Normas/Padrões: IEC 61000 (Electromagnetic Compatibility).

1.2.6.2.9. Isolamento e Proteção de Cabos: Uso de materiais isolantes e proteções adequadas para os cabos elétricos, evitando danos e riscos de curto-circuito. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 60332 (Testes de cabos elétricos).

1.2.6.2.10. Proteção contra Desbalanceamento de Cargas: Implementação de medidas para prevenir e corrigir desbalanceamento entre fase-terra-neutro e outros problemas elétricos que podem impactar no bom funcionamento dos equipamentos. A responsabilidade pela correção de quaisquer problemas detectados, tanto na instalação quanto na manutenção, será da CONTRATADA, devendo seguir Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 61000-4-30 (Compatibilidade Eletromagnética - Parte 4-30: Técnicas de Medição de Qualidade da Energia Elétrica).

1.2.6.2.11. Manutenção Preventiva e Corretiva: Realização de manutenção preventiva e corretiva de toda a infraestrutura elétrica para garantir a continuidade e segurança dos serviços. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

1.2.6.2.12. Filtros de Linha com Tomadas Adicionais: Permissão para o uso de filtros de linha com tomadas adicionais, desde que dimensionados para não ocasionar sobrecargas. Estes devem seguir as normas de segurança específicas para garantir que não causem incidentes. Conforme Normas/Padrões: NBR 14136 (Plugues e Tomadas para Uso Doméstico e Similar), NBR 13571 (Fios e Cabos Elétricos).

1.2.6.2.13. Prevenção e correção contra fuga de corrente (baixa isolamento, folgas em bornes, cabos e conectores etc.), mau aterramento etc.): Adoção de medidas para garantir a melhor proteção dos cabos e componentes elétricos, prevenindo riscos de curto-circuito e falhas na rede. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 60228 (Conductors of Insulated Cables).

1.2.6.3. A CONTRATADA poderá utilizar a infraestrutura elétrica e física interna preexistente, desde que esta atenda integralmente aos requisitos de qualidade e normas aplicáveis. Neste caso, a CONTRATADA assumirá a responsabilidade pela manutenção preventiva e corretiva da infraestrutura utilizada.

1.2.7. A CONTRATADA é responsável pelo fornecimento de um kit mínimo infraestrutura que garanta o perfeito funcionamento de todos os equipamentos da solução ofertada, assegurando a qualidade de entrega do serviço. O kit mínimo de ativação deve incluir:

1.2.7.1. Rack para armazenamento de todos equipamentos e elementos elétricos de proteção (filtro de linha, no-break e estabilizador).

1.2.7.2. Infraestrutura elétrica completa, incluindo tomadas e proteções elétricas adequadas.

1.2.7.3. No-break obrigatório para todos os PCs.

1.2.7.4. Materiais elétricos e de rede interna necessários para instalação e operação dos equipamentos.

1.2.8. Disposições Específicas para Serviços de Natureza Temporária

1.2.8.1. Considerando as características operacionais específicas de determinados serviços temporários contratados no âmbito da Nova Rede Corporativa do Estado de Pernambuco, aplicam-se as condições excepcionais previstas neste item às seguintes modalidades:

- Serviço de Rede Sem Fio Temporário com Segurança, conforme previsto no ADENDO IV – SERVIÇO DE REDE SEM FIO;
- Link de Acesso Temporário (LAT) – Tipo 1, Tipo 2 e Tipo 3, conforme previsto no ADENDO V – SERVIÇO DE CONECTIVIDADE DE REDE LOCAL.

1.2.8.2. Para os serviços elencados no subitem anterior, o faturamento mínimo será sempre correspondente a 30 (trinta) dias corridos, ainda que o período efetivo de utilização seja inferior, como em casos de eventos pontuais, ações emergenciais ou projetos de curta duração.

1.2.8.3. Para viabilizar agilidade na ativação e economicidade nas execuções temporárias, fica autorizada a utilização de equipamentos com uso prévio, desde que:

- Estejam em perfeito estado de funcionamento;
- Sejam livres de danos aparentes;
- Estejam atualizados com as versões mais recentes de firmware ou software do fabricante;
- Atendam integralmente às exigências técnicas, funcionais e de segurança dispostas no Termo de Referência e nos respectivos Adendos vinculados aos serviços.

1.2.8.4. A exceção prevista no item 9.3 abrange também os equipamentos e soluções integrantes da Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 ou Tipo 2, conforme especificado no ADENDO III – SEGURANÇA DE REDE LOCAL, quando estes forem utilizados em conjunto com os serviços temporários listados no item 9.1. Nestes casos, o faturamento da UTM seguirá as mesmas condições do serviço temporário associado, com faturamento mínimo de 30 (trinta) dias corridos e limitado ao período de utilização do respectivo serviço temporário.

1.2.8.5. Os serviços de natureza temporária citados neste item, bem como as respectivas soluções de segurança associadas conforme disposto no item 9.4, não estarão sujeitos à carência mínima de 6 (seis) meses prevista no Termo de Referência para os demais serviços. Para estes casos, a carência mínima será de 30 (trinta) dias corridos, contados a partir da ativação do serviço.

1.2.9. O faturamento dos serviços será permitido exclusivamente para os itens previstos na Tabela de Preços constante do Termo de Referência, vedando-se qualquer cobrança adicional por atividades acessórias ou operacionais.

1.2.10. A execução dessas atividades deverá ocorrer de forma organizada e sem impacto na continuidade dos serviços prestados pela CONTRATANTE, respeitando as normas e boas práticas aplicáveis. A CONTRATADA deverá planejar, documentar e comunicar previamente quaisquer intervenções, garantindo total transparência e alinhamento com os gestores responsáveis.

1.2.11. O descumprimento dos prazos ou a não realização das atividades conforme as especificações poderá resultar em glosas, penalidades contratuais e demais sanções cabíveis, conforme previsto no Termo de Referência e na regulamentação vigente.

1.2.12. A CONTRATADA deverá implementar, manter, operar e evidenciar a execução dos processos e controles descritos a seguir, em conformidade com as melhores práticas de gestão de serviços de TI, alinhadas à ISO/IEC 20000-1:2018 ou versão superior aplicável, assegurando sua efetividade, mensurabilidade, rastreabilidade e aderência contínua. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

1.2.12.1. Implementação e manutenção de um Sistema de Gestão de Serviços (SGS) formalmente documentado, com escopo definido, controle de versões e mecanismo de melhoria contínua;

1.2.12.2. Estabelecimento, aprovação e divulgação de política de gestão de serviços, alinhada aos objetivos institucionais da CONTRATANTE;

1.2.12.3. Definição formal de papéis, responsabilidades e autoridades, incluindo proprietários de processos e responsáveis por controles;

1.2.12.4. Manutenção de catálogo de serviços atualizado, contendo descrição, escopo, requisitos, dependências, níveis de serviço e público-alvo;

1.2.12.5. Processo estruturado para planejamento, transição, validação e entrada em operação de novos serviços ou alterações;

1.2.12.6. Elaboração, testes periódicos e manutenção de planos de continuidade e recuperação de serviços de TI críticos;

1.2.12.7. Procedimentos formalizados para resposta a incidentes graves e desastres, incluindo tempos de recuperação (RTO) e ponto de recuperação (RPO);

1.2.12.8. Processo de gerenciamento de incidentes com registro, categorização, priorização, escalonamento, resolução e encerramento formal;

1.2.12.9. Processo de gerenciamento de requisições de serviço com definição de critérios de priorização, prazos e fluxo de atendimento;

1.2.12.10. Processo de gerenciamento de problemas com identificação de causa raiz, base de erros conhecidos e ações de mitigação;

1.2.12.11. Processo de habilitação de mudanças com avaliação de risco, aprovação formal, plano de rollback e revisão pós-implementação;

1.2.12.12. Gerenciamento de implantações com controle de versões, testes, validação e autorização prévia para entrada em produção;

1.2.12.13. Gerenciamento de configuração e ativos de serviço, com inventário atualizado, controle de itens de configuração (CIs) e mapeamento de dependências;

1.2.12.14. Processo de gerenciamento de acesso, com concessão, revisão periódica e revogação de acessos baseada em perfis e segregação de funções;

1.2.12.15. Monitoramento contínuo de serviços, infraestrutura e processos, com geração de alertas e tratamento proativo de eventos;

1.2.12.16. Definição, apuração e reporte de indicadores de desempenho (KPIs) e níveis de serviço (SLAs), com análise crítica periódica;

1.2.12.17. Processo estruturado de comunicação com a CONTRATANTE, incluindo tratamento de reclamações, solicitações e feedbacks;

- 1.2.12.18. Planejamento e execução de auditorias internas periódicas do SGS, com registro de evidências e planos de ação;
- 1.2.12.19. Processo de tratamento de não conformidades, com ações corretivas e preventivas, análise de causa e acompanhamento de eficácia;
- 1.2.12.20. Programa contínuo de capacitação, com trilhas de treinamento, avaliação de eficácia e registro formal;
- 1.2.12.21. Processo de gestão de fornecedores envolvidos na prestação do serviço, incluindo avaliação de desempenho e conformidade;
- 1.2.12.22. Gestão de riscos aplicada ao SGS, com identificação, análise, tratamento e monitoramento contínuo dos riscos;
- 1.2.12.23. Controle documental e de registros do SGS, garantindo integridade, confidencialidade, disponibilidade e versionamento;
- 1.2.12.24. Todos os processos e controles deverão ser suportados pela ferramenta de ITSM, garantindo rastreabilidade ponta a ponta;
- 1.2.12.25. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados.
- 1.2.13. A CONTRATADA deverá fornecer documentação técnica completa, atualizada e rastreável, de forma progressiva, ao término de cada fase, entrega técnica ou ativação relevante, bem como na implantação integral do objeto, incluindo obrigatoriamente documentação do tipo AS BUILT, refletindo fielmente a configuração efetivamente implantada.
- 1.2.13.1. A documentação AS BUILT deverá contemplar, no mínimo, quando aplicável ao serviço entregue:
- 1.2.13..1.1. Diagramas lógicos e físicos atualizados da rede;
- 1.2.13.1.2. Topologia detalhada (LAN, WAN, WLAN, backbone, interligações, redundâncias);
- 1.2.13.1.3. Endereçamento IP, VLANs, rotas e políticas de roteamento;
- 1.2.13.1.4. Configurações de equipamentos ativos (switches, roteadores, firewalls, controladoras, etc.);
- 1.2.13.1.5. Políticas implementadas (ACLs, regras de firewall, segmentações, QoS, etc.);
- 1.2.13.1.6. Inventário completo de ativos instalados, com modelo, número de série, firmware/versão e localização física;
- 1.2.13.1.7. Mapeamento de portas físicas e lógicas;
- 1.2.13.1.8. Documentação de integrações com sistemas externos;
- 1.2.13..1.9. Registro de parametrizações específicas realizadas;
- 1.2.13.1.10. Relação de licenças instaladas e respectivas vigências;
- 1.2.13.1.11. Registro de eventuais customizações técnicas executadas;
- 1.2.13.1.12. A documentação prevista no ADENDO XV para encerramento e consolidação documental.
- 1.2.13.2. A documentação relativa a cada ativação/fase/entrega deverá ser disponibilizada em até 15 (quinze) dias corridos após o respectivo aceite/homologação pela CONTRATANTE, ou conforme marco equivalente definido no Plano do Projeto, podendo a CONTRATANTE sustar o pagamento da respectiva entrega ou fase até a regularização da documentação.
- 1.2.13.3. A documentação final consolidada (AS BUILT completo e inventário final), correspondente ao encerramento do Plano de Assunção, deverá ser entregue em até 30 (trinta) dias corridos após a conclusão formal da assunção, sem

prejuízo das entregas progressivas, podendo a CONTRATANTE sustar o pagamento da respectiva entrega até a regularização da documentação.

1.2.13.4. Toda a documentação deverá ser entregue em língua portuguesa, em formato digital aberto e editável, com versionamento e histórico de alterações, e atualizada sempre que houver modificação relevante na infraestrutura.

1.2.13.5. A documentação técnica entregue pela CONTRATADA poderá ser submetida à verificação técnica pela CONTRATANTE, com o objetivo de validar sua aderência à infraestrutura efetivamente implantada.

1.2.13.5.1. Caso sejam identificadas inconsistências, omissões ou divergências em relação ao ambiente operacional, a CONTRATADA deverá realizar as correções necessárias no prazo máximo de 10 (dez) dias corridos, sem ônus adicional para a CONTRATANTE.

1.2.13.6. A ausência ou inconsistência da documentação técnica poderá caracterizar inexecução parcial da entrega, sujeitando a CONTRATADA às medidas administrativas cabíveis, conforme previsto neste Termo de Referência e no instrumento contratual.

1.2.14. A CONTRATADA será integralmente responsável pelo fornecimento, emissão, renovação, revogação, instalação, configuração e gestão de todos os certificados digitais necessários ao pleno funcionamento da Nova Rede Corporativa, independentemente da tecnologia, módulo ou componente envolvido (incluindo, mas não se limitando a UTM, NAC, ZTNA, WAF, VPN, portais web, APIs, integrações e demais serviços deste Termo de Referência e seus adendos);

1.2.14.1 Os certificados deverão:

1.2.14.1.1. Ser válidos e emitidos por Autoridades Certificadoras confiáveis (públicas ou privadas), conforme o caso de uso;

1.2.14.1.2. Atender aos requisitos de segurança vigentes, incluindo uso de algoritmos e tamanhos de chave aderentes às boas práticas de mercado;

1.2.14.1.3. Garantir suporte a criptografia forte, vedado o uso de protocolos e cifras obsoletas ou consideradas inseguras;

1.2.14.1.4. Ser providos sem ônus adicional à CONTRATANTE, inclusive quanto a licenciamento, cadeia de certificação e renovações durante toda a vigência contratual;

1.2.14.1.5. Permitir sua utilização para todos os cenários da Nova Rede Corporativa, incluindo autenticação de usuários, dispositivos, serviços, inspeção de tráfego criptografado, publicação segura de aplicações e estabelecimento de túneis criptográficos;

1.2.14.1.6. Possibilitar revogação imediata em caso de comprometimento, bem como rotação periódica conforme políticas de segurança;

1.2.14.1.7. Ser plenamente compatíveis com navegadores seguros amplamente utilizados no mercado, bem como com os sistemas operacionais já especificados ao longo deste Termo de Referência e seus respectivos adendos, e com as integrações corporativas utilizadas pela CONTRATANTE;

1.2.14.2. A CONTRATADA deverá garantir que não haja interrupção de serviço decorrente de expiração, má configuração ou ausência de certificados digitais, sendo responsável pela gestão proativa de seu ciclo de vida.

1.2.15. Gestão de Ciclo de Vida, Suporte e Licenciamento dos Equipamentos e Soluções:

1.2.15.1. A CONTRATADA deverá garantir que todos os equipamentos, sistemas, softwares, firmwares, licenças e componentes das soluções fornecidas e operadas no âmbito do LOTE 01 permaneçam, durante toda a vigência contratual, dentro de seu ciclo de vida suportado pelo fabricante, observando rigorosamente as políticas oficiais de End of Life (EoL), End of Support (EoS), End of Service Life (EoSL), End of Sale (EoSale) ou equivalentes;

1.2.15.2. A CONTRATADA deverá realizar o acompanhamento contínuo do ciclo de vida dos ativos, mantendo controle atualizado sobre datas de fim de comercialização, datas de fim de suporte técnico, datas de fim de atualizações de segurança, situação de licenciamento, subscrição e contratos de suporte;

1.2.15.3. Não será admitida, em nenhuma hipótese, a operação de equipamentos ou soluções que:

1.2.15.3.1. Estejam fora do período de suporte do fabricante;

1.2.15.3.2. Não recebam atualizações de segurança;

1.2.15.3.3. Possuam licenças expiradas, suspensas ou em desacordo com os termos contratuais ou do fabricante.

1.2.15.4. A CONTRATADA deverá planejar e executar a substituição, atualização ou migração de quaisquer equipamentos, softwares ou soluções que se aproximem ou atinjam o fim de seu ciclo de vida suportado, de forma proativa, garantindo continuidade dos serviços, manutenção dos níveis mínimos de serviço e preservação da segurança da informação, desempenho e estabilidade do ambiente;

1.2.15.5. A CONTRATADA deverá comunicar formalmente à CONTRATANTE, com antecedência mínima de 6 (seis) meses, a ocorrência de eventos de fim de ciclo de vida (EoL/EoS), apresentando:

1.2.15.5.1. Análise de impacto técnico e operacional;

1.2.15.5.2. Plano de substituição ou atualização;

1.2.15.5.3. Cronograma de execução;

1.2.15.5.4. Garantia de compatibilidade com o ambiente existente.

1.2.15.6. Todos os custos relacionados à manutenção de licenciamento, renovações, atualizações, substituições ou migrações necessárias para manter os ativos dentro de seu ciclo de vida suportado serão de responsabilidade exclusiva da CONTRATADA, não cabendo qualquer ônus adicional à CONTRATANTE;

1.2.15.7. A CONTRATADA deverá manter evidências documentais auditáveis relativas ao ciclo de vida, licenciamento e suporte dos ativos, podendo tais informações ser solicitadas a qualquer tempo pela CONTRATANTE ou por órgãos de controle e fiscalização.

### **1.3. Obrigações aplicáveis ao LOTE 01 e LOTE 02:**

1.3.1. A CONTRATADA deve executar todos os serviços e instalações de acordo com as especificações e demais equipamentos técnicos que integram este Edital, obedecendo rigorosamente às Normas Técnicas da ABNT e das concessionárias de serviços públicos, e as especificações técnicas contidas em todos os adendos/anexos deste termo.

1.3.2. A CONTRATADA será responsável por realizar, sem ônus para a CONTRATANTE, todas as instalações, mudanças de endereço, mudanças internas, solicitações de serviço, upgrades, ampliações, emissões de relatórios e configurações dos itens contratados, garantindo a execução dentro dos prazos estabelecidos no Termo de Referência e seus Adendos.

1.3.3. A CONTRATADA deve executar o controle tecnológico de materiais, componentes e sistemas construtivos (ensaios laboratoriais) para evidenciar o atendimento às Normas Técnicas da ABNT e dos CONTRATANTES ou das concessionárias de serviços.

1.3.4. A CONTRATADA deve executar, às suas expensas, as ligações definitivas das instalações às redes públicas conforme especificado neste Termo.

1.3.5. A CONTRATADA deve entregar, na mais perfeita ordem e limpeza, as instalações, após a execução do objeto do presente Instrumento, deixando o local totalmente limpo em condições de normais de operações técnicas.

1.3.6. A CONTRATADA deve responsabilizar-se pelo armazenamento e guarda de todos os equipamentos e demais recursos tecnológicos, como cabos, calhas, conectores etc. e ferramentas a serem utilizados na execução da implantação do objeto contratado.

1.3.7. A CONTRATADA deve, em momento definido pela CONTRATANTE Principal, fornecer todos os recursos necessários (equipamentos, pessoal, soluções de telemática etc.) para permitir a migração dos serviços até o momento prestado, para o próximo fornecedor do serviço vencedor da licitação seguinte. De tal forma que possibilite realizar tal transição com os menores impactos possíveis aos CONTRATANTES, garantindo os princípios da continuidade do serviço público. Tal procedimento de transição deverá ser estabelecido e acordado entre a CONTRATANTE, a CONTRATADA atual e a futura. Tal atividade não deverá ter ônus adicionais para a CONTRATANTE.

1.3.8. A CONTRATADA deve prover a gestão de manutenção preventiva e corretiva, no seu próprio ambiente, respeitando os limites estabelecidos dos Níveis Mínimos de Serviços (NMS), definidos neste Termo.

1.3.9. A CONTRATADA deve realizar a manutenção preventiva (diagnóstico padrão, limpeza, verificação de cabos e conectores etc.) dos recursos de telemática, dos serviços da Nova Rede Corporativa, visando, proativamente, mantê-los em pleno funcionamento.

1.3.10. A CONTRATADA deve prover assistência técnica de forma permanente, durante a vigência contratual, evitando gastos adicionais com peças de reposição e manutenção dos equipamentos, isto é, caso ocorra alguma falha, a CONTRATADA garante a substituição do equipamento por um equivalente ou superior, atendendo aos prazos requeridos no nível mínimo de serviço.

1.3.11. A CONTRATADA, deve adotar o Protocolo IPv6 em toda Nova Rede Corporativa, sendo de sua responsabilidade a implantação, configuração, manutenção e gestão de uso de todos os endereços IPv6. Garantir a coexistência, bem como, a interoperabilidade entre IPv6 e IPv4 nos equipamentos conectados nesta Rede e os produtos que suportam ambos os protocolos, mantendo as conexões entre eles, não devendo isolar redes por versão de protocolo IP.

1.3.12. A CONTRATADA deve considerar os conceitos relacionados neste Termo, no que tange a logística de preparação, entrega, instalação, configuração, manutenção preventiva e corretiva dos recursos da solução adotada, na prestação dos serviços contratados da Nova Rede Corporativa.

1.3.13. A CONTRATADA, deve prover e manter os recursos e serviços, a serem operacionalizados para Nova Rede Corporativa em todos os seus endereços contratados;

1.3.14. A CONTRATADA deve disponibilizar, para acesso dos CONTRATANTES aderentes, sistema de gestão da manutenção em plataforma web, fornecendo informações acerca dos itens contratados, seus status, bem como os relatórios de atendimento.

1.3.15. A CONTRATADA deve apresentar à CONTRATANTE aderente, um número de controle para cada atendimento preventivo ou corretivo.

1.3.16. A CONTRATADA deve disponibilizar telefone e endereço eletrônico de atendimento para abertura de chamados, visando o atendimento das demandas no período citado neste Termo.

1.3.17. A CONTRATADA deve garantir que toda a interação com relação a abertura de chamados, manutenção programada e registro de ocorrências, deve ser realizada através do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), para ter um único ponto de Gestão de Demandas e Registro de Ocorrências;

1.3.18. A CONTRATADA deve encaminhar um técnico para prestação de suporte local (on site), quando houver falha(s) na prestação do(s) serviço(s), sem custos adicionais, caso o atendimento remoto não seja efetivo na resolução dos chamados.

1.3.19. A CONTRATADA deve disponibilizar, nos diversos meios de comunicação (help-desk, sistema de acompanhamento de chamados etc.) informações ao CONTRATANTE sobre a situação de atendimento do chamado técnico, o diagnóstico, as providências adotadas e/ou implementadas e a data e hora da solução do incidente.

1.3.20. Infraestrutura de cabos em postes ou equivalente para os Lotes 1 e 2  
1.3.20.1 Declaração e protocolo:

1.3.20.1.1 Até a assinatura do contrato, as Licitantes provisoriamente classificadas vencedoras deverão apresentar:  
1.3.20.1.1.1 Para o Lote 1, apresentar declaração de intenção de ocupação de postes (ou uso de rede subterrânea/própria) nos 14 municípios listados abaixo:

- Arcoverde
- Cabo de Santo Agostinho
- Caruaru
- Garanhuns
- Jaboatão dos Guararapes
- Olinda

- Palmares
- Paulista
- Pesqueira
- Recife
- Salgueiro
- Serra Talhada
- Petrolina
- Vitória de Santo Antão

1.3.20.1.1.2 Para o Lote 2, apresentar declaração de intenção de ocupação de postes (ou uso de rede subterrânea/própria) no município de Recife.

1.3.20.1.1.3 Comprovante de protocolo do pedido de viabilidade técnica junto à distribuidora de energia ou à operadora parceira.

1.3.20.2 Contratos definitivos / autorizações

1.3.20.2.1 A CONTRATADA deverá entregar o contrato de compartilhamento de postes, documento de posse de postes próprios ou autorização formal de terceiro titular da infraestrutura nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.2.1.1 Para a RMR, 90 (noventa) dias;

1.3.20.2.1.2 Para os demais municípios, 150 (cento e cinquenta) dias.

1.3.20.2.1.3 Para o Lote 2, 30 (trinta) dias

1.3.20.3 Vistoria física

1.3.20.3.1 A CONTRATADA deverá apresentar relatório de vistoria atestando liberação dos pontos de fixação nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.3.1.1 Para a RMR, 120 (cento e vinte) dias;

1.3.20.3.1.2 Para os demais municípios, 210 (duzentos e dez) dias.

1.3.20.3.1.3 Para o Lote 2, 60 (sessenta) dias

1.3.20.4 Entrega dos circuitos

1.3.20.4.1 A CONTRATADA deverá ativar integralmente todos os links conforme SLA nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.4.1.1 Para a RMR, 180 (cento e oitenta) dias;

1.3.20.4.1.2 Para os demais municípios, 365 (trezentos e sessenta e cinco) dias.

1.3.20.4.1.3 Para o Lote 2, 90 (noventa) dias

1.3.20.5 A CONTRATADA deverá apresentar declaração de que mantém presença física dentro da área de abrangência do novo projeto com, no mínimo, um "ponto de presença" (POP) nos municípios listados no item 96.1.1.1, apresentando registro de infraestrutura existente nestes municípios através de ARTs registradas no CREA ou registro do ponto de presença (estação) na ANATEL em nome da CONTRATADA ou de SUBCONTRATADA, dentro do prazo de 90 (noventa) dias contados a partir da assinatura do contrato.

#### 1.4. Obrigações aplicáveis ao LOTE 01 e LOTE 03:

1.4.1. A CONTRATADA deverá implementar, manter e operar, durante toda a vigência contratual, um Sistema de Gestão de Segurança da Informação (SGSI) efetivo, em conformidade com os requisitos da ISO/IEC 27001, contemplando controles compatíveis com o escopo dos serviços contratados e assegurando sua efetividade, mensurabilidade, rastreabilidade e aderência contínua. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

1.4.1.1. Política de segurança da informação formalmente estabelecida, aprovada pela CONTRATANTE, periodicamente revisada e amplamente divulgada;

1.4.1.2. Processo estruturado e contínuo de identificação, análise, avaliação e tratamento de riscos de segurança da informação, com critérios definidos e registro formal;

1.4.1.3. Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP), com testes periódicos e evidências documentadas;

1.4.1.4. Implementação de autenticação multifator (MFA) para acessos privilegiados, administrativos e remotos;

1.4.1.5. Controle de acesso lógico baseado nos princípios de privilégio mínimo, necessidade de conhecimento e segregação de funções;

1.4.1.6. Processo formal de gestão de identidades e acessos (IAM), incluindo concessão, revisão periódica e revogação tempestiva;

1.4.1.7. Processo estruturado de gestão de incidentes de segurança da informação, incluindo detecção, resposta, comunicação, registro e lições aprendidas;

1.4.1.8. Processo contínuo de gestão de vulnerabilidades, incluindo varreduras periódicas, classificação de risco, priorização e remediação;

1.4.1.9. Processo de gestão de mudanças com avaliação de impacto em segurança, aprovação formal e rastreabilidade completa;

1.4.1.10. Adoção de controles técnicos de proteção, incluindo criptografia de dados sensíveis em trânsito e em repouso, quando aplicável;

1.4.1.11. Implementação de mecanismos de registro e monitoramento (logs), com retenção adequada, integridade e capacidade de auditoria;

1.4.1.12. Conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo proteção de dados pessoais e atendimento a direitos dos titulares, quando aplicável ao escopo;

1.4.1.13. Controles de segurança física e ambiental nos ambientes computacionais, incluindo controle de acesso, vigilância e proteção contra riscos físicos;

1.4.1.14. Gestão de fornecedores e terceiros com acesso a informações ou ativos, incluindo avaliação de segurança e requisitos contratuais;

1.4.1.15. Programa contínuo de conscientização e treinamento em segurança da informação, com registro e avaliação de eficácia;

1.4.1.16. Execução de auditorias internas com manutenção de evidências e relatórios;

1.4.1.17. Tratamento formal de não conformidades, com definição, implementação e acompanhamento de ações corretivas;

1.4.1.18. Monitoramento contínuo da eficácia dos controles, com definição de indicadores, métricas e relatórios periódicos;

1.4.1.19. Manutenção de documentação e registros do SGSI com controle de versões, integridade e rastreabilidade;

1.4.1.20. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados.

1.4.2. A CONTRATADA deverá implementar, manter e operar, durante toda a vigência contratual, um Sistema de Gestão de Privacidade da Informação (SGPI), estruturado em conformidade com a ISO/IEC 27701, integrado ao SGSI, assegurando a proteção dos dados pessoais tratados no âmbito do contrato. O sistema deverá garantir efetividade, mensurabilidade, rastreabilidade e aderência contínua, observando integralmente a Lei nº 13.709/2018. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

1.4.2.1. Política de privacidade e proteção de dados pessoais formalmente estabelecida, com diretrizes específicas para tratamento de dados sensíveis e críticos;

1.4.2.2. Designação de Encarregado (DPO) com atuação efetiva, autonomia e capacidade de resposta a incidentes envolvendo dados sensíveis;

1.4.2.3. Classificação da informação e dos dados pessoais, com identificação explícita de dados sensíveis e definição de níveis de proteção diferenciados;

1.4.2.4. Registro detalhado das atividades de tratamento (ROPA), incluindo identificação de tratamentos de alto risco e dados sensíveis;

1.4.2.5. Mapeamento de fluxos de dados com identificação de pontos de exposição, transferência e compartilhamento, especialmente entre órgãos públicos e sistemas críticos;

1.4.2.6. Implementação de controles reforçados para dados sensíveis, incluindo criptografia obrigatória em trânsito e em repouso, controle de acesso restritivo e monitoramento contínuo;

1.4.2.7. Aplicação dos princípios de minimização de dados, limitação de finalidade e necessidade, especialmente em bases contendo dados de saúde, educação e segurança;

1.4.2.8. Processo estruturado para atendimento aos direitos dos titulares, com tratamento prioritário para dados sensíveis;

1.4.2.9. Realização obrigatória de Relatório de Impacto à Proteção de Dados (RIPD/DPIA) para tratamentos que envolvam dados sensíveis ou operações críticas;

1.4.2.10. Processo robusto de gestão de incidentes de privacidade, com notificação tempestiva à CONTRATANTE, autoridades competentes e titulares, quando aplicável;

1.4.2.11. Gestão rigorosa de terceiros, com exigência de níveis equivalentes de proteção de dados e cláusulas contratuais específicas para dados sensíveis;

1.4.2.12. Definição de políticas de retenção e descarte seguro, com critérios diferenciados para dados sensíveis;

1.4.2.13. Monitoramento contínuo e auditoria dos acessos e tratamentos realizados sobre dados sensíveis, com trilhas de auditoria completas;

1.4.2.14. Programa contínuo de capacitação com ênfase em tratamento de dados sensíveis e riscos associados;

1.4.2.15. Monitoramento por indicadores e métricas específicas para privacidade, incluindo eventos envolvendo dados sensíveis;

1.4.2.16. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de

conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados

## **2. OBRIGAÇÕES DA CONTRATANTE**

2.1. A CONTRATANTE Principal possui as seguintes obrigações:

- 2.1.1. Prestar assessoramento no dimensionamento dos valores físicos e financeiros dos serviços contratados;
  - 2.1.2. Padronizar e formalizar as demandas e solicitações realizadas pelos CONTRATANTES aderentes;
  - 2.1.3. Controlar os fluxos contratuais junto aos Órgãos de Controle do Governo, bem como, junto a CONTRATADA e aos CONTRATANTES aderentes;
  - 2.1.4. Controlar, através da emissão de Ordens de Serviço, os limites contratuais Nova Rede Corporativa como um todo;
  - 2.1.5. Avaliar as condições do atendimento dos serviços de telemática, propor melhorias e estabelecer modelos visando a melhor execução destes serviços;
  - 2.1.6. Prover informações gerenciais referentes aos resultados dos serviços prestados pela Nova Rede Corporativa;
  - 2.1.7. Gerenciar e dar suporte ao controle da capacidade disponibilizada pelos recursos tecnológicos integrantes dos serviços contratados através da nova Rede, prestando assessoramento nas questões de qualidade, desempenho e inovação tecnológica, bem como, avaliando e aprovando os planos de implantação e o dimensionamento dos recursos técnicos para atendimento às solicitações;
- Acompanhar e analisar os registros das ocorrências, dos fatos relevantes e dos níveis de qualidade contratados, utilizando-se da solução de Sistemas Gerenciais previstos e dos relatórios emitidos.
- 2.1.8. Instaurar o processo de aplicação de penalidades para os casos de falhas e/ou atrasos na execução dos serviços da Nova Rede Corporativa e/ou que atinjam um ou mais de um CONTRATANTE aderente.

**2.2. A CONTRATANTE aderente Técnica tem como responsabilidade a Gestão Técnica Corporativa da nova Rede, contratando, hospedando e gerenciando os serviços de uso compartilhado, sendo suas obrigações:**

- 2.2.1. Efetuar os pagamentos relativos aos serviços formalmente contratados específicos à sua competência como Gerente Técnica da nova Rede, mediante efetiva comprovação dos serviços prestados aos órgãos do Poder Executivo, que dependem de recursos do Tesouro Estadual;
- 2.2.2. Adotar medidas visando um eficaz relacionamento com os fornecedores de serviços de telemática, de forma a ensejar o melhor desempenho e a melhor qualidade na prestação dos serviços contratados;
- 2.2.3. Fazer o acompanhamento da execução dos serviços contratados;
- 2.2.4. Analisar as questões relacionadas com o desenvolvimento dos serviços de telemática, identificando eventuais problemas e propondo medidas preventivas e corretivas;
- 2.2.5. Prestar apoio técnico aos usuários, acompanhando todos os serviços em fase de implantação, como também verificar e avaliar os serviços instalados e em operação;
- 2.2.6. Fornecer à SAD e às CONTRATANTES aderentes informações gerenciais e sobre fatos que possam levar à aplicação de penalidades contra qualquer fornecedor dos serviços da Nova Rede Corporativa, ou mesmo à rescisão do contrato;
- 2.2.7. Controlar e avaliar tecnicamente os serviços solicitados através das Ordens de Serviços formalizadas, bem como o acompanhamento da execução técnica destes serviços;

2.2.8. Acompanhar a execução das Ordens de Serviços, verificando, registrando, controlando suas conclusões e os eventos e ocorrências relacionados a estas, facilitando a interlocução entre os CONTRATANTES aderentes e a CONTRATADA, tendo como objetivo a efetiva conclusão dos serviços solicitados dentro dos requisitos exigidos;

2.2.9. Receber os serviços, observando os requisitos técnicos associados aos mesmos, em conformidade com todas as exigências especificadas nos itens e subitens deste Termo e seus Adendos;

2.2.10. Fornecer dados estatísticos referentes à utilização dos recursos da Nova Rede Corporativa;

2.2.11. Registrar formalmente às ocorrências e as falhas ocorridas nos serviços da da Nova Rede Corporativa;

2.2.12. Gerenciar, administrativamente e tecnicamente, as soluções operacionalizadas pela Nova Rede Corporativa, hospedando o conjunto no ambiente operacional denominado de Centro Integrado de Inteligência e Segurança Cibernética, que também atenderá as demandas repassadas via Service desk;

2.2.13. Deverá, durante o período de assunção da Nova Rede Corporativa de telemática, realizar imediatamente a retirada e/ou redução dos níveis dos serviços compartilhados da nova Rede à medida que os serviços da Nova Rede Corporativa forem sendo ativados;

2.2.14. Responsabilizar-se, em casos de danos decorrentes de culpa da CONTRATANTE, incluindo situações constatadas de mau uso, perda, roubo, furto ou extravio, pelos prejuízos causados aos equipamentos disponibilizados pela CONTRATADA, quando estes estiverem localizados em propriedades da CONTRATANTE, na execução dos serviços objeto deste Contrato. O ressarcimento será realizado com base nos preços praticados pelo mercado para um novo equipamento, igual ou similar, mediante apresentação à CONTRATANTE de documento de cotação com valores obtidos de, no mínimo, três empresas e respectiva Nota Fiscal de compra do novo equipamento.

### **2.3. Os CONTRATANTES aderentes têm as seguintes obrigações:**

2.3.1. Realizar a previsão orçamentária e financeira para lastrear os pagamentos dos serviços contratados, em conformidade com os respectivos exercícios financeiros, diretrizes e legislação vigente no âmbito dos Poderes que integram;

2.3.2. Formalizar o Termo de Adesão ao Contrato Mater nos prazos estipulados pela CONTRATANTE Principal;

2.3.3. Relacionar os serviços a serem contratados através do Adendo ao Termo de Adesão ao Contrato Mater;

2.3.4. Formalizar as Ordens de Serviços referente aos serviços solicitados nos seus respectivos Termos de Adesão;

2.3.5. Acompanhar a execução dos serviços solicitados, atestar e arcar com os devidos pagamentos dos serviços efetivamente executados;

2.3.6. Realizar as possíveis contestações de faturas, caso haja, suspendendo o pagamento e aguardando a resposta da CONTRATADA.

2.3.7. Efetuar os pagamentos relativos aos serviços contratados, mediante efetiva comprovação e atesto dos serviços prestados;

2.3.8. Atender às orientações e regras formalizadas pela CONTRATANTE Principal e pela CONTRATANTE aderente Técnica;

2.3.9. Designar servidor para cumprir a função de Gestor de Telemática, o qual deverá ser responsável pelos assuntos contratuais, orçamentários, financeiros, técnicos e operacionais, respectivamente, fiscalizando a execução físico-financeira, bem como, a qualidade da prestação dos serviços contratados de acordo com a legislação vigente;

2.3.10. Responsabilizar-se, em casos de danos decorrentes de culpa da CONTRATANTE, incluindo situações constatadas de mau uso, perda, roubo, furto ou extravio, pelos prejuízos causados aos equipamentos disponibilizados pela CONTRATADA, quando estes estiverem localizados em propriedades da CONTRATANTE, na execução dos serviços objeto deste Contrato. O ressarcimento será realizado com base nos preços praticados pelo mercado para um novo

equipamento, igual ou similar, mediante apresentação à CONTRATANTE de documento de cotação com valores obtidos de, no mínimo, três empresas e respectiva Nota Fiscal de compra do novo equipamento;

2.3.11. A CONTRATANTE poderá emitir Notificação Extrajudicial, estipulando prazo específico para que se providenciem os instrumentos jurídicos necessários para a regularização contratual, sob pena de sofrer auditoria dos Órgãos de controle, além das consequências legais cabíveis, caso configure-se mora no processo de formalização contratual por parte do CONTRATANTE aderente, conforme item 2.3.2 deste Adendo;

2.3.12. Deverá, durante o período de assunção da Nova Rede Corporativa de telemática, realizar imediatamente a retirada dos serviços contratados da nova Rede à medida que os serviços contratados da Nova Rede Corporativa de corporativa forem ativados;

2.3.13. A CONTRATANTE estará isenta de responsabilização a partir da data de ciência por parte do CONTRATANTE aderente da Notificação Extrajudicial referida no item 2.3.11 deste Adendo.

## ADENDO II – NÍVEIS MÍNIMOS DE SERVIÇO

### 1. Definições para os Níveis Mínimos de Serviço (NMS)

1.1. Este Adendo tem como objetivo estabelecer mecanismos de gestão da qualidade na prestação dos serviços contratados, disciplinando definições, métodos de aferição, critérios de avaliação e ações corretivas necessárias para garantir a adequada prestação dos serviços aos CONTRATANTES. Inclui, ainda, as respectivas glosas contratuais em caso de descumprimento dos níveis mínimos estabelecidos.

1.2. O Nível Mínimo de Serviço (NMS) define os termos e as condições sob as quais a CONTRATADA deverá prover os serviços especificados neste Termo e seus respectivos ADENDOS.

1.3. Os indicadores estabelecidos neste documento têm como finalidade garantir a qualidade, possibilitar a avaliação objetiva da CONTRATADA e fornecer subsídios para a tomada de decisão no monitoramento e aprimoramento contínuo dos serviços de Conectividade, Segurança Cibernética, Voz e Wi-Fi da Nova Rede Corporativa do Governo do Estado de Pernambuco.

1.4. Para efeito deste Termo de Referência, além das definições constantes nas regulamentações aplicáveis aos serviços de telecomunicações regidos pela ANATEL, são adotadas as seguintes definições:

1.4.1. Processo de aferição: conjunto de atividades envolvidas na coleta, processamento e agregação de dados e cálculo dos indicadores;

1.4.2. Comissão de Auditoria (CA): grupo coordenado pela ATI/SAD, responsável por estabelecer os parâmetros técnicos de execução, operacionalização e atualização dos procedimentos de aferição da Qualidade do NMS. Poderão participar da Comissão servidores, terceirizados e quaisquer outras entidades designadas (físicas ou jurídicas) para a execução dessas atividades;

1.4.3. Verificador Independente: entidade responsável pela execução total ou parcial do processo de aferição da Qualidade, conforme designação da Comissão de Auditoria;

1.4.4. Índice de Reclamações do Usuário (IR): índice destinado a avaliar a quantidade de reclamações pós-consumo recebidas por órgãos Aderentes e as providências adotadas pela CONTRATADA para sua resolução;

1.4.5. Índice de Qualidade do Serviço (IQS): índice calculado a partir da agregação de parâmetros técnicos estabelecidos neste Adendo, representando a qualidade dos serviços efetivamente entregues pela CONTRATADA aos órgãos Aderentes;

1.4.6. Índice de Qualidade Percebida (IQP): índice baseado nos resultados de Pesquisa de Qualidade Percebida, conforme previsto no Regulamento das Condições de Aferição do Grau de Satisfação e Qualidade Percebida junto aos Usuários de Serviços de Telecomunicações (Resolução nº 654, de 13 de julho de 2015) ou outro instrumento normativo que o substitua. Esse índice expressa a percepção do usuário quanto ao desempenho da CONTRATADA e deverá ser realizado pela CONTRATADA ou por instituições independentes designadas pela CONTRATANTE;

1.4.7. Interrupção: paralisação do serviço decorrente de qualquer falha de rede ou equipamentos da CONTRATADA que impeça a fruição do serviço, excluindo-se os casos de falha individual do acesso de usuário de responsabilidade da CONTRATANTE;

1.4.8. Interrupção Massiva: interrupção de grande abrangência ou que afete número significativo de PCSs;

1.4.9. Qualidade: a totalidade de características de uma prestadora que lhe conferem sua habilidade de satisfazer necessidades explícitas e implícitas dos CONTRATANTES;

1.4.10. Indicadores Informativos: indicadores de qualidade que avaliam características complementares ao desempenho aferido pelos índices IR, IQP e IQS.

1.5. A Qualidade da prestação dos serviços será aferida a partir dos seguintes indicadores: Índice de Qualidade de Serviços (IQS), Índice de Reclamação (IR) e Índice de Qualidade Percebida (IQP).

1.6. A Comissão de Auditoria, decidirá, excepcionalmente, sobre a forma de cálculo do IQS, IR e IQP, e de novos prazos de divulgação, quando o indicador não puder ser calculado e/ou consolidado, seja por eventuais atrasos no envio dos dados, seja pela sua indisponibilidade.

1.7. A CONTRATADA deverá conceder à Comissão de Auditoria acesso de LEITURA a qualquer equipamento e solução utilizada para a prestação dos serviços definidos neste Termo de Referência.

1.7.1. A Comissão de Auditoria poderá delegar esses acessos a qualquer pessoa física ou jurídica que represente seus interesses.

1.7.2. Caso o equipamento, ferramenta ou solução da CONTRATADA não possua um modo de somente leitura a CONTRATADA deverá fornecer acesso integral (LEITURA e ESCRITA), assegurando as obrigações previstas neste Termo.

1.7.3. A CONTRATADA deverá disponibilizar à Comissão de Auditoria acesso às bases de dados das ferramentas de monitoração, bem como relatórios gerenciais contendo informações sobre percentual de disponibilidade mensal de cada PCS e tempo de recuperação operacional de cada ticket aberto.

1.8. A CONTRATADA deverá fornecer relatórios customizados à Comissão de Auditoria sempre que solicitado.

1.9. A CONTRATADA deverá viabilizar meios automatizados para o envio das informações solicitadas pela Comissão de Auditoria.

1.9.1. Sempre que possível, a extração automatizada dos dados deverá ser realizada diretamente nos equipamentos que geram essas informações, garantindo sua integridade.

1.10. Caso a CONTRATADA julgue tecnicamente inviável atender a uma solicitação da Comissão de Auditoria, deverá apresentar justificativa técnica detalhada para análise e validação da Comissão. A Comissão poderá rejeitar a justificativa e manter a solicitação vigente.

1.11. A periodicidade da medição dos indicadores do NMS será:

1.11.1. Mensal: para os indicadores IQS e IR;

1.11.2. Trimestral: para o indicador IQP.

1.12. Os indicadores devem ser consolidados por CONTRATANTE ADERENTE, conforme os serviços contratados e em operação.

1.13. A CONTRATADA assume inteira responsabilidade pelo funcionamento e disponibilidade dos serviços contratados, reconhecendo que o não atendimento dos níveis de serviço pode causar impacto relevante nas operações do Governo do Estado de Pernambuco, sujeitando-se às penalidades previstas neste documento.

1.14. Os indicadores deverão ser medidos do primeiro ao último dia de cada mês e divulgação dos resultados na reunião mensal de acompanhamento com o Gestor do Contrato.

1.15. A CONTRATADA ficará desobrigada do cumprimento dos níveis de serviço enquanto a prestação de serviços estiver prejudicada em função de impedimento ou retardo decorrente de responsabilidade comprovada da CONTRATANTE.

Esta responsabilidade deverá ser comprovada mediante formalização da CONTRATADA e deverão ser validados pela CONTRATANTE.

1.16. Todos os itens de serviço descritos neste Termo deverão seguir os tempos limites de restabelecimento destacados na tabela de **LIMITES DE TEMPOS PARA CORREÇÕES DE FALHAS**.

1.17. A tabela abaixo agrupa os itens de serviço e suas respectivas classes de serviço, adendos e LOTES.

LOTE 01	
CLASSE DE SERVIÇO	DESCRIÇÃO
<b>ADENDO III - SEGURANÇA DE REDE LOCAL</b>	
SEGURANÇA	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1
SEGURANÇA	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 2
SEGURANÇA	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço
SEGURANÇA	Solução para gerenciamento de acessos à rede local - NAC
<b>ADENDO IV - SERVIÇO DE REDE SEM FIO</b>	
WIFI	Serviço de Rede Sem Fio Interno com Segurança
WIFI	Serviço de Rede Sem Fio Externo com Segurança
WIFI	Serviço de Rede Sem Fio Temporário com Segurança
WIFI	Serviço de fornecimento e implantação de Switch
<b>ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL</b>	
CONECTIVIDADE	Link de Acesso Permanente (LAP - Tipo 1)
CONECTIVIDADE	Link de Acesso Permanente (LAP - Tipo 2)
CONECTIVIDADE	Link Multitecnologia Especial (LME) - Tipo 1
CONECTIVIDADE	Link Multitecnologia Especial (LME) - Tipo 2
CONECTIVIDADE	Link Multitecnologia Especial (LME) - Tipo 3
CONECTIVIDADE	Link Acesso Temporário (LAT) - Tipo 1
CONECTIVIDADE	Link Acesso Temporário (LAT) - Tipo 2
CONECTIVIDADE	Link Acesso Temporário (LAT) - Tipo 3
<b>ADENDO VI - SEGURANÇA DE DATACENTER</b>	
SEGURANÇA	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER
SEGURANÇA	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço
SEGURANÇA	Solução de segurança de confiança zero - ZTNA
SEGURANÇA	Solução de proteção, detecção e resposta para servidores - EDR
SEGURANÇA	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR
SEGURANÇA	Solução para gerenciamento de acessos à rede datacenter - NAC
SEGURANÇA	Solução de segurança de identidade privilegiada - PAM
SEGURANÇA	Solução de filtro de mensagens indesejadas - ANTISPAM

SEGURANÇA	Solução de Filtro de Aplicações WEB - WAF
<b>ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO</b>	
SEGURANÇA	Solução de gerenciamento e monitoramento de ativos - ITAM
SEGURANÇA	Solução de gerenciamento de identidade de acesso - IAM
SEGURANÇA	Solução de monitoramento e análise de eventos de segurança - SIEM
SEGURANÇA	Solução de automação de resposta a incidentes de segurança - SOAR
SEGURANÇA	Solução para guarda de LOGs
SEGURANÇA	Serviço de disponibilização de ambiente de testes
SEGURANÇA	Solução de gerenciamento de serviços de TI - ITSM
<b>ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA</b>	
SEGURANÇA	Serviço de resposta à incidentes de cibersegurança sob demanda
SEGURANÇA	Serviço de análise de segurança de primeiro nível
SEGURANÇA	Serviço de análise de segurança especializada
SEGURANÇA	Serviço de acompanhamento de reparos
SEGURANÇA	Serviço de atenção especializada ao cliente
SEGURANÇA	Service Desk
SEGURANÇA	Serviço de operação da rede
SEGURANÇA	Serviço de análise de qualidade
SEGURANÇA	Serviço de Coordenação do CIISC
SEGURANÇA	Núcleo de Redes e Segurança Setorial
SEGURANÇA	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCs)
SEGURANÇA	Serviço de Evolução da Maturidade em Segurança da Informação
<b>ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)</b>	
VOZ	Serviço de Comunicação Unificada - SCU (Conta de usuário)
<b>ADENDO XIII – SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE</b>	
VOZ	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)
VOZ	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)
VOZ	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)
VOZ	Serviço de Ponto de Voz Fixo com Aparelho de Voz DECT IP (PVF-DECT IP)
VOZ	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)
VOZ	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)
VOZ	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)
VOZ	Serviço PVF-Fone-de-Cabeça
VOZ	Serviço Adicional de Acesso SIP (SIP TRUNK)
<b>ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER</b>	
VOZ	Serviço de Contact Center com Recurso de Voz
VOZ	Serviço de Contact Center com recurso de Whatsapp
VOZ	Serviço de Contact Center com recurso de Redes Sociais
VOZ	Serviço de Unidade de Resposta Audível (Porta de URA)
VOZ	Serviço de Comunicação por vídeo ou vídeo-chamada
VOZ	Serviço de Automatizações e Integrações - Consultoria Inicial

VOZ	Serviço de Automatizações e Integrações - Implantação
<b>ADENDO XV - SERVIÇO TRÁFEGO TELEFÔNICO EXTRAREDE REVERSO, DO TIPO DISCAGEM DIRETA GRATUITA (DDG)</b>	
VOZ	Serviço Tráfego Telefônico Extrarede Reverso, do tipo DISCAGEM DIRETA GRATUITA (DDG)
<b>ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO</b>	
TODAS	Suporte de Manutenção (12h x 7d)
TODAS	Suporte de Manutenção (24h x 7d)

Tabela 01 – Itens de serviço x classes de serviço do LOTE 01

LOTE 02	
CLASSE DE SERVIÇO	DESCRIÇÃO
<b>ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER</b>	
CONECTIVIDADE	Link de Fibra Lan To Lan 100GB (L2L)
CONECTIVIDADE	Link para Data Center de 2GB com AntiDDoS - Link Internet Trânsito (LIT)
CONECTIVIDADE	Link para Data Center de 4GB com AntiDDoS - Link Internet Trânsito (LIT)
CONECTIVIDADE	Link para Data Center de 6GB com AntiDDoS - Link Internet Trânsito (LIT)
CONECTIVIDADE	Link para Data Center de 8GB com AntiDDoS - Link Internet Trânsito (LIT)
CONECTIVIDADE	Link para Data Center de 10GB com AntiDDoS - Link Internet Trânsito (LIT)

Tabela 02 – Itens de serviço x classes de serviço do LOTE 02

LOTE 03	
CLASSE DE SERVIÇO	DESCRIÇÃO
<b>ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS</b>	
SEGURANÇA	Serviço de gestão de vulnerabilidades
SEGURANÇA	Serviço de análise forense
SEGURANÇA	Serviço de análise de segurança ofensiva (Red Team)
SEGURANÇA	Serviço de testes de intrusão (Pentest)

Tabela 03 – Itens de serviço x classes de serviço do LOTE 03

## 2. Dos Índices IQP, IR e IQS

### 2.1. Índice de Qualidade Percebida (IQP)

2.1.1. O IQP será mensurado trimestralmente por meio de Pesquisa de Satisfação e Qualidade, a ser realizada junto aos CONTRATANTES ADERENTES para os respectivos serviços prestados pela CONTRATADA, nos termos determinados pela Comissão de Auditoria;

2.1.2. A CONTRATADA será responsável por realizar a Pesquisa de Satisfação e Qualidade, devendo sugerir um conjunto de perguntas a serem validadas pela ATI antes da aplicação. A metodologia adotada deverá assegurar imparcialidade e confiabilidade dos resultados, garantindo amostras estatisticamente relevantes para cada CONTRATANTE ADERENTE.

2.1.2.1. A pesquisa deverá incluir perguntas-chave destinadas a avaliar, de forma objetiva, a qualidade dos serviços prestados pela CONTRATADA, organizadas por tipo de serviço contratado. Além disso, a pesquisa deverá contemplar avaliações gerais sobre a CONTRATADA, abrangendo aspectos contratuais e a atuação dos profissionais diretamente envolvidos na prestação dos serviços. Essa avaliação deverá abordar posturas como resolutividade, cordialidade, atenção ao cliente, presença em momentos críticos e eficácia na solução de problemas.

2.1.2.1.1. Abaixo, apresenta-se um modelo de perguntas que servirá como base para a elaboração da pesquisa:

1. Qual a sua satisfação geral com o serviço contratado?
2. Com que frequência você enfrenta problemas recorrentes com o serviço?
3. A equipe de suporte técnico da CONTRATADA resolveu seus problemas de maneira eficaz e dentro do prazo estabelecido?
4. Como você avalia a transparência e a clareza das informações fornecidas pela CONTRATADA sobre a execução dos serviços contratados?
5. A solução contratada atendeu plenamente às suas necessidades em termos de conectividade, segurança, voz e/ou Wi-Fi?
6. Como você avalia a postura dos profissionais da CONTRATADA em relação à resolução de problemas e atendimento às suas demandas?
7. Os profissionais da CONTRATADA demonstraram comprometimento, cordialidade e atenção durante o período avaliado?
8. Como você avalia a qualidade da navegação e a estabilidade dos links de acesso?
9. Como você avalia a eficiência da solução em relação à proteção contra ameaças cibernéticas?
10. Como você avalia a qualidade geral das chamadas realizadas pelo serviço de telefonia?
11. Como você avalia a qualidade do sinal da rede sem fio nos locais em que mais utiliza o serviço?
12. Como você avalia a facilidade e a segurança do processo de autenticação de usuário por meio da rede sem fio?

2.1.2.2. A CONTRATADA, mediante validação prévia da ATI, poderá incluir e modificar as perguntas.

2.1.2.3. As respostas deverão ser coletadas com base em uma escala de 1 a 10, onde 1 significa "muito insatisfeito" 10 "muito satisfeito", conforme metodologia acordada com a ATI.

2.1.2.4. A pesquisa de satisfação deverá ser aplicada por meio de uma metodologia híbrida, garantindo maior taxa de resposta e qualidade nos dados coletados. A CONTRATADA deverá adotar, no mínimo, os seguintes canais para aplicação da pesquisa:

- 2.1.2.4.1. Formulário digital enviado por e-mail ao gestor responsável de cada CONTRATANTE ADERENTE;
- 2.1.2.4.2. Contato telefônico, realizado por equipe especializada em pesquisa de satisfação, quando não houver resposta digital dentro do prazo estipulado;
- 2.1.2.4.3. Disponibilização contínua da pesquisa via portal de serviços, para permitir respostas espontâneas ao longo do período de aferição.
- 2.1.2.5. A CONTRATADA deverá utilizar uma ferramenta digital de pesquisa que possibilite a coleta e análise automatizada dos dados, permitindo a geração de relatórios quantitativos e qualitativos que consolidem a percepção dos usuários sobre os serviços contratados.
- 2.1.2.6. A CONTRATADA deverá disponibilizar um painel de monitoramento online (dashboard) para acompanhamento dos resultados pelo CONTRATANTE ADERENTE e pela ATI.

2.1.3. O IQP não será passível de glosa, servindo exclusivamente para acompanhamento da satisfação dos usuários e aprimoramento contínuo dos serviços prestados.

2.1.4. O Índice IQP deverá ser consolidado por cada CONTRATANTE ADERENTE e segmentado por tipo de serviço prestado (Conectividade, Segurança, Voz e Wi-Fi), garantindo que eventuais melhorias sejam direcionadas de forma específica para cada segmento contratado.

2.1.5. Obrigações da CONTRATADA para viabilização do IQP:

2.1.5.1. A CONTRATADA deverá prever e estruturar os seguintes recursos para execução eficaz das pesquisas de satisfação:

2.1.5.1.1. Equipe especializada em pesquisa de satisfação e qualidade percebida, que será responsável por aplicar, compilar e analisar os resultados da pesquisa, garantindo a neutralidade e a confiabilidade dos dados coletados, conforme previsto no ADENDO IX;

2.1.5.1.2. Ferramenta de pesquisa digital e automatizada, com capacidade para coletar e tabular os dados de forma estruturada, assegurando a rastreabilidade das respostas;

2.1.5.1.3. Infraestrutura para relatórios e dashboards interativos, permitindo que a ATI e os CONTRATANTES ADERENTES acessem os resultados de forma contínua e transparente.

2.1.5.2. A CONTRATADA deverá garantir que cada gestor designado pelos CONTRATANTES ADERENTES receba a pesquisa dentro dos prazos estabelecidos e terá um período máximo de 10 dias úteis para responder.

2.1.5.3. No caso de não resposta por parte do gestor da CONTRATANTE ADERENTE dentro do prazo estipulado, os seguintes critérios serão adotados:

2.1.5.3.1. O resultado da pesquisa para aquele órgão não será computado como 100% e, sim, desconsiderado do cálculo do IQP, evitando distorções nos indicadores;

2.1.5.3.2. A CONTRATADA deverá registrar as tentativas de contato e apresentar evidências documentais (e-mails, logs de chamadas telefônicas ou registros no portal), quando solicitada, para comprovação da tentativa de coleta da resposta;

2.1.5.3.3. Caso o índice de resposta de um determinado órgão seja inferior a 50% em dois ciclos consecutivos, a Comissão de Auditoria poderá solicitar ajustes metodológicos ou a aplicação de mecanismos adicionais para incentivar a participação.

2.1.6. A CONTRATANTE poderá estabelecer obrigações formais para que os gestores designados respondam à pesquisa trimestralmente, por meio de ato normativo próprio, visando garantir a efetividade da aferição.

2.1.7. A não realização da pesquisa trimestral, sua aplicação de forma incompleta ou sua manipulação visando alterar os resultados poderá ensejar à CONTRATADA advertências formais, notificações e demais penalidades previstas no contrato, sem prejuízo da adoção de medidas adicionais para garantir a sua execução.

## 2.2. Índice de Reclamações do Usuário (IR)

2.2.1. O Índice IR deverá ser consolidado mensalmente, para cada CONTRATANTE ADERENTE, segmentado por classe de serviço contratada.

2.2.2. O índice IR não será passível de glosa, servindo exclusivamente como indicador de melhoria contínua, auxiliando a CONTRATADA e os CONTRATANTES ADERENTES na identificação de problemas recorrentes, monitoramento da qualidade do atendimento e aprimoramento dos processos internos.

2.2.3. A CONTRATADA será responsável por registrar, analisar e reportar mensalmente todas as reclamações recebidas dos CONTRATANTES ADERENTES, consolidando pelo menos os seguintes aspectos:

2.2.3.1. Total de reclamações por classe de serviço (Conectividade, Segurança, Voz e Wi-Fi);

- 2.2.3.2. Percentual de reclamações solucionadas dentro do prazo máximo estabelecido no contrato;
- 2.2.3.3. Ações corretivas aplicadas e respectivas evidências de mitigação;
- 2.2.3.4. Classificação das reclamações (por gravidade, tempo de resolução e reincidência);
- 2.2.3.5. Identificação de tendências e recorrências, apresentando planos de ação corretivos e preventivos.
- 2.2.4. A CONTRATADA deverá oferecer múltiplos canais de atendimento para o registro das reclamações, garantindo acessibilidade e diversidade de meios, incluindo, no mínimo:
- 2.2.4.1. Portal Web exclusivo para o contrato;
- 2.2.4.2. Ouvidoria específica para os CONTRATANTES ADERENTES;
- 2.2.4.3. Atendimento telefônico com suporte especializado;
- 2.2.4.4. Aplicativo móvel para registro e acompanhamento de chamados;
- 2.2.4.. A CONTRATADA deverá assegurar que todos os canais sejam de fácil acesso, permitam o acompanhamento do status das reclamações e contemplem opções de feedback para os usuários.
- 2.2.5. O Índice IR será definido como a relação entre o total de reclamações registradas pelo CONTRATANTE ADERENTE durante o período de medição e a quantidade de PCS contratados, conforme especificado abaixo:
- 2.2.5.1. Para CONTRATANTES com até 5 (cinco) PCS contratados, o IR será calculado pela fórmula:
- 2.2.5.1.1. Representação Matemática:
- $$IR = \frac{\text{Total de Reclamações}}{\text{Quantidade de PCS}}$$
- Onde:
- Total de Reclamações: Representa a quantidade de reclamações qualificáveis registradas nos canais de atendimento referente à CONTRATADA, ao correspondente serviço no período de 30 (trinta) dias.
  - Quantidade de PCS: Representa a quantidade de PCSs atendidos no último dia do mês da medição.
- 2.2.5.2. Para CONTRATANTES com mais de 5 (cinco) PCS contratados:
- $$IR = \frac{\text{Total de Reclamações}}{\ln(\text{Quantidade de PCS})}$$
- Onde:
- Total de Reclamações: Representa a quantidade de registros qualificados de reclamação nos canais da CONTRATADA dentro do mês de medição.
  - Quantidade de PCS: Representa a quantidade de PCSs ativos no último dia do mês da medição.
  - Logaritmo Natural (ln): Representa a escala logarítmica utilizada para ajustar o impacto do número de reclamações em relação ao volume de PCS contratados.
- 2.2.6. A CONTRATADA terá obrigação de tratar todas as reclamações abertas da CONTRATANTE ADERENTE, dentro de um prazo máximo de 7 (sete) dias corridos a partir do registro, apresentando uma das seguintes respostas:
- Resolução completa da reclamação e fechamento do chamado;
  - Proposta de solução, incluindo prazo e medidas corretivas a serem adotadas;
  - Justificativa fundamentada para casos em que a reclamação seja considerada improcedente.

2.2.6.1. O CONTRATANTE ADERENTE poderá:

2.2.6.1.1. Aceitar a solução e encerrar a reclamação;

2.2.6.1.2. Contestar a solução e solicitar reavaliação técnica da Comissão de Auditoria.

2.2.6.2. Se a CONTRATADA considere alguma reclamação improcedente, deverá apresentar defesa técnica para análise da Comissão de Auditoria, que julgará a procedência e classificação da reclamação.

2.2.6.3. A Comissão de Auditoria poderá solicitar a um Verificador Independente a avaliação dos casos contestados pela CONTRATADA.

2.2.6.4. A Comissão de Auditoria terá a decisão final sobre eventuais divergências entre a CONTRATADA e a CONTRATANTE ADERENTE, após a devida análise de todas as informações pertinentes ao caso, assegurando a fundamentação técnica e a transparência no processo decisório.

2.2.6.5. O CONTRATANTE ADERENTE não terá limite de abertura de reclamações, podendo registrar quantas forem necessárias para garantir a conformidade do serviço.

2.2.7. A CONTRATADA deverá prever os seguintes recursos para garantir a execução eficaz da gestão de reclamações:

2.2.7.1. Equipe especializada em atendimento e resolução de problemas, disponível conforme o regime de atendimento 8h x 5d (8(oito) horas por dia e 5 (cinco) dias por semana;

2.2.7.2. Ferramenta digital para gestão automatizada de reclamações, permitindo a rastreabilidade dos chamados e a integração com sistemas de auditoria da ATI;

2.2.7.3. Infraestrutura para relatórios e dashboards interativos, garantindo que a ATI e os CONTRATANTES ADERENTES acompanhem o status das reclamações em tempo real.

2.2.8. A não execução adequada do gerenciamento do Índice IR, incluindo o não registro ou a não tratativa de reclamações dentro do prazo estabelecido, poderá resultar à CONTRATADA em advertências formais, notificações, sanções e demais penalidades previstas no contrato, sem prejuízo da adoção de medidas corretivas adicionais por parte da ATI.

### 2.3. Índice de Qualidade de Serviços (IQS)

2.3.1. O Índice de Qualidade de Serviços (IQS) será consolidado mensalmente para cada CONTRATANTE ADERENTE, considerando os diferentes tipos de serviços contratados. Cada serviço terá indicadores específicos, conforme a classificação abaixo:

Tipo de Serviço	Acrônimo
Conectividade	<b>IQS<sub>Con</sub></b>
Segurança Cibernética	<b>IQS<sub>Seg</sub></b>
Voz	<b>IQS<sub>Voz</sub></b>
Rede Wi-Fi	<b>IQS<sub>WIFI</sub></b>

Tabela 04 – Índice IQS – Tipos de serviço x Acrônimos

2.3.2. O IQS será calculado individualmente para cada tipo de serviço (Conectividade, Segurança Cibernética, Voz e Wi-Fi), com base nos parâmetros técnicos definidos neste Termo de Referência e nos seus respectivos Adendos.

2.3.3. Cada item de serviço contará com um conjunto de indicadores técnicos obrigatórios, avaliados de forma equitativa, considerando peso igualitário entre os indicadores dentro do mesmo item de serviço. Esse critério garante uniformidade na avaliação da qualidade.

2.3.4. O descumprimento dos parâmetros técnicos impactará diretamente nos indicadores dos itens de serviço e poderá resultar na aplicação de glosas contratuais, conforme os percentuais especificados neste Termo de Referência.

2.3.5. As glosas serão aplicadas mensalmente e individualmente para cada item de serviço, considerando o nível de descumprimento apurado no Item de serviço correspondente.

2.3.6. A CONTRATADA será integralmente responsável pela precisão e confiabilidade das medições, devendo disponibilizar ferramentas automatizadas e auditáveis para monitoramento, medição e análise dos indicadores, assegurando total transparência e acesso em tempo real aos dados pela CONTRATANTE.

2.3.7. A Comissão de Auditoria, ou entidade por ela designada, terá o direito de acessar equipamentos e consultar bases de informações relacionadas aos serviços prestados, exclusivamente em caráter de leitura e auditoria. O objetivo é garantir fiscalização plena e transparente de todas as informações disponibilizadas pela CONTRATADA. A CONTRATADA deverá assegurar o fornecimento imediato dos dados requisitados e prestar total colaboração com os processos de auditoria e eventuais desdobramentos necessários.

2.3.8. Os itens de serviços contratados possuem um conjunto de indicadores técnicos específicos, que podem variar de 1 a 9 indicadores por item de serviço. Esses indicadores deverão ser rigorosamente monitorados e medidos com base nos valores de referência estabelecidos para cada indicador, garantindo conformidade com os níveis mínimos exigidos.

2.3.8.1. A avaliação do descumprimento será realizada mensalmente, mediante a comparação dos resultados obtidos com os valores de referência exigidos. Para cada serviço, será verificado individualmente o percentual de indicadores que não atingiram a meta mínima estabelecida.

2.3.8.2. Cada indicador que não atender aos valores mínimos exigidos será contabilizado como descumprimento contratual. A taxa de descumprimento e o respectivo percentual de glosa serão calculadas conforme as regras abaixo:

2.3.8.2.1. Para itens de serviço que possuem 4 (quatro) ou mais indicadores técnicos, o percentual de descumprimento será calculado utilizando a fórmula abaixo:

$$\text{Percentual de Descumprimento} = \frac{\text{Quantidade de Indicadores não cumpridos}}{\text{Total de indicadores do serviço}} \times 100$$

Nota: Esse cálculo tem como objetivo determinar o impacto do descumprimento dos indicadores no desempenho geral do item de serviço contratado.

2.3.8.2.1.1. O percentual de descumprimento apurado será utilizado para determinar o correspondente percentual de glosa aplicada, conforme especificado na Tabela de Aplicação de Glosas (abaixo).

2.3.8.2.1.2. A glosa será aplicada sobre o valor mensal unitário de cada item contratado, de forma individual e escalonada, considerando o nível de descumprimento apurado para os indicadores técnicos. Abaixo segue a tabela com os critérios para aplicação de glosas:

Descumprimento dos Indicadores (%)	Glosa Aplicada (%)
------------------------------------	--------------------

Até 15%	Não há aplicação de glosa.
>15% e ≤ 25%	2,5% (dois e meio por cento) sobre o valor mensal unitário do item contratado.
>25% e ≤ 37,5%	5,0% (cinco por cento) sobre o valor mensal unitário do item contratado.
>37,5% e ≤ 50%	7,5% (sete e meio por cento) sobre o valor mensal unitário do item contratado.
Acima de 50%	10% (dez por cento) sobre o valor mensal unitário do item contratado.

Tabela 05 – Tabela de aplicação de glosas para itens de serviço com 4 (quatro) ou mais indicadores técnicos

2.3.8.2.2. Para itens de serviço que possuam 3 (três) ou menos indicadores, o cálculo da glosa será linear, conforme as seguintes regras:

**2.3.8.2.2.1. Itens de serviço com 3 (três) indicadores:**

2.3.8.2.2.1.1. 01 (um) indicador não conforme → Glosa de 5% (cinco por cento) sobre o valor mensal do serviço impactado.

2.3.8.2.2.1.2. 02 (dois) indicadores não conformes → Glosa de 7,5% (sete e meio por cento) sobre o valor mensal do serviço impactado.

2.3.8.2.2.1.3. 03 (três) indicadores não conformes → Glosa de 10% (dez por cento) sobre o valor mensal do serviço impactado.

**2.3.8.2.2.2. Itens de serviço com 2 (dois) indicadores:**

2.3.8.2.2.2.1. 01 (um) indicador não conforme → Glosa de 5% (cinco por cento) sobre o valor mensal do serviço impactado.

2.3.8.2.2.2.2. 02 (dois) indicadores não conformes → Glosa de 10% (dez por cento) sobre o valor mensal do serviço impactado.

**2.3.8.2.2.3. Itens de serviço com apenas 1 indicador:**

2.3.8.2.2.3.1. 01 (um) indicador não conforme → Glosa de 10% (dez por cento) sobre o valor mensal do serviço impactado.

**2.3.8.3. Regras gerais para aplicação das glosas**

2.3.8.3.1. A glosa será aplicada mensalmente, com base na média das medições dos indicadores do serviço avaliado.

2.3.8.3.2. O limite máximo de aplicação será de 10% sobre o valor mensal do serviço afetado, ainda que ocorram múltiplas infrações no mesmo mês.

2.3.8.3.3. Caso um único evento resulte no descumprimento de múltiplos indicadores, como NMS e indisponibilidade do serviço, por exemplo, cada descumprimento será contabilizado separadamente para a aplicação de glosas, garantindo que todos os impactos sejam considerados.

2.3.8.3.4. A CONTRATADA não poderá compensar descumprimentos de um serviço com desempenhos positivos de outro.

2.3.8.3.5. A contabilização do índice de descumprimento será realizada com base exclusivamente nos indicadores que apresentarem medições válidas no período avaliado.

2.3.8.3.5.1. Indicadores que, por qualquer motivo, não tiverem medições disponíveis no período não serão considerados para o cálculo da glosa.

2.3.8.3.5.2. A aplicação da glosa será proporcional aos indicadores efetivamente monitorados e mensurados, garantindo que o cálculo reflita os resultados apurados.

2.3.8.3.6. As glosas deverão ser aplicadas na fatura mensal, refletindo o desconto correspondente na fatura do mês subsequente ao período de medição.

2.3.8.3.7. A fatura glosada deverá ser acompanhada de um relatório detalhado, contendo os cálculos e os indicadores que resultaram na aplicação da glosa.

2.3.8.3.8. Os valores decorrentes das glosas deverão ser abatidos na fatura do mês subsequente à ocorrência do evento, sem prejuízo da aplicação de penalidades adicionais previstas no contrato.

2.3.8.3.9. A CONTRATADA poderá apresentar justificativa formal para contestação de glosa, que será avaliada pela ATI e/ou Comissão de Auditoria.

2.3.8.3.10. Anualmente os indicadores poderão ser revistos e reeditados se for de comum acordo entre ATI/SAD e CONTRATADA.

2.3.8.3.11. Omissão, falha ou manipulação de dados nas medições serão considerados descumprimento contratual grave, passível de sanções adicionais conforme previsto no contrato.

2.3.8.3.12. A não entrega dos relatórios mensais detalhados implicará em descumprimento contratual, sujeitando a CONTRATADA a penalidades previstas no contrato.

## 2.3.9. Indicador de Qualidade de Serviço de Conectividade (IQSCON )

2.3.9.1. Os serviços de conectividade contratados para o ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL (LOTE 01) e ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER (LOTE 02) serão avaliados de acordo com os seguintes indicadores técnicos, que determinarão a qualidade da prestação do serviço:

Acrônimo	Indicador	Descrição
IND <sub>C1</sub>	Latência	Mede o tempo médio de transmissão bidirecional de pacotes de dados.
IND <sub>C2</sub>	Jitter	Mede a variação na latência da conexão.
IND <sub>C3</sub>	Perda de Pacotes	Mede a capacidade da rede em entregar pacotes ao destino final.
IND <sub>C4</sub>	Disponibilidade	Mede o percentual de tempo em que o serviço esteve operacional.
IND <sub>C5</sub>	Cumprimento de Prazo	Mede a conformidade da CONTRATADA nos prazos de instalação, reparos e mudanças de endereço.
IND <sub>C6</sub>	Cumprimento da Velocidade de download e upload	Mede se os valores contratados de volume de dados transmitidos por segundo de download e upload foram atendidos.

Tabela 06 – Indicadores do serviço de conectividade

Nota: Os valores mínimos de serviço (NMS) por tipo de conectividade estão especificados na Tabela 07 de Níveis Mínimos por Serviço e Tipo de Acesso (abaixo).

2.3.9.2. Para fins de composição do IQS<sub>CON</sub>, seguem os Níveis mínimos por serviço (NMS) para os serviços de Conectividade exigidos no projeto (LOTE 01 e LOTE 02) e serão referência para os cálculos do IQS.

#### 2.3.9.2.1. LOTE 01

Parâmetro Técnico	LA						
	LAP		LAT/ LME				
	Banda Larga (LBL)	Dedicado (LD)	Banda Larga	Dedicado	5G FWA	LEO (Satélite)	MEO (Satélite)
Latência Máxima	80 ms	50 ms	80 ms	50 ms	30 ms	100 ms	270 ms
Jitter Máximo	40 ms	5 ms	40 ms	5 ms	5 ms	20 ms	30 ms
Perda de Pacotes	≤ 2%	≤ 0,5%	≤ 2%	≤ 0,5%	≤ 0,5%	≤ 1%	≤ 1,5%
Disponibilidade	≥ 98%	≥ 99,5%	≥ 98%	≥ 99,5%	≥ 98,5%	≥ 98,5%	≥ 98,5%
Cumprimento de Prazo	Tabela Limites de Tempos para Correções de Falhas						
Garantia de Banda (Down-load)	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	80% da contratada	80% da contratada	80% da contratada
Garantia de Banda (Upload)	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	80% da contratada	10% da contratada	10% da contratada

Tabela 07 - Tabela de Níveis Mínimos por Serviço e Tipo de Acesso LOTE 01

#### 2.3.9.2.2. LOTE 02

Acrônimo Indicador	INDICADORES	SERVIÇOS DE CONECTIVIDADE	
		LIT	LPL
IND <sub>C1</sub>	Latência (ms)	≤ 40ms	≤ 5ms
IND <sub>C2</sub>	Jitter (ms)	≤ 2 ms	≤ 2 ms
IND <sub>C3</sub>	Perda de Pacotes (%)	≤ 1%	≤ 1%
IND <sub>C4</sub>	Disponibilidade (%)	≥99,7	≥99,7
IND <sub>C5</sub>	Cumprimento de Prazo	Tabela Limites de Tempos para Correções de Falhas	
IND <sub>C6</sub>	Garantia de Banda	100% da contratada	100% da contratada

Tabela 08 - Tabela de Níveis Mínimos por Serviço e Tipo de Acesso LOTE 02

#### 2.3.9.3. Exemplo Didático de Aplicação de Glosa

➤ Considere um serviço de conectividade com 6 indicadores técnicos e um circuito contratado que apresenta os seguintes resultados ao final do período de avaliação

- IND<sub>C1</sub> - Latência: Cumpriu a meta ☒
- IND<sub>C2</sub> - Jitter: Cumpriu a meta ☒
- IND<sub>C3</sub> - Perda de Pacotes: Não cumpriu ✗
- IND<sub>C4</sub> - Disponibilidade: Cumpriu a meta ☒
- IND<sub>C5</sub> - Cumprimento de Prazos: Não cumpriu ✗
- IND<sub>C6</sub> - Velocidade de Download e Upload: Cumpriu a meta ☒

#### ➤ Cálculo do Percentual de Descumprimento

- Indicadores descumpridos: 2 de 6
- Percentual de Descumprimento = (Quantidade de Indicadores não cumpridos/ Total de indicadores do serviço) x 100

$$\text{Percentual de Descumprimento} = (2/6) \times 100 = 33,33\%$$

- Aplicação da Glosa:

De acordo com a tabela de glosas, 33,33% de descumprimento se enquadra na faixa de ">25% e ≤ 37,5%", resultando em uma glosa de 5,0% sobre o valor mensal unitário do circuito contratado.

### 2.3.10. Indicador de Qualidade de Serviço de Ponto de Voz Fixo (IQS<sub>voz</sub>)

2.3.10.1. Os indicadores de composição do IQS<sub>voz</sub>, deverão ser avaliados de acordo com os seguintes indicadores técnicos e Níveis mínimos por serviço (NMS) para os serviços de Comunicação Unificada (ADENDO XII), PVF e Tráfego Extrarrede Reverso (ADENDO XIII) e Contact Center (ADENDO XIV), que determinarão a qualidade da prestação do serviço:

ACRÔNIMO	INDICADOR	DESCRIÇÃO	NMS
INDV1	Latência (ms)	Mede o tempo médio de transmissão bidirecional de pacotes enviados a partir do serviço de voz, conectado na rede WIFI para o PVF, com destino ao datacenter de voz.	≤ 100ms
INDV2	Jitter (ms)	Mede a variação na latência de pacotes enviados a partir do serviço de voz, conectado na rede WIFI para o PVF, com destino ao datacenter de voz.	≤ 20 ms
INDV3	Perda de Pacotes (%)	Mede a incapacidade da rede em entregar pacotes trafegados entre o serviço de voz, conectado na rede WIFI, e o datacenter de voz.	≤ 0,5%
INDV4	Disponibilidade (%)	Mede o percentual de tempo em que o serviço de voz esteve operacional.	Contact Center, Serviço de Cloud <sup>(*)</sup> e T. Extrarrede: ≥99,9% UC: ≥99,5% PVF: ≥98,5%
INDV5	Cumprimento de Prazo	Mede a conformidade da CONTRATADA nos prazos de instalação, reparos e mudanças de endereço.	Conforme tabela de Limites de tempos para correções de falhas

INDV6	Reincidência de Falha	Mede a quantidade de vezes que a mesma falha ocorreu no serviço, três ou mais vezes dentro de um período de 30 dias.	≥ 3 falhas
-------	-----------------------	----------------------------------------------------------------------------------------------------------------------	------------

Tabela 09 – Indicadores do serviço de Ponto de Voz Fixo

**Nota (\*):** Em caso de indisponibilidade do serviço de Cloud, a glosa será aplicada a todas as contratações dos Contratantes Aderentes, abrangendo todos os serviços impactados, incluindo PVFs, tráfego extrarrede reverso, contact center e UC.

### 2.3.11. Índice de Qualidade de Serviço de Rede Sem Fio Interno, Externo e Temporário (IQS<sub>WIFI</sub>)

2.3.11.1. Os indicadores de composição do IQS<sub>WIFI</sub>, deverão ser avaliados de acordo com os seguintes indicadores técnicos e Níveis mínimos por serviço (NMS), que determinarão a qualidade da prestação do serviço:

ACRÔNIMO	INDICADOR	DESCRIÇÃO	NMS
INDW1	Latência na rede interna (ms)	Mede o tempo médio de transmissão bidirecional de pacotes de dados de qualquer terminal, conectado na rede WIFI, com destino ao gateway do PCS.	≤ 10ms
INDW2	Jitter (ms)	Mede a variação na latência da conexão de qualquer terminal, conectado na rede WIFI, com destino ao gateway do PCS.	≤ 5 ms
INDW3	Perda de Pacotes na rede interna (%)	Mede a capacidade da rede em entregar pacotes ao destino final de qualquer terminal, conectado na rede WIFI, com destino ao gateway do PCS.	≤ 0,5%
INDW4	Disponibilidade (%)	Mede o percentual de tempo em que o serviço esteve operacional.	≥99%
INDW5	Cumprimento de Prazo	Mede a conformidade da CONTRATADA nos prazos de instalação, reparos e mudanças de endereço.	Conforme Tabela de Limites de tempos para correções de falhas
INDW6	Reincidência de Falha	Mede a quantidade de vezes que a mesma falha ocorreu no serviço, três ou mais vezes dentro de um período de 30 dias.	≥ 3 falhas

Tabela 10 – Coeficientes de Pesos para o de Serviço de Rede Sem Fio

Nota: Os indicadores INDW1, 2 e 3 deverão ser medidos através de terminais dentro do ambiente do PCS.

### 2.3.12. Indicador de Qualidade de Serviço de Segurança (IQS<sub>SEG</sub>)

2.3.12.1. Os indicadores que compõem o IQS<sub>SEG</sub> são aplicáveis aos serviços de segurança previstos no LOTE 01 e LOTE 03. Esses indicadores serão avaliados com base em parâmetros técnicos, conforme itens de serviço listados nas tabelas abaixo, e nos Níveis Mínimos de Serviço (NMS) estabelecidos.

2.3.12.2. A aplicação de glosas será realizada sobre o item de serviço correspondente ao indicador descumprido, considerando o percentual de descumprimento especificado na Tabela de Aplicação de Glosas. A seguir, são apresentados os indicadores técnicos de segurança, com suas respectivas metas por Adendo:

#### 2.3.12.2.1. LOTE 01:

ADENDO	Indicador	Nome do Indicador	Descrição da forma de medir	Meta
ADENDO III - SEGURANÇA DE REDE LO- CAL	<b>Firewall PCS - Pequeno Porte</b> (Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - PEQUENO PORTE)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Capacidade do uso da CPU	O uso da CPU não deve atingir 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
		Capacidade do uso de Memória	O consumo de memória deve permanecer abaixo de 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
	<b>Firewall PCS - Médio Porte</b> (Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - MÉDIO PORTE)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Capacidade do uso da CPU	O uso da CPU não deve atingir 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
		Capacidade do uso de Memória	O consumo de memória deve permanecer abaixo de 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
	<b>Serviço HA - PCS</b> (Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)

		Capacidade do uso da CPU	O uso da CPU não deve atingir 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
		Capacidade do uso de Memória	O consumo de memória deve permanecer abaixo de 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
	Solução para gerenciamento de acessos à rede local - NAC	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)

Tabela 11 – Indicadores e métricas NMS do ADENDO III (SEGURANÇA DE REDE LOCAL)

ADENDO	Indicador	Nome do Indicador	Descrição da forma de medir	Meta
ADENDO VI - SEGURANÇA DE DATACENTER	Firewall Datacenter (Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Capacidade do uso da CPU	O uso da CPU não deve atingir 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
		Capacidade do uso de Memória	O consumo de memória deve permanecer abaixo de 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
	Serviço HA - Datacenter (Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em	99,90%

			relação ao tempo total disponível em um mês.	
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Capacidade do uso da CPU	O uso da CPU não deve atingir 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
		Capacidade do uso de Memória	O consumo de memória deve permanecer abaixo de 80% da capacidade operacional em intervalos consecutivos de 5 minutos, durante qualquer período de medição.	< 80%
	<b>EDR/XDR</b> (Solução de proteção, detecção e resposta para servidores - EDR)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Consumo médio de memória RAM	Indicador que mede a utilização de memória RAM pelo agente de EDR/XDR nos servidores, garantindo a disponibilidade de recursos para as aplicações core.	< 512 MB
		Consumo médio de CPU	Impacto médio do processamento do agente de EDR/XDR na CPU do servidor durante a operação normal de varredura e monitoramento.	< 5%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Percentual de dispositivos atualizados com patches de segurança	Proporção de dispositivos com patches de segurança atualizados em relação ao total	100%

Tabela 12 – Indicadores e métricas NMS do ADENDO VI - SEGURANÇA DE DATACENTER)

ADENDO	Indicador	Nome do Indicador	Descrição da forma de medir	Meta
<b>ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO</b>	<b>Gestão de ativos</b> (Solução de gerenciamento e monitoramento de ativos - ITAM)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%

		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Relatório de inventário	Prazo para entrega do relatório atualizado do inventário de ativos.	Até o 5º dia útil
	<b>Identidade de acesso</b> (Solução de gerenciamento de identidade de acesso - IAM)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Atendimento de requisições de acesso	Tempo médio para processamento e conclusão de solicitações de acesso.	2h corridas
		Percentual de senhas com conformidade de política	Proporção de senhas que atendem aos requisitos definidos na política de segurança.	100%
		Revogação de acessos	Tempo médio para processar e executar solicitações de revogação de acesso.	2h corridas
		Relatório de revisão de acessos privilegiados	Prazo para entrega do relatório da revisão periódica de usuários com acessos privilegiados.	Até o 5º dia útil
	<b>Monitoramento de alertas</b> (Solução de monitoramento e análise de eventos de segurança - SIEM)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Tempo de detecção de incidentes	Tempo médio entre a ocorrência e a detecção de incidentes.	15 minutos corridos
		Taxa máxima de falsos positivos	Percentual máximo aceitável de alertas incorretamente identificados como ameaças.	10%
	<b>Resposta a incidentes automatizada</b> (Solução de automação de resposta a incidentes de segurança - SOAR)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está	99,90%

			operacional e acessível em relação ao tempo total disponível em um mês.	
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Tempo de início da contenção incidentes	Medida a partir da média do tempo gasto para iniciar as ações de contenção após a detecção de incidentes.	20 minutos corridos
		Tempo máximo para isolar ativos comprometidos	Medida a partir da média do tempo gasto para realizar o isolamento de ativos identificados como comprometidos a partir do início da contenção de incidentes.	10 minutos corridos
		Percentual de respostas a tentativas de phishing detectadas	Proporção de tentativas de phishing que receberam resposta adequada.	100%
	<b>Guarda de LOGs</b> (Solução para guarda de LOGs)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
		Tempo máximo para recuperação de logs online	Medida a partir da média do tempo gasto para disponibilizar logs armazenados no ambiente online.	2h úteis
		Tempo máximo para recuperação de logs backup	Medida a partir da média do tempo gasto para disponibilizar logs armazenados em backup.	24h úteis
	<b>Ambiente de Testes</b> (Serviço de disponibilização de ambiente de testes)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas
		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)
	<b>Gerenciamento TI-ITSM</b> (Solução de gerenciamento de serviços de TI - ITSM)	Atendimento no Prazo	Descumprimento dos prazos máximos para execução dos serviços contratados, incluindo incidentes, ativações, mudanças operacionais ou instalações.	Conforme serviço na Tabela de Limites de Tempos para Correções de Falhas

		Disponibilidade do serviço	Indicador que mede o tempo durante o qual o serviço está operacional e acessível em relação ao tempo total disponível em um mês.	99,90%
		Reincidência	Ocorrência da mesma falha três ou mais vezes em 30 dias, independentemente do cumprimento do prazo de resolução, evidenciando correção ineficaz.	< 3 (três)

Tabela 13 – Indicadores e métricas NMS do ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO

ADENDO	Indicador	Nome do Indicador	Descrição da forma de medir	Meta
ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA	Resposta a incidentes (Serviço de resposta à incidentes de cibersegurança sob demanda)	Documentação do incidente	Prazo para documentar completamente um incidente após sua resolução.	24h corridas
	Serviço de análise de segurança de primeiro nível	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.
		Relação de Analistas Presenciais no CIISC	Percentual de analistas alocados presencialmente no ambiente do CIISC da CONTRATANTE em relação ao total de analistas contratados para o serviço, apurado mensalmente.	50%
	Grupo de Especialistas (Serviço de análise de segurança especializada)	Percentual de vulnerabilidades críticas corrigidas dentro do prazo	Proporção de vulnerabilidades críticas que foram corrigidas dentro do prazo estabelecido no plano de correção.	95%
		Campanhas mensais (campanhas de conscientização)	Quantidade mínima de campanhas de conscientização a serem realizadas por mês	mínimo 1
		Simulações de phishing (campanhas de conscientização)	Frequência de realização de simulações de phishing para teste de conscientização	trimestral
		Treinamentos (campanhas de conscientização)	Execução dos treinamentos de segurança conforme planejado	conforme cronograma
		Relatório de efetividade (campanhas de conscientização)	Frequência de entrega dos relatórios sobre a efetividade das campanhas	mensal
	Serviço de acompanhamento de reparos	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.
	Serviço de atenção especializada ao cliente	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.

	<b>Service Desk</b> (Service Desk)	Disponibilidade do serviço	Período em que o serviço de monitoramento deve estar ativo e operacional.	100%
		Tempo máximo na espera	Medida a partir da média do tempo gasto por um usuário aguardando antes de ser atendido.	60 segundos
		Taxa máxima de abandono	Percentual máximo aceitável de chamadas abandonadas pelos usuários.	5%
		Resolução em primeiro contato	Percentual de casos resolvidos durante o primeiro contato com o usuário.	75%
		Satisfação do usuário	Percentual de avaliações positivas recebidas dos usuários após atendimento.	85% positivo
	Serviço de operação da rede	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.
	<b>Qualidade do serviço</b> (Serviço de análise de qualidade)	Turnover máximo da equipe	Taxa máxima aceitável de rotatividade da equipe no período de um ano contabilizado a partir do momento da assinatura do contrato.	15% anual
		Relatórios de serviço mensal	Medida a partir da média do tempo gasto para entrega do relatório mensal de serviços	até o 5º dia útil
		Certificações da equipe	Percentual da equipe que deve manter as certificações exigidas.	100% conforme exigido
	Serviço de Coordenação do CIISC	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.
		Presença de Liderança no CIISC	Quantidade mínima de profissionais com função de liderança ou coordenação presentes fisicamente no ambiente do CIISC da CONTRATANTE durante o horário de funcionamento definido pela ATI,	2 profissionais
	Núcleo de Redes e Segurança Setorial	Acionamentos Mal Sucedidos	Mede a ausência de resposta da CONTRATADA aos acionamentos da ATI, quando todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, conforme evidenciado por chamado registrado no Service-Desk.	Será tolerado apenas um acionamento mal sucedido por mês.

Tabela 14 – Indicadores e métricas NMS do ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA

**Nota 1: Indicador: Acionamentos Mal Sucedidos**

➤ **Descrição da Forma de Medir**

Mede a efetividade do atendimento da CONTRATADA aos acionamentos realizados pela ATI, com base na Matriz de Comunicação estabelecida entre ambas as partes.

Será considerado um acionamento mal sucedido sempre que todas as tentativas de contato listadas na Matriz de Comunicação não forem atendidas, sendo a ocorrência formalmente registrada pela ATI por meio de chamado no Service-Desk.

A caracterização do acionamento mal sucedido será feita pela ATI por meio da abertura de chamado no Service-Desk, evidenciando as ligações não atendidas em toda a escala de recorrência prevista na Matriz de Comunicação.

#### ➤ Regras e Estrutura da Matriz de Comunicação

- A Matriz de Comunicação deverá conter, no mínimo, três contatos distintos para cada item de serviço contratado.
- Os contatos poderão ser repetidos entre diferentes serviços, mas não poderá ser utilizado o número do Help-Desk da Operação como contato primário.
- Todos os contatos informados deverão possuir canais ativos de comunicação (telefone, celular e e-mail corporativo) e estar disponíveis conforme o regime de atendimento do serviço.
- O tempo máximo de resposta deverá ser imediato para serviços críticos e conforme escala de atendimento para os demais serviços.

#### ➤ Meta

Será tolerado apenas **um acionamento mal sucedido por mês**. A partir do segundo evento no mesmo período, será aplicada glosa.

#### 2.3.12.2.2. LOTE 03

ADENDO	Indicador	Nome do Indicador	Descrição da forma de medir	Meta
ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS	Vulnerabilidades (Serviço de gestão de vulnerabilidades)	Cobertura mensal	Percentual de ativos que devem ser verificados mensalmente quanto a vulnerabilidades.	100%
		Relatório de vulnerabilidades	Prazo para entrega do relatório da gestão de vulnerabilidades mensal.	Até o 5º dia útil
		Verificação de correções críticas	Medida a partir da média do tempo gasto para verificar a efetividade das correções implementadas após a aplicação das correções.	72h corridas
	Forense (Serviço de análise forense)	Tempo de acionamento para análise forense	Medida a partir da média do tempo gasto para iniciar as atividades de análise forense após solicitação.	1h útil
		Percentual de evidências forenses preservadas	Proporção de evidências que mantêm sua integridade durante a análise forense.	100%
		Relatório de análise forense	Medida a partir da média do tempo gasto médio para entregar o relatório após a conclusão da análise.	48h corridas
	Teste de Intrusão (Serviço de testes de intrusão (Pentest))	Execução	Realização dos testes de intrusão conforme planejamento aprovado	conforme cronograma aprovado
		Entrega de relatório	Medida a partir da média do tempo gasto para entrega do relatório detalhado após conclusão dos testes	até 5 dias úteis após conclusão
		Apresentação executiva	Medida a partir da média do tempo gasto entre a conclusão dos testes e realizar apresentação dos resultados para a equipe executiva	até 10 dias úteis após conclusão

		Retest de correções	Medida a partir da média do tempo gasto para realizar novos testes após implementação das correções	até 30 dias após correções
	Serviço de análise de segurança ofensiva (Red Team)	Cobertura dos testes	Medida a partir do percentual de vetores de ataque testados em relação ao total planejado	100%
		Relatório de testes	Medida a partir da média do tempo gasto médio para entregar o relatório de testes mensal.	Até o 5º dia útil

Tabela 15 – Indicadores e métricas NMS do ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS

### 2.3.13. Metodologia de Medição

#### 2.3.13.1. Objetivo

2.3.13.1.1. A CONTRATADA deverá utilizar uma metodologia padronizada e auditável para medição contínua dos parâmetros técnicos de desempenho e qualidade especificados neste Adendo. Os testes deverão ser conduzidos de forma sistemática, garantindo medições representativas e coerentes com a experiência real dos usuários da Nova Rede Corporativa.

#### 2.3.13.1.2. Normas e Padrões Aplicáveis

2.3.13.1.2.1. As medições deverão seguir os seguintes padrões técnicos reconhecidos:

2.3.13.1.2.1.1. RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) – Para validação inicial do serviço antes da ativação de cada link.

2.3.13.1.2.1.2. RFC 6349 (Framework for TCP Throughput Testing) – Para medições regulares de desempenho, garantindo que os testes sejam não-invasivos e representem a experiência real do usuário.

2.3.13.1.2.1.3. Resolução nº 717/2019 da Anatel – Como base regulatória para parâmetros de qualidade.

#### 2.3.13.2. Ferramenta de Medição

2.3.13.2.1. As medições deverão ser realizadas por meio do SIMET (Sistema de Medição de Tráfego Internet do NIC.br), plataforma nacionalmente reconhecida para testes de qualidade da conexão à Internet. O SIMET oferece um ambiente independente, padronizado e auditável, permitindo a verificação de parâmetros como:

2.3.13.2.1.1. Velocidade de Download e Upload (conforme garantia contratual);

2.3.13.2.1.2. Latência e Jitter;

2.3.13.2.1.3. Perda de Pacotes;

2.3.13.2.1.4. Disponibilidade do Serviço;

2.3.13.2.1.5. Outros indicadores relevantes à operação dos serviços contratados.

2.3.13.2.2. A CONTRATADA poderá utilizar ferramentas complementares para medições internas, desde que justifique tecnicamente a necessidade, assegure a equivalência metodológica em relação ao SIMET e obtenha a aprovação formal da ATI para utilização.

#### 2.3.13.3. Infraestrutura para Testes

2.3.13.3.1. Alocação e Configuração dos Servidores de Medição

2.3.13.3.1.1. A CONTRATADA deverá disponibilizar e configurar um ou mais servidores dedicados para a realização dos testes, garantindo:

2.3.13.3.1.1.1. Alocação do(s) servidor(es) de medição na infraestrutura da solução em nuvem/datacenter da Nova Rede Corporativa, garantindo conectividade otimizada com os Pontos Conectados Seguros (PCSs);

2.3.13.3.1.1.2. Capacidade de processamento suficiente para suportar as medições simultâneas realizadas em múltiplos pontos da rede;

2.3.13.3.1.1.3. Utilização de endereços IP públicos e roteáveis para evitar interferências de NATs ou firewalls no processo de medição.

2.3.13.3.1.2. Caso seja necessário mais de um servidor de medição, a CONTRATADA deverá justificar a necessidade técnica e demonstrar que a distribuição dos servidores otimizará a confiabilidade das medições, garantindo representatividade das amostragens.

### **2.3.13.3.2. Definição dos Pontos de Medição**

2.3.13.3.2.1. A CONTRATADA deverá realizar os testes entre cada PCS ativo e o servidor de medição na infraestrutura de nuvem/datacenter da Nova Rede Corporativa, garantindo que todas as localidades atendidas tenham suas conexões avaliadas. Além disso, para análise complementar da qualidade dos serviços e interconexões, a CONTRATANTE poderá solicitar testes adicionais entre os PCSs e:

2.3.13.3.2.1.1. Os principais Pontos de Troca de Tráfego (PTT) e backbones nacionais, validando a qualidade da interconexão com a Internet;

2.3.13.3.2.1.2. Os servidores de serviços críticos da Administração Pública, aferindo a qualidade da conexão com aplicações governamentais essenciais.

2.3.13.3.2.1.3. Os testes nos itens imediatamente acima não serão obrigatórios para aferição dos links de acesso, mas poderão ser requisitados a qualquer momento pela CONTRATANTE como parte do processo de auditoria e monitoramento avançado da Nova Rede Corporativa.

### **2.3.13.4. Critérios das Medições**

2.3.13.4.1. As medições deverão ser realizadas de forma automática, contínua e representativa de cada um dos indicadores técnicos, obedecendo os seguintes critérios:

2.3.13.4.1.1. As medições deverão ser coletadas diariamente, em intervalos de um minuto, durante o período correspondente ao regime de manutenção contratado pelo CONTRATANTE ADERENTE (12h x 5 dias, 12h x 7 dias ou 24h x 7 dias).

2.3.13.4.1.2. O ciclo de avaliação será mensal, considerando a média de todas as medições realizadas dentro do período;

2.3.13.4.1.3. A consolidação do indicador será o resultado da média aritmética das medições realizadas dentro do mês para determinar se o indicador foi ou não atingido.

2.3.13.4.1.4. Os valores obtidos do indicador serão confrontados com os Níveis Mínimos de Serviço (NMS) definidos neste Termo de Referência.

2.3.13.4.1.5. A CONTRATADA deverá consolidar os dados obtidos em relatórios semanais e mensais, fornecendo uma visão clara da qualidade do serviço e destacando quaisquer anomalias detectadas durante o período de medição.

### **2.3.13.5. Registro e Acompanhamento dos Resultados**

2.3.13.5.1. A CONTRATADA deverá armazenar e disponibilizar todos os resultados das medições durante todo o período contratual, respeitando um prazo mínimo de 48 meses, garantindo:

2.3.13.5.1.1. O armazenamento dos dados deve seguir a estratégia de armazenamento em camadas (tiered storage), sendo obrigatória a manutenção dos registros das bases em armazenamento online para os últimos 12 meses e em armazenamento offline para o restante do período, garantindo a integridade, segurança e disponibilidade para consultar.

2.3.13.5.1.2. Os dados poderão ser compactados para periodicidade de 5 minutos após 30 dias da data de sua coleta.

2.3.13.5.1.3. O fornecimento, sem ônus para a CONTRATANTE, cópia integral e atualizada de todas as bases de dados e informações armazenadas pelos sistemas, a qualquer tempo (quando solicitado pela ATI ou Comissão de Auditoria) ou no caso de rescisão\ término do contrato.

2.3.13.5.1.4. Os relatórios detalhados, auditáveis e exportáveis (formatos CSV, JSON, XML), permitindo análises e correlação de eventos;

2.3.13.5.1.5. A possibilidade de consulta histórica dos resultados, assegurando rastreabilidade e transparência no cumprimento dos NMSs;

### 3. Limites de Tempos para Correções de Falhas

3.1. A CONTRATADA deverá atender aos NMS's elencados na tabela abaixo, de LIMITES DE TEMPOS PARA CORREÇÕES DE FALHAS, onde apresentamos os itens de serviços descritos neste Termo da nova Rede, com seus níveis e limites de tempos de recuperação, para medição de NMS nos casos de falhas, referentes aos serviços contratados e em uso.

3.1.1. De acordo com as definições de Níveis Mínimos de Serviço e do índice IQS, os limites abaixo compõem o indicador de Cumprimento de Prazo e desta forma o descumprimento é passível de aplicações de glosas.

LIMITES DE TEMPOS PARA CORREÇÕES DE FALHAS			
LOTE 01			
Seq.	Descrição do Serviço	Regime de Manutenção (horas x dias)	Limite de Tempo de Recuperação (horas corridas)
ADENDO III - SEGURANÇA DE REDE LOCAL			
1	Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha - Tipo 1 e Tipo 2 <sup>(3)</sup>	12 x 5 (Padrão) ou regime contratado para o PCS	Região Metropolitana : Até 4 horas Polos do Interior <sup>(1)</sup> : Até 4 horas Demais Localidades <sup>(2)</sup> : Até 8 horas
2	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço <sup>(3)</sup>		
3	Solução para gerenciamento de acessos à rede local - NAC		
ADENDO IV - SERVIÇO DE REDE SEM FIO			
4	Serviço de Rede Sem Fio Interno e Externo com Segurança (O tempo de manutenção do Ser-	12 x 5 (Padrão) ou regime contratado para o PCS	Região Metropolitana : Até 4 horas Polos do Interior <sup>(1)</sup> :

	viço de fornecimento e implantação de Switch está inserido neste item)		Até 4 horas Demais Localidades <sup>(2)</sup> : Até 8 horas
5	Serviço de Rede Sem Fio Temporário com Segurança	24 x 7	
ADENDO V - SERVIÇO DE CONECTIVIDADE DE REDE LOCAL			
6	Link de Acesso Permanente (LAP) - Tipo 1 e Tipo 2 <sup>(3)</sup>	12 x 5 (Padrão) ou regime contratado para o PCS	Região Metropolitana : Até 4 horas Polos do Interior <sup>(1)</sup> : Até 4 horas Demais Localidades <sup>(2)</sup> : Até 8 horas
7	Link Multitecnologia Especial (LME) - Tipo 1, Tipo 2 e Tipo 3 <sup>(3)</sup>		
8	Link Acesso Temporário (LAT) - Tipo 1, Tipo 2 e Tipo 3 <sup>(3)</sup>	24 x 7	
ADENDO VI - SEGURANÇA DE DATACENTER			
9	Serviço de fornecimento e implantação de Solução unificada de segurança de rede - DATACENTER	24 x 7	Até 2 horas
10	Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para DATACENTER com fornecimento dos equipamentos necessários para ativação do serviço		
11	Solução de segurança de confiança zero - ZTNA		
12	Solução de proteção, detecção e resposta para servidores - EDR		
13	Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR		
14	Solução para gerenciamento de acessos à rede datacenter - NAC		
15	Solução de segurança de identidade privilegiada - PAM		
16	Solução de filtro de mensagens indesejadas - ANTISPAM		
17	Solução de Filtro de Aplicações WEB - WAF		
ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO			
18	Solução de gerenciamento e monitoramento de ativos - ITAM	24 x 7	Até 2 horas
19	Solução de gerenciamento de identidade de acesso - IAM		
20	Solução de monitoramento e análise de eventos de segurança - SI-		

	EM		
21	Solução de automação de resposta a incidentes de segurança - SO-AR		
22	Solução para guarda de LOGs		
23	Serviço de disponibilização de ambiente de testes		
24	Solução de gerenciamento de serviços de TI - ITSM		
<b>ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA</b>			
25	Serviço de resposta à incidentes de cibersegurança sob demanda		
26	Serviço de análise de segurança de primeiro nível		
27	Serviço de análise de segurança especializada		
28	Serviço de acompanhamento de reparos		
29	Serviço de atenção especializada ao cliente		
30	Service Desk	24x7	Até 2 horas
31	Serviço de operação da rede		
32	Serviço de análise de qualidade		
33	Serviço de Coordenação do CIISC		
34	Núcleo de Redes e Segurança Setorial		
35	Serviço adicional de Monitoramento do Núcleo de Redes e Segurança Setorial (pacotes 50 PCSs)		
36	Serviço de Evolução da Maturidade em Segurança da Informação		
<b>ADENDO XII - SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)</b>			
37	Serviço de Comunicação Unificada - SCU (Conta de usuário)	24x7	Até 2 horas
<b>ADENDO XIII – SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE</b>			
38	Serviço de Ponto de Voz Fixo com aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL)		
39	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP Mesa TIPO I)	12 x 5 (Padrão) ou	Até 8 horas
40	Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP Mesa TIPO II)	regime contratado para o PCS	
41	Serviço de Ponto de Voz Fixo com		

	Aparelho de Voz DECT IP (PVF-DECT IP)		
42	Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE)		
43	Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual)		
44	Serviço Headset sem fio (PVF-sem fio Fone de Cabeça)		
45	Serviço PVF-Fone-de-Cabeça		
46	Serviço Tráfego Telefônico Extra-rede Reverso, do tipo DISCAGEM DIRETA GRATUITA (DDG)	24x7	Até 2 horas
47	Serviço Adicional de Acesso SIP (SIP TRUNK)	12 x 5 (Padrão) ou regime contratado para o PCS	Região Metropolitana : Até 4 horas Polos do Interior (1): Até 4 horas Demais Localidades(2): Até 8 horas
<b>ADENDO XIV - SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER</b>			
48	Serviço de Contact Center com Recurso de Voz		
49	Serviço de Contact Center com recurso de Whatsapp		
50	Serviço de Contact Center com recurso de Redes Sociais		
51	Serviço de Unidade de Resposta Audível (Porta de URA)		
52	Serviço de Comunicação por vídeo ou vídeo-chamada		
53	Serviço de Automatizações e Integrações - Consultoria Inicial		
54	Serviço de Automatizações e Integrações - Implantação		
55	Serviço de interface de tronco SIP (SIP TRUNK)		

Tabela 16 – LIMITES DE TEMPOS PARA CORREÇÕES DE FALHAS – LOTE 01

**Nota (1):** As 15 cidades consideradas como **Polos do Interior** deverão obedecer a um Limite de Tempo de Recuperação máximo de 4 horas, por serem estratégicas e concentrarem um maior número de Pontos Conectados Seguros (PCSs). As cidades classificadas como polos são: Afogados da Ingazeira, Araripina, Arcoverde, Cabrobó, Carpina, Caruaru, Garanhuns, Ouricuri, Palmares, Pesqueira, Petrolândia, Petrolina, Salgueiro, Serra Talhada e Vitória de Santo Antão.

Adicionalmente, as cidades que atualmente compõem a Região Metropolitana do Recife (RMR), contemplando um conjunto estratégico de 15 municípios, são: Abreu e Lima, Araçoiaba, Cabo de Santo Agostinho, Camaragibe, Goiana, Igarassu, Ilha de Itamaracá, Ipojuca, Itapissuma, Jaboatão dos Guararapes, Moreno, Olinda, Paulista, Recife e São Lourenço da Mata.

Fonte: <https://www.pdui-rmr.pe.gov.br/RMR>

**Nota (2):** Os municípios que não pertencem à **Região Metropolitana do Recife (RMR)** nem estão classificados como **Polos do Interior** serão denominados “**Demais Localidades**” e terão um Limite de Tempo de Recuperação máximo de 8 horas.

**Exceção:** O **Distrito de Fernando de Noronha** terá um **acréscimo de 14 horas** ao tempo estabelecido para as Demais Localidades, totalizando um tempo máximo de recuperação de 22 horas.

**Nota (3):** Caso a CONTRATADA realize um diagnóstico incorreto do incidente, como abrir um chamado para falha no acesso e, posteriormente, constatar que a falha era no firewall, o tempo total de correção será contabilizado de forma única para todos os serviços impactados, evitando a fragmentação indevida do tempo de reparo e garantindo a correta mensuração do tempo de indisponibilidade.

Para os seguintes itens de serviço, onde há uma relação intrínseca de funcionamento entre a Solução Unificada de Segurança (firewall) e o Link de Acesso (LAP, LME e LAT), o tempo de falha contabilizado na Tabela de Limites de Tempos para Correções de Falhas será considerado como um tempo único de correção, evitando segmentação indevida do troubleshooting:

- Serviço de fornecimento e implantação de Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 e Tipo 2;
- Serviço de configuração das Soluções Unificadas de Segurança em Alta Disponibilidade (HA), com fornecimento dos equipamentos necessários para ativação do serviço;
- Link de Acesso Permanente (LAP) – Tipo 1 e Tipo 2;
- Link Multitecnologia Especial (LME) – Tipo 1, Tipo 2 e Tipo 3;
- Link de Acesso Temporário (LAT) – Tipo 1, Tipo 2 e Tipo 3.

Para efeitos de glosa, caso o tempo total ultrapasse o limite estabelecido para correção da falha, a penalização será aplicada a todos os itens de serviço envolvidos no incidente, garantindo que o impacto do erro de identificação seja refletido proporcionalmente no contrato.

LOTE 02			
Seq.	Descrição do Serviço	Regime de Manutenção (horas x dias)	Limites do tempo de Entrega (dias corridos)
ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER			
1	Link de Fibra Lan To Lan 100GB (L2L)	24x7	Até 2 horas
2	Link para Data Center de 2GB, 4GB, 6GB, 8GB e 10 GB com AntiDDoS - Link Internet Trânsito (LIT)		

Tabela 17 – LIMITES DE TEMPOS PARA CORREÇÕES DE FALHAS – LOTE 02

3.2. O tempo de restabelecimento é contabilizado dentro do período definido para o Regime de Manutenção.

3.3. O tempo de restabelecimento do item de serviço é contado a partir da abertura do chamado, seja ele proativo e/ou reativo, para o Centro Integrado de Inteligência e Segurança Cibernética.

3.4. O início do atendimento técnico, referente à abertura do chamado será realizado de forma remota. Caso o atendimento remoto não seja efetivo na resolução dos chamados, a CONTRATADA deverá encaminhar um técnico para prestação de suporte local (on site), sem custos adicionais.

3.5. O prazo de restabelecimento da prestação dos serviços depende do Nível Mínimo de Serviço especificado para cada serviço, e será contado o seu tempo, a partir da abertura do chamado, seja ele proativo e/ou reativo.

3.6. O chamado permanecerá aberto, contando o tempo para medição dos Níveis Mínimos de Serviço, até que a CONTRATADA solucione o incidente, providencie o encerramento do chamado, homologação pelo serviço do Centro Integrado de Inteligência e Segurança Cibernética e o aceite do CONTRATANTE aderente.

3.7. A CONTRATADA deverá disponibilizar, a qualquer tempo, informações ao CONTRATANTE, ATI, SAD, Comissão de Auditoria e Verificador independente, sobre a situação de atendimento do chamado técnico, o diagnóstico, as providências adotadas e/ou implementadas e a data e hora da solução do incidente.

#### 4. Limites de Tempos para Execução de Solicitações de Serviços

4.1. A realização de atividades específicas inerentes aos serviços já instalados e prestados na Nova Rede Corporativa, poderá ser solicitada pelos Contratantes Aderentes através de abertura de chamados técnicos no serviço da Operação CIISC. Na tabela abaixo, de LIMITES DE TEMPOS PARA EXECUÇÃO DE SOLICITAÇÕES DE SERVIÇOS, apresentamos os itens de serviço com as atividades a serem medidas e os prazos de atendimento das demandas para a CONTRATADA. A glosa no faturamento pelo não atendimento da solicitação desses serviços no prazo estabelecido é de 1,50% (um e meio por cento) por dia de atraso, para cada serviço correspondente:

#### LIMITES DE TEMPOS PARA EXECUÇÃO DE SOLICITAÇÕES DE SERVIÇOS

##### LOTE 01

seq	Item de Serviço	Atividade para Medição	Limites do tempo de Solicitação de Serviços (dias ou horas corridas)
1	Serviço de Segurança da Rede	Relatório de Segurança.	Até 3 dias
2		Relatório de Ataque.	Até 3 dias
3		Disponibilização de logs dos dispositivos ou serviços da Rede armazenados de forma online ou offline.	Online até 2h úteis Offline até 24h úteis
4	Solução unificada de Segurança de Rede	Configuração	Até 1 dia
5		Configurações de controle de acesso	Até 2 horas
6		Relatório Gerais (tráfego, gerencial, operacional entre outros)	Até 3 dias
7	Serviço de Núcleo de Redes e Segurança Setorial	Configuração	Até 2 dias
8	Serviço de Operação da Rede	Atualização da documentação do Sistema de Gestão de Ordem de Serviço (SGOS). A documentação descreve requisitos ou modelagem do banco de dados ou diagrama de classes ou diagrama de sequências ou de testes	Até 15 dias para cada tipo de documentação

9		Alteração do código SGOS que não envolve modificação de banco de dados e fluxo. Esta só será solicitada após possuir a solicitação da documentação atual do sistema e documentação que prevê as mudanças	Até 5 dias
10		Alteração do código SGOS que envolve mudança no banco de dados e/ou fluxo.	Até 60 dias
11		Alteração do código SGOS que envolve alteração no fluxo.	
12		Alterações no banco de dados. Esta só será solicitada após possuir a solicitação da documentação atual do sistema e documentação que prevê as mudanças	
13		Relatório de análise de desempenho do SGOS	Até 3 dias
14		Relatórios gerenciais	Até 2 dias por tipo de relatório
15	Serviços de Links de Acesso (LAP e LME)	Configuração	Até 1 dia
16	Serviços de Link de Acesso LAT	Configuração	Até 1 dia
17	Serviço de Rede Sem Fio Interno e Externo	Configuração	Até 1 dia
18	Serviço de Rede Sem Fio Temporário	Configuração	Até 1 dia
19	Serviço de Comunicação Unificada - SCU (Conta de usuário)	Configuração	Até 1 dia
20	Serviço Adicional de Acesso SIP (SIP TRUNK)	Configuração	Até 1 dia
21	Todos tipos de Pontos de Voz Fixos (PVF)	Configuração e mudança de categoria	Até 1 dia para cada 100 PVFs solicitados.
22		Mudança de local dentro do estabelecimento.	Até 7 dias para cada 30 PVFs solicitados.
23	Serviço do tipo Discagem Direta Gratuita (DDG) - 0800	Cadastrar ou alterar quantidade de PVFs participantes do grupo 0800	Até 2 dias
24	Serviço de Infraestrutura de Voz para Contact Center	Gravação e ativação de mensagens personalizadas, para cada conjunto de até 10 (dez) mensagens.	Até 5 dias
25		Configuração, para cada conjunto de até 05 (cinco) itens de configuração	Até 2 dias
26	Serviço de Infraestrutura de Voz para Contact Center (Curadoria)	Solicitações de atualizações e melhorias necessárias aplicadas ao sistema	Até 2 dias
27	Serviços de correções de fatura	Solicitação de Retificação/correção de fatura(s) mensal apresentada(s) com erro(s) ou cobrança indevida.	Até 30 dias

Tabela 18 – Limites de Tempos para Execução de Solicitações de Serviços

LOTE 02			
seq	Item de Serviço	Atividade para Medição	Limites do tempo de Solicitação de Serviços
1	Serviços L2L e LIT	Configurações	Até 1 dia
2		Disponibilização de ponto de espelhamento de tráfego para análise.	Até 2 dias
3		Relatórios Gerais de serviços	Até 3 dias

Tabela 19 – Limites de Tempos para Execução de Solicitações de Serviços – LOTE 02

## 5. Manutenções Programadas

5.1. As manutenções programadas realizadas pela CONTRATADA que impactem parcial ou totalmente qualquer serviço contratado deverá ser previamente aprovada pelos Contratantes Aderentes afetados e comunicadas à ATI com a devida antecedência.

5.2. A CONTRATADA deverá informar à ATI e aos Contratantes Aderentes com antecedência mínima de 5 (cinco) dias corridos, detalhando:

5.2.1. Data e horário da manutenção;

5.2.2. Serviços impactados e grau de impacto previsto;

5.2.3. Medidas de mitigação adotadas para minimizar os efeitos da manutenção;

5.2.4. Justificativa técnica para a necessidade da intervenção;

5.2.5. Tempo estimado para conclusão.

5.3. A CONTRATADA não poderá realizar manutenções programadas em períodos críticos previamente definidos pela ATI e/ou pelos Contratantes Aderentes, salvo em casos emergenciais devidamente justificados e autorizados.

5.4. O período de manutenção programada não será contabilizado como indisponibilidade para fins de medição de indicadores e aplicação de glosas, desde que:

5.4.1. Tenha sido formalmente aprovado pela ATI e pelos Contratantes Aderentes afetados;

5.4.2. Tenha sido executado dentro do prazo e escopo acordado;

5.4.3. O serviço tenha sido completamente restabelecido dentro do período comunicado.

5.5. Manutenções programadas que resultem em impactos não previstos ou indisponibilidade além do período autorizado serão consideradas descumprimento contratual, sujeitando a CONTRATADA às penalidades aplicáveis, incluindo glosas e sanções previstas no contrato.

5.6. A CONTRATADA deverá manter um registro histórico de todas as manutenções programadas realizadas ao longo da vigência do contrato, disponibilizando à ATI relatórios detalhados contendo:

5.6.1. Datas e horários das intervenções;

5.6.2. Serviços impactados e duração da atividade;

5.6.3. Justificativa técnica para cada manutenção;

5.6.4. Evidências de execução e restabelecimento do serviço.

## 6. Comunicação - Relatório de Níveis Mínimos de Serviço

6.1. A CONTRATADA deverá consolidar e fornecer aos Contratantes Aderentes e à ATI relatórios detalhados sobre o cumprimento dos Níveis Mínimos de Serviço (NMS) estabelecidos no contrato. Os relatórios devem apresentar informações gerenciais e operacionais que permitam o acompanhamento da qualidade dos serviços prestados, bem como a identificação de falhas e oportunidades de melhoria.

6.2. O formato, a estrutura e a forma de entrega dos relatórios mensais serão definidos pela ATI, em conjunto com a CONTRATADA, devendo ser padronizados e auditáveis. O relatório deve conter, no mínimo, as seguintes informações:

6.2.1. Número do chamado registrado;

6.2.2. Data e hora da abertura e/ou reabertura do chamado;

6.2.3. Data e hora do início do atendimento técnico;

6.2.4. Data e hora do fechamento do chamado;

6.2.5. Descrição detalhada do problema ocorrido;

6.2.6. Classificação do chamado conforme Nível de Criticidade;

6.2.7. Descrição da solução aplicada;

6.2.8. Identificação do tempo em que o chamado ficou aguardando ação da Contratante Aderente;

6.2.9. Tempo total de paradas programadas autorizadas;

6.2.10. Tempo de Recuperação Operacional (downtime entre a falha e a normalização do serviço);

6.2.11. Tempo de disponibilidade mensal do serviço, calculado conforme critérios estabelecidos neste Termo de Referência;

6.2.12. Quantidade total de incidentes registrados, resolvidos e pendentes no período;

6.2.13. Percentual de conformidade com os Níveis Mínimos de Serviço, discriminado por item contratado;

6.2.14. Aplicação de glosas e penalidades, se houver descumprimentos contratuais;

6.2.15. Ações corretivas ou preventivas implementadas para evitar recorrências de falhas.

6.3. O relatório mensal de Níveis Mínimos de Serviço (NMS) deverá ser entregue até o quinto dia útil do mês subsequente ao período de apuração, de forma eletrônica e em formato padronizado, garantindo a rastreabilidade e a possibilidade de auditoria das informações apresentadas.

6.4. Todas as informações utilizadas na apuração dos Indicadores de Nível Mínimo de Serviço deverão ser extraídas diretamente dos sistemas de monitoramento da CONTRATADA, mantendo sua integridade e autenticidade. Os dados deverão ser apresentados tanto na sua forma original (bruta) quanto consolidados em relatórios gerenciais.

6.5. Além dos relatórios enviados para a ATI, a CONTRATADA deverá fornecer relatórios específicos para cada Contratante Aderente, contemplando exclusivamente os serviços contratados e os respectivos indicadores de desempenho.

6.6. A CONTRATADA deverá disponibilizar, para fins de auditoria, um painel de monitoramento online (dashboard), de acesso restrito aos Contratantes Aderentes, à ATI e a quem a ATI designar, contendo os principais indicadores de desempenho e a evolução histórica dos níveis de serviço, permitindo a verificação em tempo real dos dados reportados nos relatórios mensais.

6.7. O descumprimento da entrega dos relatórios mensais, a omissão de informações, bem como a apresentação de dados inconsistentes ou manipulados serão considerados infrações contratuais graves, sujeitando a CONTRATADA à aplicação de penalidades previstas no contrato.

6.8. A CONTRATADA será integralmente responsável pela geração, consolidação e disponibilização dos indicadores de desempenho e qualidade (NMS, IQS, IR e IQP), bem como de todas as evidências técnicas que subsidiem sua apuração, devendo tais informações constituir a base oficial para fins de medição contratual, aplicação de glosas e faturamento, até a eventual atuação de Verificador Independente designado pela CONTRATANTE.

### ADENDO III - SEGURANÇA DE REDE LOCAL

#### 1. Implantação, prestação dos serviços e manutenibilidade do contrato

##### 1.1. Implantação dos equipamentos e serviços de segurança:

1.1.1. A CONTRATADA deve realizar a implantação dos equipamentos que compõem o serviço de segurança de última milha seguindo o cronograma proposto para atendimento dos níveis de maturidade citados no serviço de evolução da maturidade em segurança da informação;

1.1.2. Todos os equipamentos utilizados na implantação do serviço devem ser novos, sem uso anterior, garantindo a longevidade e a eficiência da infraestrutura;

##### 1.2. Condições para renovação do contrato:

1.2.1. A cada renovação do contrato, e como condição para a renovação, a CONTRATADA deverá realizar uma análise prévia das Soluções Unificadas de Segurança de Rede, para determinar se será necessário realizar a atualização, substituindo-as por modelos mais recentes ou versões atualizadas que atendam, no mínimo, às especificações originais deste Termo de Referência e aos requisitos adicionais decorrentes do crescimento e evolução da rede ao longo do período, a ser validado pela CONTRATANTE técnica ATI;

1.2.2. Nos casos em que a análise mostrar que o equipamento está atendendo ao perfil de tráfego da localidade, essa obrigatoriedade poderá ser revogada pela comissão de auditoria;

1.2.3. Esta atualização deve assegurar a continuidade da proteção e o desempenho adequado para a infraestrutura, considerando as demandas de tráfego, ameaças cibernéticas e requisitos técnicos vigentes à época;

1.2.4. A substituição dos equipamentos deverá ser realizada sem ônus adicional para a CONTRATANTE, respeitando o cronograma previamente acordado e garantindo a mínima interrupção dos serviços;

##### 1.3. Instalação, Operação e Manutenção dos Pontos Conectados Seguros (PCS):

1.3.1. Instalar, operacionalizar e manter os serviços de Link de Acesso nos Pontos Conectados Seguros;

1.3.2. Poderão ser instalados links multitecnologias de qualquer fonte, incluindo links da REPEPE - Rede Pernambucana de Pesquisa e Educação, que atendam aos requisitos mínimos deste Termo de Referência, desde que previamente aprovados pela CONTRATANTE técnica ATI, garantindo flexibilidade e adequação às necessidades específicas da Nova Rede corporativa;

1.3.3. Prover em todo o serviço de Ponto Conectado Seguro - PCS, as funcionalidades descritas neste Termo de Referência, na solução de conectividade CPE (Customer Premises Equipment) apresentada pela CONTRATADA;

1.3.3.1. As funcionalidades devem ser gerenciadas de forma centralizada, e disponibilizadas no Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

1.3.3.2. Caso a solução ofertada não implemente nativamente todas as funcionalidades requeridas no Termo de Referência, será aceito o uso de composições com outras soluções, desde que seja garantido e comprovado o atendimento integral a todos os requisitos técnicos exigidos neste Termo de Referência, assegurando ainda a plena interoperabilidade entre os componentes da solução ofertada;

##### 1.4. Continuidade e integridade dos dados em caso de falha:

1.4.1. Em caso de soluções compostas, a CONTRATADA deve assegurar a continuidade das funcionalidades mesmo na ausência de um dos links externos. Deve ser garantida a capacidade de armazenamento local de logs e a comunicação entre produtos de diferentes fabricantes sem depender de conexão externa. Além disso, é essencial que o plano de

controle e gestão das soluções seja local e autônomo, garantindo a continuidade dos serviços que não utilizam a conexão externa preservando a integridade das operações da Nova Rede Corporativa;

1.4.2. Possuir, permitir, garantir, prover e implementar, que a solução deve assegurar o roteamento automático e transparente entre dois links ativos no CPE (Customer Premises Equipment), de forma que, em caso de falha em um dos links, o outro assuma imediatamente, mantendo o funcionamento ininterrupto da rede incluído a do Serviço de Rede Sem FIO (SRSF) e que todas as funcionalidades essenciais, como autenticação, gerenciamento de APs e controle de tráfego, devem operar de forma contínua e autônoma durante a troca de links, garantindo a estabilidade e eficiência da rede;

1.4.3. Deve ser implementado um mecanismo de segurança robusto que assegure a integridade e a confidencialidade dos dados trafegados e armazenados, mesmo em casos de interrupção de todos os links externos. Esse mecanismo deve prevenir tentativas de acesso não autorizado e garantir que todos os registros de log estejam protegidos contra manipulações ou acessos indevidos, mesmo em situações de falha ou isolamento da rede.

1.5. Prover na solução adotada, que os dispositivos de conectividade de cada PCS tenham as seguintes características:

1.5.1. A solução instalada deverá ser totalmente compatível com a largura de banda CONTRATADA dos links de banda larga, contando com todos os recursos de hardware necessários (memória, processamento, I/O e portas de comunicação) para pleno funcionamento e para o atendimento satisfatório de todo o tráfego gerado no PCS onde o link de acesso (LBL/LD/LME/LAT) estiver instalado;

1.5.1.1. A solução deverá manter desempenho adequado mesmo com todas as funcionalidades habilitadas simultaneamente, incluindo assinaturas de IPS atualizadas, políticas de segurança ativas, e gerenciamento de tráfego em protocolos como DNS, HTTP, SMTP, HTTPS, FTP, além de suportar aplicações de redes sociais, plataformas de colaboração, NAT e geração de logs;

1.5.1.2. Caso o uso de CPU e/ou memória atinja 80% da capacidade operacional em intervalos de 5 minutos, durante qualquer período de execução do contrato, a solução deverá automaticamente registrar no sistema de gerenciamento do Centro Integrado de Inteligência e Segurança Cibernética (CIISC) a quantidade de usuários ativos, throughput e conexões simultâneas ativas;

1.5.1.3. Após o registro do evento, a CONTRATADA, em parceria com o CONTRATANTE e a ATI, deverá realizar ações necessárias para substituição, atualização e/ou configuração do equipamento, sem custos adicionais para o CONTRATANTE.

1.6. Cada Link de Banda Larga deve ser disponibilizado, de forma integrada e gerenciável pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, aos serviços de voz, dados e segurança, suportados pelo protocolo TCP/IPv6;

1.7. Garantir a implantação do aumento de velocidade, quando solicitado. O aumento de velocidade se dará a partir da emissão de Ordens de Serviços pelo CONTRATANTE aderente, devidamente formalizada. A implantação será de forma transparente, isto é, sem gerar impacto, interrupções e custos adicionais de reinstalações. O serviço apenas será considerado concluído quando for formalmente validado pelo Centro Integrado de Inteligência e Segurança Cibernética, pela CONTRATANTE aderente e pela Gestão Técnica da Nova Rede – ATI, só após estes procedimentos o serviço poderá ser faturado com o novo valor da velocidade solicitada. Os recursos e equipamentos envolvidos nestes aumentos de velocidade deverão suportar as atualizações tecnológicas previstas nesta facilidade;

1.8. Atribuir para cada Link de banda larga, endereços IPv6. A relação e o gerenciamento dos IPs públicos a serem atribuídos, são da responsabilidade da ATI;

## 2. Serviço de fornecimento e implantação de Solução unificada de segurança de rede de última milha

Tabela - 1 - Especificações mínimas da solução

Item	Especificação	Solução Unificada de Segurança de Rede	
		Tipo 1	Tipo 2
1	<i>Throughput de Firewall (Gbps)*</i> *	12	24
2	Conexões simultâneas (milhões)	1.2	2.4
3	Novas conexões por segundo (mil)	90	180
4	<i>Throughput de IPSec (Gbps)**</i>	2.4	4,8
5	Proteção combinada* contra ameaças (Gbps)**	2	4
6	Qtd mínima de <i>interfaces</i> (Gbps)	4	8
7	Qtd mínima de <i>interfaces</i> (10 Gbps)	2	4
9	Quantidade de Instâncias Virtuais Licenciadas***	2	2

\* Na proteção combinada contra ameaças, a solução instalada deverá ter os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.

\*\* Será admitida variação máxima de até 10% (dez por cento) exclusivamente nos parâmetros de desempenho Throughput de Firewall, Throughput de IPSec, Proteção combinada contra ameaças. A tolerância aplica-se somente aos valores de desempenho, não sendo extensível a nenhum outro requisito funcional, arquitetural, de segurança, capacidade de hardware, protocolos suportados, integração, licenciamento ou características obrigatórias descritas neste Termo de Referência.

\*\*\* Ter, no mínimo, as instâncias virtuais definidas na tabela. Esses equipamentos devem ser disponibilizados com apenas 02 (duas) instâncias virtuais ativa, sendo as demais instâncias ativadas mediante solicitação da CONTRATANTE aderente ou da CONTRATANTE aderente Técnica (ATI).

#### 2.1. Requisitos gerais das soluções unificadas de segurança de rede:

2.1.1. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;

2.1.2. Possuir quantidade de memória e processamento suficientes para atendimento de todas as funcionalidades e desempenho, de acordo com a velocidade do Link de Acesso contratado, solicitados neste Termo de Referência;

2.1.3. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);

2.1.4. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

2.1.5. Garantir o envio dos logs para os sistemas de monitoramento do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa em tempo real;

2.1.6. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH, software cliente ou WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

2.2. Requisitos mínimos das funcionalidades de Rede e Firewall dos Pontos Conectados Seguros:

- 2.2.1. Ter tecnologia de Firewall do tipo statefull;
- 2.2.2. Ser otimizada para análise de conteúdo de aplicações em camada 7;
- 2.2.3. Permitir, para o gerenciamento da solução, interface de administração via web ou cliente próprio no próprio dispositivo integrada com bases de usuários LDAP, LDAP/AD;
- 2.2.4. Realizar VLAN com Tags padrão 802.1q;
- 2.2.5. Possuir suporte a agregação de links 802.3ad e LACP;
- 2.2.6. Realizar política baseada em roteamento (policybasedrouting) ou política baseada em encaminhamento (policybasedforwarding);
- 2.2.7. Realizar DHCP Relay e DHCP Server;
- 2.2.8. Possuir suporte a sub-interfaces ethernet lógicas;
- 2.2.9. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 2.2.10. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 2.2.11. Funcionar com tradução de porta (PAT);
- 2.2.12. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 2.2.13. Implementar e suportar NAT64 e NAT46;
- 2.2.14. Implementar NAT66, quando solicitado pela ATI ou o CONTRATANTE aderente;
- 2.2.15. Implementar o protocolo ICMP;
- 2.2.16. Implementar balanceamento de link por hash do IP de origem, como também por hash do IP de origem e destino;
- 2.2.17. Suportar o balanceamento de no mínimo três circuitos (links) simultaneamente, implementando balanceamento de carga, sendo possível definir o percentual de tráfego que será escoado por cada um dos links;
- 2.2.18. Possuir proteção contra falsificação de endereços (anti-spoofing);
- 2.2.19. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.2.20. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 2.2.21. Suportar OSPF gracefulrestart;
- 2.2.22. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.2.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 2.2.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 2.2.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 2.2.27. Possuir suporte à criação de sistemas virtuais no mesmo equipamento (appliance);
- 2.2.28. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 2.2.29. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 2.2.30. Operar durante o período de vigência do contrato para as funcionalidades de controle de aplicações, antivírus, IPS, VPN IPsec, QOS, de-criptografia SSL ou SSH, e protocolos de roteamento dinâmico;
- 2.2.31. Realizar controles de políticas por porta e protocolo;
- 2.2.32. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 2.2.33. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 2.2.34. Realizar controle de políticas por código de País;
- 2.2.35. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);

- 2.2.36. Realizar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 2.2.37. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 2.2.38. Realizar controle de inspeção e de-criptografia de SSH ou SSL por política;
- 2.2.39. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 2.2.40. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
  - 2.2.40.1. Drop sem notificação do bloqueio ao usuário;
  - 2.2.40.2. Drop com notificação do bloqueio ao usuário;
  - 2.2.40.3. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
  - 2.2.40.4. TCP-Reset para o cliente;
  - 2.2.40.5. TCP-Reset para o server ou para os dois lados da conexão.
  - 2.2.40.6. Serão aceitas outras nomenclaturas e classificações que representem as mesmas ações.
- 2.2.41. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 2.3. Requisitos mínimos da funcionalidade de controle de aplicações dos Pontos Conectados Seguros:
  - 2.3.1. Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
  - 2.3.2. Realizar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
  - 2.3.3. Reconhecer no mínimo 5.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail, entre outros;
  - 2.3.5. Inspeccionar o payload de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;
  - 2.3.6. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;
  - 2.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da deep web (ex.: rede Tor);
  - 2.3.8. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
  - 2.3.9. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
  - 2.3.10. Atualizar a base de assinaturas de aplicações automaticamente;
  - 2.3.11. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
  - 2.3.12. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
  - 2.3.13. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
  - 2.3.14. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
  - 2.3.15. Manter a segurança da rede eficiente, realizando o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
  - 2.3.16. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
  - 2.3.17. A solução deverá permitir a criação e aplicação de regras ou assinaturas personalizadas de segurança;
  - 2.3.18. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
  - 2.3.19. Permitir a configuração de alertas quando uma aplicação for bloqueada;
  - 2.3.20. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
  - 2.3.21. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a

aplicação de políticas de controle adequadas;

2.3.22. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;

2.3.23. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;

2.3.24. Possuir, permitir, garantir, realizar e implementar a diferenciação de aplicações Proxies e permitir a aplicação de políticas de controle adequadas;

2.3.25. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

2.4. Requisitos mínimos da funcionalidade de prevenção de ameaças dos Pontos Conectados Seguros:

2.4.1. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

2.4.2. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

2.4.3. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

2.4.4. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

2.4.5. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;

2.4.6. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;

2.4.7. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;

2.4.8. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);

2.4.9. Permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura;

2.4.10. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.4.11. Permitir o bloqueio de vulnerabilidades;

2.4.12. Permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos;

2.4.13. Incluir proteção contra ataques de negação de serviços (DoS);

2.4.14. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);

2.4.15. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;

2.4.16. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc.;

2.4.17. Detectar e bloquear a origem de programas de varredura de portas (portscans);

2.4.18. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

2.4.19. Possuir assinaturas para bloqueio de ataques de buffer overflow;

2.4.20. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;

2.4.21. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

2.4.22. Identificar, alertar e bloquear comunicação com botnets;

2.4.23. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

2.4.24. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes

informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

2.4.25. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou anti-malware;

2.4.26. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

2.4.27. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

2.4.28. Identificar nos eventos o país de onde partiu a ameaça;

2.4.29. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;

2.4.30. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

2.4.31. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

2.4.32. Deve ser capaz de aplicar de forma complementar às assinaturas de antivírus, a inspeção, bem como prevenir ataques através do bloqueio efetivo do malware desconhecido (Dia Zero) capaz de analisar completamente o arquivo no ambiente sandbox, sem que ele seja entregue parcialmente ao cliente;

2.4.33. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;

2.5. Requisitos mínimos da funcionalidade de filtro de conteúdo dos Pontos Conectados Seguros:

2.5.1. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;

2.5.2. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.5.3. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.5.4. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;

2.5.5. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.5.6. Permitir a criação de categorias de URLs customizadas;

2.5.7. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;

2.5.8. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;

2.5.9. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

2.5.10. Permitir a customização de página de bloqueio;

2.6. Requisitos mínimos da funcionalidade de identificação de usuários dos Pontos Conectados Seguros:

2.6.1. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;

2.6.2. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

2.6.3. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.6.4. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;

2.6.5. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;

2.6.6. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;

2.6.7. Permitir a integração com tokens ou agentes para autenticação dos usuários;

- 2.6.8. A solução deverá permitir a integração com serviços de diretório e provedores de identidade (IdP), possibilitando a autenticação centralizada de usuários. A integração poderá ocorrer de forma direta ou por meio de soluções intermediárias de gerenciamento de identidade, devendo utilizar protocolos e padrões amplamente aceitos pelo mercado;
- 2.6.9. A solução deverá garantir o registro adequado e detalhado dos logs de acesso à internet, contemplando, no mínimo, a identificação do usuário autenticado, data e hora do acesso, endereço IP de origem, destino acessado e ação realizada. A identificação do usuário deverá estar associada à identidade fornecida pelo serviço de diretório ou provedor de identidade integrado à solução;
- 2.7. Requisitos mínimos das funcionalidades de Qualidade de Serviço (QoS) e Modelagem de Tráfego dos Pontos Conectados Seguros:
- 2.7.1. Realizar Traffic Shaping para a solução de segurança dos Pontos Conectados Seguros;
- 2.7.2. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 2.7.3. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 2.7.4. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 2.7.5. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 2.7.6. Realizar QoS (Traffic Shaping) em interface agregadas ou redundantes.
- 2.8. Requisitos mínimos da funcionalidade de filtro de dados dos Pontos Conectados Seguros:
- 2.8.1. Identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 2.8.2. Identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos;
- 2.8.3. Identificar e prevenir a transferência de informações definidas como sensíveis pela CONTRATANTE (por exemplo, número de cartão de crédito etc.) possibilitando a criação de novos tipos de dados via expressão regular.
- 2.9. Requisitos mínimos da funcionalidade de geolocalização dos Pontos Conectados Seguros:
- 2.9.1. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 2.9.2. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 2.9.3. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 2.10. Requisitos mínimos da funcionalidade de Redes Virtuais Privadas (VPNs) dos Pontos Conectados Seguros:
- 2.10.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 2.10.2. Suportar nativamente a criação de VPN IPsec utilizando 3DES;
- 2.10.3. Suportar nativamente a criação de VPN IPsec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 2.10.4. Suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1;
- 2.10.5. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 2.10.6. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.10.7. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;
- 2.10.8. A solução deve suportar interoperabilidade VPN com equipamentos de diferentes fabricantes, mediante a implementação de padrões abertos amplamente utilizados no mercado, incluindo suporte aos protocolos IPsec, IKEv2, AES, SHA-2, Diffie-Hellman e NAT-T, garantindo a compatibilidade com quaisquer soluções que adotem tais padrões;
- 2.10.9. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPsec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 2.10.10. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 2.10.11. Realizar atribuição de DNS nos clientes remotos de VPN;
- 2.10.12. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 2.10.13. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.10.14. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 2.10.15. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 2.10.16. Manter uma conexão segura com o portal durante a sessão;

- 2.10.17. Garantir e prover solução IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 2.10.18. Garantir e prover solução de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS;
- 2.11. Funcionalidade de virtualização:
- 2.11.1. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;
- 2.11.2. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 2.12. Funcionalidade de SD-WAN:
- 2.12.1. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;
- 2.12.2. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 2.12.3. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 2.12.4. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.;
- 2.12.5. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 2.12.6. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 2.12.7. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 2.12.8. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 2.12.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 2.12.10. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 2.12.11. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- 2.12.12. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 2.12.13. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 2.12.14. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;
- 2.12.16. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 2.12.17. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar pelo menos um dos métodos descritos abaixo:
- 2.12.17.1. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 2.12.17.2. Passivo: uso do tráfego real para as medições;
- 2.12.18. A solução de SD-WAN deve possuir, garantir, implementar, permitir e possibilitar o uso de túneis VPN

dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

### 3. Solução para gerenciamento de acessos à rede local - NAC

3.1. Este item deve incluir o licenciamento da controladora, se aplicável, durante todo o período do contrato, e as unidades serão contratadas individualmente de forma granular;

3.2. Todas as funcionalidades descritas devem estar devidamente licenciadas, com suporte do fabricante e com a possibilidade de atualização para novas versões para o período total do contrato;

3.3. A Solução de Gerenciamento de Acessos à Rede (NAC) deverá ser fornecida e mantida integralmente pela CONTRATADA. A solução poderá ser implementada em formato virtual, físico ou em Nuvem (seguindo os requisitos mínimos do ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM), conforme necessidade. Toda a responsabilidade pela operação, atualização e manutenção será exclusiva da CONTRATADA;

3.4. Deve funcionar, com todas as funcionalidades ativas, em camada de rede Layer 3;

3.5. A solução deve ser entregue em alta disponibilidade;

3.6. Possuir plataforma unificada que combina AAA e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas, permitindo licenciamento futuro das funções de NAC e BYOD;

3.7. Suporte a seguintes fontes para autenticação:

3.7.1. Microsoft Active directory;

3.7.2. Kerberos;

3.7.3. LDAP;

3.7.4. Radius;

3.7.5. HTTP;

3.7.6. Lista estática de endereços MAC;

3.7.7. Deve possuir integração com o item Solução unificada de segurança de rede para possibilitar "Single Sign-on" (SSO) para os usuários identificados.

3.8. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

3.8.1. Atributos do usuário autenticado;

3.8.2. Hora do dia, dia da semana;

3.8.3. Tipo de dispositivo utilizado;

3.8.4. Localização do usuário;

3.8.5. Tipo de autenticação utilizado;

3.9. Permitir a visualização de todas as informações relativas a cada transação/autenticação em uma única tela, como:

3.9.1. Data e Hora;

3.9.2. Mac Address do dispositivo;

3.9.3. Classificação do dispositivo;

3.9.4. Usuário;

3.9.5. Equipamento que requisitou a autenticação (origem);

3.9.6. Método de autenticação utilizado;

3.9.7. Fonte de autenticação utilizada para validação;

3.9.8. Perfil de acesso aplicado;

3.9.9. Todos os atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Logs já filtrados para a requisição em análise;

3.10. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

3.10.1. Lista com os últimos Alertas do sistema;

3.10.2. Gráfico com o status das autenticações aceitas e rejeitadas;

3.10.3. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;

- 3.10.4. Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 3.10.5. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora etc.), por sistema operacional (ex. Windows, Linux, MacOS etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server etc.);
- 3.11. Deve suportar a coleta de informações, para classificação, usando no mínimo:
- 3.11.1. DHCP fingerprint;
- 3.11.2. HTTP;
- 3.11.3. MAC OUI;
- 3.11.4. SNMP;
- 3.11.5. Subnet Scanner;
- 3.11.6. MDM;
- 3.11.7. TCP Fingerprinting;
- 3.11.8. Deve possuir base de regras e categorias de dispositivos pré-configurada;
- 3.11.9. Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;
- 3.11.10. Deve suportar a integração com soluções de MDM (Mobile Device Management) de forma nativa ou por meio de API;
- 3.11.11. Suporte a RADIUS CoA ou mecanismo equivalente de alteração dinâmica de autorização, e Web authentication;
- 3.12. Deve suportar os seguintes métodos de autenticação:
- 3.12.1. TLS;
- 3.12.2. TTLS;
- 3.12.3. PEAP;
- 3.12.4. MD5;
- 3.12.5. GTC;
- 3.12.6. MSCHAPV2;
- 3.12.7. WPA;
- 3.12.8. Online Certificate Status Protocol (OCSP);
- 3.12.9. WEB Authentication;
- 3.12.10. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP);
- 3.12.11. Suporte a aplicação de políticas em ambiente multi vendor de Wireless, LAN e VPN;
- 3.13. A solução deverá permitir integração funcional com soluções de segurança de terceiros amplamente adotadas no mercado, possibilitando a troca de informações de contexto e a aplicação coordenada de políticas de controle de acesso, segmentação, quarentena ou isolamento, por meio de mecanismos nativos, conectores ou APIs documentadas, admitindo-se soluções tecnicamente equivalentes;
- 3.14. Deve suportar integração com no mínimo os seguintes sistemas operacionais: Android, Apple MAC OSX e iOS, Linux Ubuntu, Microsoft Windows;
- 3.15. Deve ser capaz de implementar políticas de segurança baseadas em no mínimo:
- 3.15.1. Localidade;
- 3.15.2. Usuários e ou grupo de Usuários;
- 3.15.3. Hosts ou grupo de Hosts;
- 3.15.4. Usuário temporário;
- 3.15.5. Guest;
- 3.16. Deve implementar resposta automática a incidente com integração ao item Solução Unificada de Segurança de Rede deste edital, ou seja, os incidentes detectados pela Solução Unificada de Segurança de Rede devem ser utilizados para resposta automática ao incidente, como, por exemplo, mover o host afetado para uma VLAN de quarentena;
- 3.17. Deve fazer a checagem de compliance dos Endpoints (Hosts). Os Endpoints (Hosts) são computadores, dispositivos móveis ou qualquer outro equipamento que necessite se conectar à rede. A checagem de compliance deve verificar se os Endpoints (Hosts) seguem as políticas de segurança definidas pelo ABC;
- 3.18. Deve realizar a checagem de compliance dos Endpoints (Hosts) por meio de mecanismos de verificação devendo suportar, no mínimo, a verificação com agente permanente, bem como a verificação temporária, a qual

poderá ser implementada por meio de agente temporário ou de forma agentless;

3.19. Deve fazer a checagem de compliance dos Endpoints (Hosts), verificando no mínimo os seguintes itens:

3.19.1. Atualização de segurança do sistema operacional, Windows, MacOS ou Linux;

3.19.2. Antivírus;

3.19.3. Informações do sistema operacional;

3.20. Deve detectar dispositivos Internet das Coisas (IoT) como por exemplo impressoras, câmeras de cftv, controles de acesso biométricos, smart TVs;

3.21. Deve mover dispositivos IoT para VLANs pré-determinadas;

3.22. Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptação da comunicação;

3.23. Deve suportar EDUROAM;

3.24. Suporte à integração com plataforma de terceiros usando HTTP/RESTful API;

3.25. Suporte aos seguintes recursos através de IPv6:

3.25.1. Administração via WEB e CLI;

3.25.2. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;

3.26. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona";

3.27. A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos às seguintes atividades anormais detectadas na rede:

3.27.1. Autenticações;

3.27.2. Acesso a dispositivos de rede;

3.27.3. Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios;

3.27.4. Atividades irregulares nos servidores da solução;

3.28. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato de no mínimo PDF;

3.29. Deve possuir ferramentas para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

3.30. Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

3.31. Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

3.32. Deve permitir que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;

3.33. Deve realizar o caching de endereço MAC dos usuários visitantes;

3.34. Deve fornecer os certificados SSL válidos para o captive portal ou necessária para qualquer outra interação usuário e sistemas, tais como AD e servidores de e-mail;

3.35. Todas as licenças devem ser fornecidas para todo o período do contrato.

#### **4. Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) com fornecimento dos equipamentos necessários para ativação do serviço**

4.1. O serviço consiste em configurar os Firewalls para operar em modo de alta disponibilidade, garantindo que um dispositivo possa assumir automaticamente as funções do outro em caso de falha;

4.2. A CONTRATANTE aderente poderá solicitar a qualquer momento durante a vigência do contrato, o serviço de Alta Disponibilidade (HA) para a Solução Unificada de Segurança de Rede;

4.3. A configuração deve garantir a continuidade do serviço de rede e a integridade dos dados durante e após o processo de failover;

4.4. Para o serviço, deverão ser disponibilizados todos os cabos e conectores, bem como dois switches necessários para complementar a infraestrutura para alta disponibilidade (HA);

4.5. Requisitos mínimos dos switches para o serviço de alta disponibilidade (HA):

Tabela 2 - Especificações mínimas da solução

Item	Especificação	Quantidades de portas do Switches
1	Interfaces de 1 Gbps para conexão de cabos de par metálico UTP com conector RJ-45	16
2	10 Gigabit Ethernet com conectores SFP+	4

- 4.5.1. Deve possuir no mínimo 16 (dezesesseis) interfaces de 1 Gbps para conexão de cabos de par metálico UTP com conector RJ-45.
- 4.5.2. Deve possuir, no mínimo, 4 portas 10 Gigabit Ethernet com conectores SFP+, sendo que a escolha do tipo e a necessidade de transceiver a serem fornecidos (10GBASE-T ou 10GBASE-SR) deverá depender dos resultados da topologia do local (Solução unificada de segurança de rede, quantidade/velocidade dos Links de Acesso), garantindo a melhor adequação às condições e requisitos da infraestrutura existente no PCs.
- 4.5.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- 4.5.4. Deve possuir 1 (uma) interface USB;
- 4.5.5. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);
- 4.5.6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 4.5.7. Deve possuir tabela MAC no mínimo com suporte a 24.000 endereços;
- 4.5.8. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 4.5.9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- 4.5.10. Deve suportar a comutação de Jumbo Frames;
- 4.5.11. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- 4.5.12. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 4.5.13. Deve implementar serviço de DHCP Relay;
- 4.5.14. Deve suportar IGMP snooping para controle de tráfego de multicast;
- 4.5.15. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 4.5.16. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 4.5.17. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 4.5.18. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 4.5.19. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- 4.5.20. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
- 4.5.21. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 4.5.22. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 4.5.23. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

- 4.5.24. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- 4.5.25. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 4.5.26. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 4.5.27. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 4.5.28. Deve suportar MAC Authentication Bypass (MAB);
- 4.5.29. Deve implementar RADIUS CoA (Change of Authorization);
- 4.5.30. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 4.5.31. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 4.5.32. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 4.5.33. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 4.5.34. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 4.5.35. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 4.5.36. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 4.5.37. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 4.5.38. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 4.5.39. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 4.5.40. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 4.5.41. Deve permitir ser gerenciado através de IPv6;
- 4.5.42. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 4.5.43. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 4.5.44. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 4.5.45. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 4.5.46. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 4.5.47. Deverá suportar ser configurado e monitorado através de REST API;
- 4.5.48. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 4.5.49. Todos os acessórios para montagem e fixação deverão ser fornecidos;

#### ADENDO IV - SERVIÇO DE REDE SEM FIO (SRSF) MODALIDADE INTERNO (INDOOR) E EXTERNO (OUTDOOR)

##### 1. Requisitos gerais

1.1. O Serviço de Rede Sem Fio (SRSF) deve possuir, permitir, garantir, prover e implementar na solução as seguintes características, que a LICITANTE classificada como vencedora do certame licitatório deve apresentar na fase de

habilitação uma matriz cruzada, informando as páginas do fabricante do equipamento ou *software* ou qualquer item do serviço onde comprove que atende as especificações e os requisitos obrigatórios a serem atendidos, contidos nesse Termo de Referência;

1.2. A LICITANTE deve apresentar na proposta de preços a descrição de como será a prestação dos serviços incluindo uma descrição do Serviço de Rede Sem Fio (SRSF) para a Nova Rede, sendo disponibilizado e precificado por *access point*, tanto Interno(*indoor*) como Externo(*outdoor*) atendendo aos princípios gerais e requisitos contidos neste Termo de Referência;

1.3. Após o recebimento da Ordem de Serviço (OS), a CONTRATADA deverá agendar e realizar o Site Survey em coordenação com o Gestor de TI do Órgão. A data do Site Survey deverá ser previamente acordada entre as partes. Uma vez concluído o Site Survey, a CONTRATADA terá o prazo estabelecido no item 6.7 *LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, CONFIGURAÇÃO E ENTREGA* deste Termo de Referência, para entregar o relatório detalhado ao Gestor do Órgão, contendo todas as informações e recomendações necessárias e os quantitativos dos APs e como será implementado, para a continuidade dos serviços;

1.4. O Serviço de Rede Sem Fio (SRSF) deverá ser dimensionado e disponibilizado na infraestrutura da CONTRATANTE aderente, sendo interligado ao serviço de Links de Acesso (LA) contratado. O SRSF também deve funcionar de forma gerenciada e integrada com as Soluções de Segurança do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

1.5. O Serviço de Rede Sem Fio (SRSF) deverá ser provido por uma solução integrada de software e hardware, com controladoras de rede sem fio local ou utilizando solução de gerenciamento em nuvem pública do mesmo fabricante, pontos de acesso internos (*indoor*) e/ou externos (*outdoor*) compatíveis com as Soluções de Segurança adotadas;

1.6. O Serviço de Rede Sem Fio (SRSF) externo (*outdoor*), pode ser disponibilizado em área externa ao PCS - Ponto Cliente Seguro, deverá ser interligado ao CPE (*Customer Premises Equipment*) do PCS;

1.7. Realizar os serviços especificados no item “Serviço de Garantia de Qualidade Contínua do SRSF” no momento da abertura da Ordem de Serviço para implementação do Serviço de Rede Sem Fio (SRSF), reunindo as informações necessárias para o início das atividades, incluindo o levantamento do quantitativo de APs tanto para o serviço de rede sem fio interno quanto para o externo. A aprovação deve ser realizada em conjunto com a ATI e o CONTRATANTE aderente.

1.8. Topologia de Implantação e Infraestrutura de Conectividade

1.8.1. A topologia de implantação do Serviço de Rede Sem Fio (SRSF) deverá ser, por padrão, em arquitetura Mesh, conforme previsto neste Termo de Referência, garantindo flexibilidade, redundância e cobertura ampliada;

1.8.2. Excepcionalmente, a implantação poderá ser realizada em topologia cabeada ou híbrida (mista), quando as condições técnicas, estruturais ou de interferência do ambiente justificarem tal necessidade, desde que a justificativa da viabilidade técnica seja formalmente apresentada pela CONTRATADA e validada pela CONTRATANTE técnica (ATI-PE) constando no respectivo relatório de Site Survey;

1.8.3. A infraestrutura necessária para implantação do Serviço de Rede Sem Fio (SRSF) em topologia cabeada somente poderá incluir o Serviço de Fornecimento e Implantação de Switch às custas da CONTRATANTE quando a adoção dessa topologia for previamente justificada e aprovada pela CONTRATANTE técnica (ATI-PE), mediante análise e validação formal no relatório de Site Survey.

1.8.3.1. Caso a utilização da topologia cabeada não seja aprovada pela ATI-PE, a CONTRATADA deverá adequar o projeto e a implantação conforme as orientações técnicas emitidas pela CONTRATANTE técnica.

1.8.3.2. Nos casos em que a topologia seja parcialmente aprovada, a ATI-PE indicará, de forma expressa, quais custos poderão ser assumidos pela CONTRATANTE, cabendo à CONTRATADA suportar integralmente os demais custos relacionados a switches e demais elementos de infraestrutura necessários ao pleno funcionamento do serviço, sem qualquer ônus adicional para a CONTRATANTE.

1.8.3.3. Na hipótese de a CONTRATADA utilizar switches próprios, fora do escopo do “**Serviço de Fornecimento e Implantação de Switch**”, estes equipamentos deverão obrigatoriamente atender às especificações técnicas mínimas previstas neste Termo de Referência, incluindo:

- Backhaul de 10 Gigabits (10G);
- Suporte a PoE no padrão IEEE 802.3bt (ou superior);
- Plena compatibilidade com os Pontos de Acesso (APs) Wi-Fi 7.

1.8.3.4. Os equipamentos utilizados deverão ser fornecidos, configurados, operados e mantidos integralmente pela CONTRATADA, sem qualquer ônus adicional para a CONTRATANTE.

1.8.4. Em qualquer cenário de implantação, toda a infraestrutura física necessária à interligação dos Pontos de Acesso (APs) deverá ser fornecida e instalada pela CONTRATADA, incluindo, mas não se limitando a:

- Cabos de par trançado Categoria 6A (ou superior), adequados para suportar comunicação de até 10 Gbps por Ponto de Acesso, conforme os requisitos de desempenho do padrão Wi-Fi 7;
- Cabos de fibra óptica, quando aplicável, com conversores de mídia (SFP+) para RJ-45 10Gbps;
- Patch cords, conectores, canaletas, dutos, tomadas, racks e acessórios necessários à interligação dos APs, switches e controladoras;
- Fontes, injetores PoE e transceptores compatíveis com o padrão IEEE 802.3bt (ou superior);
- Demais elementos físicos indispensáveis ao pleno funcionamento da solução.

1.8.5. A CONTRATADA será integralmente responsável pelo fornecimento, instalação, certificação, documentação, operação e ativação de toda a infraestrutura utilizada, sem qualquer ônus adicional para a CONTRATANTE.

1.8.6. Independentemente da topologia adotada, o desempenho mínimo exigido deverá ser plenamente atendido pela CONTRATADA, conforme as especificações técnicas e funcionais deste Termo de Referência.

1.8.7. Possuir, permitir, garantir, prover e implementar suporte à operação dos Pontos de Acesso (APs) em modo cabeado, Mesh ou híbrido, assegurando interoperabilidade plena entre os APs conectados por diferentes topologias, com gerenciamento, configuração e aplicação de políticas de rede unificadas por meio da controladora Wi-Fi.

## 1.9. Composição e Interoperabilidade da Solução

1.9.1. Caso a solução ofertada não implemente nativamente todas as funcionalidades requeridas no Termo de Referência, será aceito o uso de composições com outras soluções, desde que seja garantido e comprovado o atendimento integral a todos os requisitos técnicos exigidos neste Termo de Referência, assegurando ainda a plena interoperabilidade entre os componentes da solução ofertada.

1.9.2. Todas as soluções e tecnologias empregadas deverão operar de forma integrada, sob gestão centralizada e unificada, garantindo compatibilidade funcional, interoperabilidade comprovada e integração padronizada com as plataformas da CONTRATANTE técnica (ATI-PE), em conformidade com as boas práticas de segurança e governança tecnológica.

1.9.3. Caso a composição da solução envolva tecnologias ou fabricantes distintos, a CONTRATADA deverá apresentar descrição detalhada da arquitetura de integração, demonstrando que a implementação assegura desempenho, disponibilidade, segurança, manutenção e suporte técnico equivalentes ou superiores aos de uma solução nativamente integrada.

1.9.4. A CONTRATADA deverá comprovar, no Plano de Implantação e Integração, que todos os componentes atuarão de forma coesa, compatível e gerenciável a partir de uma interface central, assegurando o atendimento integral aos Níveis Mínimos de Serviço (NMS) e aos requisitos técnicos definidos neste Termo de Referência.

## 2. Gerenciamento (Controladora Wi-Fi)

2.1 Possuir, permitir, garantir, prover e implementar uma solução de gerenciamento (controladora Wi-Fi) que possa ser oferecida na nuvem, de forma remota ou local (por meio de controladora física ou solução equivalente), assegurando o controle e monitoramento em tempo real de todos os APs instalados nas diversas localidades do Estado de Pernambuco. A solução deve ser integrada às soluções de segurança do Centro Integrado de Inteligência e Segurança Cibernética (CIISC) da Nova Rede Corporativa, podendo empregar APIs ou plataformas complementares que assegurem integração funcional plena, interoperabilidade e visibilidade unificada, garantindo uma gestão eficiente e segura da rede.

2.2. Possuir, permitir, garantir, prover e implementar, na solução de gerenciamento, a centralização completa do controle e a visualização integrada de toda a topologia da rede de Access points (APs). A visualização deve ser disponibilizada por meio de aplicações web intuitivas, acessíveis aos usuários indicados pela CONTRATANTE aderente e CONTRATANTE TÉCNICA, assegurando fácil acesso e monitoramento. No ambiente da CONTRATANTE TÉCNICA, a rede de APs deve ser exibida em tempo real no painel de gerenciamento da Nova Rede Corporativa, proporcionando uma visão abrangente, detalhada e continuamente atualizada da infraestrutura, permitindo intervenções rápidas e precisas sempre que necessário;

2.3. Possuir, permitir, garantir, prover e implementar na solução de gerenciamento, a centralização e o monitoramento em tempo real do desempenho da rede MESH Wi-Fi, incluindo métricas de performance, throughput e interferências. A solução deve garantir visibilidade contínua e precisa desses parâmetros, permitindo ajustes imediatos e garantindo a estabilidade, eficiência e qualidade do serviço em toda a rede;

2.4. Possuir, permitir, garantir, prover e implementar que todas as funcionalidades descritas no Adendo de Serviço de Rede sem Fio (SRSF) sejam suportadas e operem de forma simultânea e ininterrupta, tanto no gerenciamento unificado por controladora quanto no modo MESH. A solução deve assegurar a plena integração e funcionamento contínuo das funcionalidades em ambas as configurações, garantindo a eficiência e a flexibilidade da rede;

2.5. Os logs da SRSF devem ser encaminhados para a Solução de Guarda de Logs descrita no ADENDO VIII;

### 3. Gerenciamento dos pontos de acessos sem fio

3.1. Possuir, permitir, garantir, prover e implementar que o gerenciamento de todos os pontos de acesso sem fio de forma centralizada, utilizando controladoras ou tecnologias equivalentes, para disponibilizar alta disponibilidade, eficiência no controle de tráfego e facilidade de configuração e monitoramento em tempo real atendendo aos seguintes requisitos mínimos:

3.1.1. Possuir, permitir, garantir, prover e implementar mecanismos que assegurem o controle, supervisão e gerência centralizada de todos os Pontos de Acesso (APs) sem fio pelo Centro Integrado de Inteligência e Segurança Cibernética (CIISC) da Nova Rede Corporativa. A solução deverá permitir a integração direta com as plataformas do CIISC, por meio de APIs seguras ou interfaces equivalentes, garantindo visibilidade unificada, correlação de eventos de segurança e administração centralizada da rede Wi-Fi, sem prejuízo do gerenciamento local realizado pela controladora da CONTRATADA.

3.1.2. Possuir, permitir, garantir, prover e implementar que o sistema de gerenciamento e todas as suas funcionalidades deverão ser acessíveis via navegador (browser) *Web*;

3.1.3. Possuir, permitir, garantir, prover e implementar uma solução de monitoramento que disponibilize estatísticas e relatórios detalhados sobre usuários, dispositivos conectados e o fluxo de tráfego (*traffic flow*) na rede Wi-Fi. A solução deve oferecer dados em tempo real e históricos, permitindo análise de desempenho, padrões de uso e otimização do gerenciamento de rede, com informações precisas sobre *throughput*, e distribuição de carga entre os APs;

3.1.4. Possuir, permitir, garantir, prover e implementar mecanismos de gerenciamento de alarmes e eventos que ocorram na rede Wi-Fi;

3.1.5. Possuir, permitir, garantir, prover e implementar a atualização de *firmware* em massa para todos os APs da rede Wi-Fi, de maneira sincronizada e automatizada. A solução deve assegurar que as atualizações sejam aplicadas

simultaneamente, minimizando interrupções no serviço e garantindo que todos os dispositivos permaneçam seguros, atualizados e operando com as versões mais recentes de *firmware* homologadas;

3.1.6. Possuir, permitir, garantir, prover e implementar o controle de acesso dos usuários à rede Wi-Fi, assegurando autenticação segura, gerenciamento de permissões e restrições conforme políticas definidas. A solução deve permitir a configuração de diferentes níveis de acesso e autenticação, garantindo que apenas usuários autorizados possam se conectar e utilizar os recursos da rede;

3.1.7. Possuir, permitir, garantir, prover e implementar a geração de gráficos detalhados, como os de tráfego de rede, uso de banda, desempenho de APs e outras métricas essenciais. A solução deve oferecer visualizações claras e intuitivas para facilitar o monitoramento e a análise da rede Wi-Fi, permitindo ajustes rápidos e eficientes conforme necessário;

3.1.8. Possuir, permitir, garantir, prover e implementar a extração de mapas detalhados da rede Wi-Fi, exibindo a localização exata dos rádios (APs) instalados. A solução deve oferecer uma visualização clara e precisa da distribuição dos APs, facilitando o monitoramento, a análise de cobertura e a otimização da rede;

3.1.9. Possuir, permitir, garantir, prover e implementar um mecanismo de *Auto-Tuning* de RF (Radiofrequência) para a rede Wi-Fi, capaz de ajustar dinamicamente o canal de comunicação e a potência de transmissão dos rádios dos APs. A solução deve realizar essas configurações de forma automática e contínua, otimizando o desempenho e minimizando interferências, sempre que necessário, para garantir a melhor cobertura e estabilidade da rede;

3.1.10. Possuir, permitir, garantir, prover e implementar a capacidade de gerenciar, de forma centralizada e integrada em um sistema único, todos os Pontos de Acesso (APs) fornecidos pela solução de Serviço de Rede Sem Fio (SRSF). A solução deve oferecer controle completo e unificado sobre a configuração, monitoramento e otimização dos APs, assegurando eficiência, segurança e facilidade de administração para toda a rede Wi-Fi;

3.1.11. Possuir, permitir, garantir, prover e implementar a visualização centralizada dos clientes *wireless* conectados, através de uma console de gerenciamento unificado que exiba informações detalhadas em tempo real sobre cada dispositivo, permitindo o monitoramento e controle eficientes da rede Wi-Fi;

3.1.12. Prover, permitir, garantir, fornecer e implementar, conforme a necessidade da CONTRATANTE, o serviço DHCP por SSID, para disponibilizar endereçamento IP automático aos clientes *wireless* conectados. A solução deve assegurar a configuração e gestão eficiente de múltiplos escopos de DHCP, permitindo a distribuição organizada de endereços IP, segmentação de rede e controle otimizado dos dispositivos conectados à rede Wi-Fi;

3.1.13. Possuir, permitir, garantir, prover e implementar a configuração de endereçamento IPv4 e IPv6 por SSID, assegurando que cada rede Wi-Fi possa distribuir automaticamente endereços IP para os dispositivos conectados. A solução deve oferecer flexibilidade na gestão de endereços para suportar tanto o protocolo IPv4 quanto o IPv6, permitindo a coexistência e configuração eficiente dos dois protocolos, conforme as necessidades de segmentação e segurança da rede;

3.1.14. Possuir, permitir, garantir, prover e implementar a capacidade de escolher se o tráfego de cada SSID será enviado à controladora central ou comutado diretamente pela *interface* do ponto de acesso (AP) em uma determinada VLAN. A solução deve assegurar flexibilidade no gerenciamento de tráfego, permitindo definir políticas que otimizem o desempenho e a segurança da rede, com a opção de direcionar o tráfego conforme as necessidades de segmentação e arquitetura da rede Wi-Fi;

3.1.15. Possuir, permitir, garantir, prover e implementar a capacidade de definir quais redes serão gerenciadas pela controladora, por meio de conexões simultâneas, e quais redes serão comutadas diretamente pela *interface* dos pontos de acesso sem fio. A solução deve oferecer flexibilidade para configurar o direcionamento do tráfego de cada SSID, permitindo uma gestão eficiente da segmentação de rede e garantindo que o tráfego seja encaminhado conforme as necessidades de arquitetura e desempenho da rede Wi-Fi;

3.1.16. Possuir, permitir, garantir, prover e implementar autenticação para a rede Wi-Fi utilizando bases externas, como servidores LDAP, LDAP/AD (*Active directory*) ou RADIUS, assegurando integração segura e eficiente com sistemas de autenticação centralizados. A solução deve garantir compatibilidade e flexibilidade na gestão de

credenciais, permitindo que usuários se autenticuem na rede sem fio usando suas credenciais existentes em diretórios corporativos externos;

3.1.17. Possuir, permitir, garantir, prover e implementar a autenticação de usuários na solução SRSF em integração com a Solução de Gerenciamento de Identidade de Acesso da Nova Rede Corporativa, possibilitando autenticação federada através de bases externas, como Google Workspace (GSuite), Microsoft 365 / Entra ID (Azure AD) ou Active Directory On-Premises, por meio de componentes de controle de acesso à rede (NAC) ou equivalentes. A solução deve assegurar compatibilidade total e interoperabilidade com esses sistemas, garantindo um processo de login seguro, eficiente e baseado nas credenciais corporativas existentes dos usuários.

3.1.18. Possuir, permitir, garantir, prover e implementar suporte à norma de autenticação 802.1X via RADIUS na controladora *wireless*, assegurando uma autenticação segura e centralizada de usuários, com integração a sistemas de gerenciamento de identidade corporativos;

3.1.19. Possuir, permitir, garantir, prover e implementar suporte a *Fast Roaming*, assegurando que os usuários mantenham conectividade contínua e sem interrupções ao se deslocarem entre diferentes pontos de acesso na rede;

3.1.20. Possuir, permitir, garantir, prover e implementar a configuração de *Captive portal* por SSID, permitindo personalizar o processo de autenticação para usuários conectados, com opções de controle de acesso e registro de uso;

3.1.21. Possuir, permitir, garantir, prover e implementar a configuração de parâmetros de rádio, como banda e canal, diretamente na controladora *wireless*, proporcionando flexibilidade para ajustar e otimizar o desempenho da rede de acordo com o ambiente e as necessidades específicas;

3.1.22. Possuir, permitir, garantir, prover e implementar que a comunicação entre os pontos de acesso sem fio e a controladora *wireless* possa ser estabelecida utilizando protocolos proprietários do fabricante ou através de IPv6, assegurando flexibilidade e compatibilidade na implementação da solução;

3.1.23. Possuir, permitir, garantir, prover e implementar um método de descoberta automática de novos Pontos de Acesso (APs) na rede, utilizando técnicas de *Broadcast* ou *Multicast*, facilitando a integração e expansão da rede sem fio;

3.1.24. Possuir, permitir, garantir, prover e implementar uma lista de gestão de Pontos de Acesso, incluindo APs aceitos e Pontos de Acesso indevidos (Rogue), com recursos para identificação e bloqueio automático de dispositivos não autorizados;

3.1.25. Possuir, permitir, garantir, prover e implementar o uso de *Protected Management Frames* (PMF) para proteger as comunicações de gerenciamento entre APs e dispositivos, assegurando maior segurança contra ataques como *spoofing* e *de-authentication*;

3.1.26. Possuir, permitir, garantir, prover e implementar o provisionamento automático de canais dos Pontos de Acesso sem fio, com agendamento flexível de dia e horário, para minimizar interferências e otimizar o desempenho da rede;

3.1.27. Possuir, permitir, garantir, prover e implementar a configuração de horários específicos para a ativação de determinados SSIDs, conforme as necessidades da CONTRATANTE, permitindo um controle preciso sobre a disponibilidade da rede;

3.1.28. A solução de rede sem fio deve realizar a integração com a solução de firewall. Essa integração deve possibilitar a aplicação de políticas de segurança baseada na identidade do usuário;

3.1.29. Possuir, permitir, garantir, prover e implementar a definição de um número máximo de clientes permitidos por SSID, garantindo o controle de acesso e a qualidade de serviço da rede;

3.1.30. Possuir, permitir, garantir, prover e implementar a criação, gestão e operação de redes MESH Wi-Fi, assegurando conectividade contínua e expansão flexível por meio de APs interconectados. A solução deve permitir que a rede MESH se auto-organize e ajuste automaticamente a cobertura e o desempenho, otimizando a distribuição

de sinal conforme a topologia e as demandas variáveis do ambiente, garantindo estabilidade e eficiência em áreas de alta densidade e de grande extensão, conforme as exigências da CONTRATANTE;

3.1.31. Possuir, permitir, garantir, prover Implementar o Serviço de Rede Sem Fio (SRSF) utilizando equipamentos indoor com tecnologia MESH, prioritariamente nos Pontos Conectados Seguros (PCS). A solução MESH deve garantir conectividade contínua e flexível, otimizando desempenho e cobertura conforme as demandas do ambiente;

3.1.32. Possuir, permitir, garantir, prover e implementar que todos os Pontos de Acesso na configuração de rede MESH tenham pelo menos um rádio configurado exclusivamente para a comunicação de *backhaul* MESH, assegurando uma conexão estável e dedicada;

3.1.33. Possuir, permitir, garantir, prover e implementar a comunicação dos APs com a controladora por meio de um SSID de backhaul separado ou outra solução que assegure um tráfego interno exclusivo da Rede MESH, não acessível aos clientes Wi-Fi;

3.1.34. Garantir que cada malha MESH tenha apenas um Ponto de Acesso conectado à rede cabeada, atuando como o nó raiz da malha para gerenciar e distribuir o tráfego na rede MESH. Cada Malha MESH deverá ser composta por até 8 (oito) Pontos de Acesso, sendo um Ponto de Acesso como nó raiz e no máximo 7 Pontos de Acesso conectados a esse nó raiz por meio da rede MESH;

3.1.35. Possuir, permitir, garantir, prover e implementar que os Pontos de Acesso remotos propaguem o SSID da rede MESH ou tecnologia que assegure **equivalência funcional, com características e performance equiparáveis e interoperabilidade** ao padrão MESH, assegurando conectividade contínua e eficiente entre nós distantes. A solução deve garantir redistribuição automática de tráfego, otimizando a cobertura e o desempenho com baixa latência e alta disponibilidade, de acordo com os parâmetros de Qualidade de Serviço (QoS) do Wi-Fi 7 e versões anteriores;

3.1.36. Possuir, permitir, garantir, prover e implementar que os Pontos de Acesso remotos sejam capazes de se conectar ao SSID da MESH diretamente do nó raiz ou de qualquer outro nó remoto, garantindo redundância e resiliência na comunicação;

3.1.37. Possuir, permitir, garantir, prover e implementar o SSID dedicado ao *backhaul*, operando na frequência definida durante a implementação pela CONTRATANTE TÉCNICA, podendo ser no rádio de 6 GHz ou 5 GHz para modelos indoors. Essa adaptação assegura uma comunicação eficiente e de alta velocidade, respeitando os requisitos do serviço;

3.1.38. Possuir, permitir, garantir, prover e implementar o SSID dedicado ao backhaul, operando no rádio de 5 GHz. Caso a solução oferecida inclua a frequência de 6 GHz (homologada pela ANATEL) cabe à CONTRATANTE TÉCNICA, durante o período de implementação, definir qual frequência será utilizada para configurar o *backhaul* em modelos outdoor. Essa flexibilidade assegura um desempenho confiável e adaptável às especificidades do ambiente externo, promovendo eficiência e robustez na comunicação em áreas abertas;

3.1.39. Possuir, permitir, garantir, prover e implementar que os rádios de 2.4 GHz e 5 GHz sejam utilizados com SSIDs dedicados ao atendimento aos usuários, otimizando a conectividade e garantindo a separação adequada do tráfego de *backhaul* e de acesso do cliente;

3.1.40. Garantir, prover e implementar mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por *e-mail* ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

3.1.41. Possuir, permitir, garantir, prover e implementar que a solução do Serviço de Rede Sem Fio (SRSF) ofereça autenticação de acesso utilizando bases externas, como Facebook, Google, Microsoft e LinkedIn. Caso uma dessas plataformas exija uma conta corporativa para configuração, a responsabilidade pela criação e manutenção dessa conta será da CONTRATADA, sem custos adicionais para a CONTRATANTE;

3.1.42. Possuir, garantir, prover e implementar mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso sem fio gerenciados;

- 3.1.43. Possuir, garantir, prover e implementar mecanismo de balanceamento de tráfego/usuários entre pontos de acesso sem fio;
- 3.1.44. Possuir, garantir, prover e implementar mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios dos pontos de acesso sem fio;
- 3.1.45. Possuir, permitir, garantir, prover e implementar a identificação de Pontos de Acesso sem fio com *firmware* desatualizado e realizar a atualização de forma automatizada e centralizada via *interface* gráfica, tanto em soluções locais quanto na nuvem através da Gerência da Nova Rede. A solução deve assegurar que as atualizações possam ser efetuadas de maneira rápida e eficiente, garantindo a segurança e a estabilidade contínua de todos os APs na rede;
- 3.1.46. Possuir, permitir, garantir, prover e implementar bloquear clientes *wireless* que tenham sinal fraco, definindo um valor do sinal a partir do qual tais clientes serão ignorados;
- 3.1.47. Permitir suprimir Pontos de Acesso Indevidos (Rogue) detectados através de frames de autenticação e bloqueio do endereço MAC deste AP;
- 3.1.48. Possuir, permitir, garantir, prover e implementar a funcionalidade de selecionar individualmente, em cada *Access point* (AP), quais SSIDs serão propagados, permitindo uma configuração flexível e personalizada para atender às necessidades específicas de cada localidade da rede;
- 3.1.49. Possuir, permitir, garantir, prover e implementar a configuração de prioridade de tráfego por SSID (Service Set Identifier), utilizando os mecanismos de Quality of Service (QoS) disponíveis no padrão 802.11be/ax;
- 3.1.50. Possuir, permitir, garantir, prover e implementar a configuração de diferentes níveis de prioridade para cada SSID, garantindo que aplicações críticas, como videoconferências, VoIP, e streaming em alta definição, recebam tratamento preferencial;
- 3.1.51. Possuir, permitir, garantir, prover e implementar a configuração de filas de prioridade, com base em categorias de tráfego, como voz, vídeo e dados, de acordo com o padrão Wi-Fi Multimedia (WMM);
- 3.1.52. Possuir, permitir, garantir, prover e implementar a configuração de alocação dinâmica de largura de banda por SSID para otimizar o desempenho em ambientes de alta densidade de dispositivos;
- 3.1.53. Possuir, permitir, garantir, prover e implementar associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;
- 3.1.54. Possuir, permitir, garantir, prover e implementar um controle de acesso à rede (NAC - Network Access Control) que seja integrado à controladora Wi-Fi ou através de outra solução alternativa que execute essa funcionalidade. Esta solução deve ter a capacidade de identificar automaticamente o tipo de dispositivo conectado (profiling) e aplicar de maneira automática a política de acesso apropriada, assim como a VLAN de destino adequada;
- 3.1.55. As políticas de acesso à rede devem ser baseadas:
- 3.1.55.1. Em características do equipamento (Endereço MAC, Sistema Operacionais, entre outros);
- 3.1.55.2. Usuário conectado e autenticado à rede.
- 3.1.56. Possuir, permitir, garantir, prover e implementar recurso para indicar graficamente os dispositivos conectados em cada SSID, assim como a quantidade de tráfego e sessões referentes a eles nos últimos minutos e horas;
- 3.1.57. Possuir, permitir, garantir, prover e implementar visibilidade de quais aplicações estão trafegando pela rede Wi-Fi;
- 3.1.58. possuir, permitir, garantir, prover e implementar mecanismos de atualização automática para a detecção e classificação de aplicações. Deve incluir uma base de dados abrangente de aplicações *web*, organizada em categorias como jogos, compartilhamento de arquivos, aplicações comerciais, redes sociais e outros tipos relevantes. Essa base de dados deve ser atualizada continuamente pelo fabricante durante toda a vigência do contrato, assegurando visibilidade e controle do tráfego de rede.

3.1.59. Possuir, permitir, garantir, prover e implementar todas as funcionalidades passíveis de configuração através da Controladora *wireless*;

3.1.60. Possuir, permitir, garantir, prover e implementar ajuste automático de canais em caso de sobreposição de antenas adjacentes;

3.1.61. Possuir, permitir, garantir, prover e implementar funcionalidade de ajuste de potência automática de forma a estender cobertura no caso de falha de APs;

3.1.62. Possuir, permitir, garantir, prover e implementar recurso que detecte e controle a recepção de pacotes *wireless* com base em limiar de sinal configurável, assegurando que apenas sinais de força adequada sejam processados, contribuindo para a eficiência e o desempenho da rede ao minimizar a interferência de sinais fracos ou instáveis;

3.1.63. Possuir, permitir, garantir, prover e implementar filtro de aplicação capaz de reconhecer e bloquear conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais e outras categorias definidas. Esse controle deve permitir a aplicação de políticas específicas para grupos ou dispositivos, ajustando o acesso conforme as necessidades da rede. Caso o recurso exija licenciamento adicional, a licença deverá ser fornecida pelo período total de vigência do contrato da nova Rede, conforme este termo de referência;

3.1.64. Possuir, permitir, garantir, prover e implementar a capacidade de reconhecimento de aplicações utilizando a técnica de DPI (Deep Packet Inspection), permitindo monitorar o perfil de acesso dos usuários e implementar políticas de controle de tráfego de acordo com as necessidades da rede. Essa funcionalidade deve estar disponível durante todo o período de vigência do contrato do serviço;

3.1.65. Possuir, permitir, garantir, prover e implementar através da mesma técnica de DPI, identificar aplicações sensíveis ao negócio e permitir a priorização desse tráfego com a devida marcação de QoS (Quality of Service), garantindo que os serviços críticos tenham a largura de banda e prioridade adequadas para manter o desempenho exigido;

#### **4. Segurança do Serviço de Rede Sem Fio (SRSF)**

4.1. O Serviço de Rede Sem Fio (SRSF) deverá possuir, garantir e implementar mecanismos que assegurem a confidencialidade e integridade dos dados transmitidos, conforme os padrões de segurança da nova rede, atendendo aos seguintes requisitos mínimos:

4.1.1. Possuir, garantir e implementar a criptografia dos dados transmitidos em conformidade com os padrões mais elevados de segurança;

4.1.2. Possuir, garantir e implementar o uso de Wi-Fi Protected Access 2 (WPA2) ou superior por SSID, utilizando-se de AES e/ou TKIP para garantir a segurança das transmissões;

4.1.3. Possuir, garantir e implementar o uso de Wi-Fi Protected Access 3 (WPA3) ou superior por SSID, utilizando AES, para aumentar a segurança em conformidade com as melhores práticas de proteção de rede;

4.1.4. Permitir e garantir o controle de acesso por MAC Address, possibilitando a criação de listas de controle de dispositivos autorizados e bloqueados;

4.1.5. Permitir e garantir a criação de Múltiplos PSK para o mesmo SSID, podendo combinar um MAC a um MPSPK;

4.1.6. Possuir, garantir e implementar a configuração de controle de acesso via protocolo IEEE 802.1X/EAP, garantindo autenticação robusta e segura para os usuários da rede;

4.1.7. Deverá suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

4.1.8. Possuir, garantir e implementar a segmentação de rede utilizando o protocolo IEEE 802.1Q, possibilitando a criação de VLANs para a separação lógica e controle de tráfego de rede;

- 4.1.9. Possuir, garantir e implementar um sistema de detecção de intrusão (WIDS) para rede sem fio, com capacidade para detectar e bloquear ataques de Broadcast De-authentication, assegurando a integridade do ambiente *wireless*;
- 4.1.10. Possuir e implementar WIDS integrado com capacidade de detecção de ataques de Spoofed De-authentication, garantindo a proteção contra tentativas de falsificação de identidade de rede;
- 4.1.11. Possuir e garantir WIDS integrado com detecção de senhas WEP fracas, implementando ações preventivas para mitigar vulnerabilidades associadas a senhas de baixa segurança;
- 4.1.12. Possuir, garantir e implementar WIDS com capacidade de detectar bridges *wireless* não autorizadas, evitando comunicações não permitidas dentro da rede;
- 4.1.13. Possuir, garantir e implementar proteção contra-ataques do tipo ARP Poisoning na Controladora *wireless*, prevenindo ataques que visam a interceptação de comunicações;
- 4.1.14. Permitir, garantir e implementar a autenticação transparente de usuários da rede Wi-Fi em domínios LDAP, LDAP-AD, Windows ou compatível, integrando com os sistemas de autenticação da CONTRATANTE;
- 4.1.15. Permitir, garantir e implementar o bloqueio de tráfego interno entre usuários conectados ao mesmo SSID;
- 4.1.16. Permitir, garantir e implementar a configuração e o bloqueio de tráfego entre diferentes SSIDs, assegurando a segmentação adequada e a segurança de dados entre redes distintas;
- 4.1.17. Permitir, garantir e implementar o monitoramento garantindo a supressão de Pontos de Acesso indevidos (Rogue Access points) ou não autorizados, prevenindo interferências e brechas de segurança na rede;
- 4.1.18. Permitir, garantir e implementar a criptografia da comunicação entre os pontos de acesso sem fio e a Controladora Wireless, garantindo a integridade e segurança das informações gerenciadas.

## 5. Serviço de Rede Sem Fio Interno com Segurança

5.1. Requisitos específicos para o equipamento do tipo Solução unificada de segurança de rede sem fio Wi-Fi:

5.1.1. **Padrão Wi-Fi:** 802.11be (Wi-Fi 7), com compatibilidade com os padrões anteriores: 802.11ax (Wi-Fi 6), 802.11ac (Wi-Fi 5), 802.11n (Wi-Fi 4), 802.11g (Wi-Fi 3), 802.11a/b, garantindo maior capacidade de dados, melhor eficiência e menor latência;

5.1.2. **Bandas de Frequência:** Possuir no mínimo um rádio 2.4 GHz, possuir no mínimo um rádio 5 GHz e possuir no mínimo um rádio 6 GHz;

5.1.3. **Capacidade de Dados Mínima nas Frequências e MIMO:**

5.1.3.1. 2.4 GHz no mínimo 1 Gbps, MIMO 4x4;

5.1.3.2. 5.0 GHz no mínimo 5,7 Gbps, MIMO 4x4;

5.1.3.3. 6.0 GHz no mínimo 11 Gbps, MIMO 4x4;

5.1.4. **Largura do Canal:**

5.1.4.1. Frequência: 2.4 GHz, 20 MHz e 40 MHz;

5.1.4.2. Frequência: 5.0 GHz, 20 MHz, 40 MHz, 80 MHz e 160 MHz;

5.1.4.3. Frequência: 6.0 GHz, 20 MHz, 40 MHz, 80 MHz, 160 MHz e 320 MHz;

5.1.5. Possuir, permitir, garantir, prover e implementar no mínimo 06 (seis) antenas internas;

5.1.6. Possuir, permitir, garantir, prover e implementar ter o ganho mínimo das antenas internas sendo de no mínimo 4 dBi no rádio de 2.4Ghz, de no mínimo 5 dBi no rádio de 5Ghz e de no miminho 5 dBi no rádio de 6 Ghz;

5.1.7. Deve permitir, garantir, implementar a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deverá ser possível criar no mínimo até 08 (oito) SSIDs por rádio;

- 5.1.8. Suportar no mínimo 200 clientes simultâneos por Ponto de acesso (AP);
- 5.1.9. Possuir, permitir, garantir, prover e implementar sistema antifurto do tipo Kensington Security Lock ou similar ou qualquer solução de antifurto implementada pela CONTRATADA;
- 5.1.10. **Modulação:** 4096 QAM nas frequências de 5.0Ghz e 6.0Ghz, usada em todos os dispositivos Wi-Fi 7;
- 5.1.11. **MU-MIMO:** Possuir e garantir o uso de Multi-User MIMO em Uplink e Downlink, garantindo a comunicação simultânea com vários dispositivos;
- 5.1.12. **OFDMA:** Possuir e garantir o uso do Orthogonal Frequency-Division Multiple Access, garantindo que vários dispositivos compartilhem o espectro simultaneamente;
- 5.1.13. **BSS Coloring:** Possuir e garantir o uso de BSS Coloring para diferenciar redes Wi-Fi sobrepostas e reduzir interferências, melhorando o desempenho em ambientes de alta densidade de dispositivos.
- 5.1.14. **PoE (Power over Ethernet):** Possuir e garantir o uso do padrão (802.3bt);
- 5.1.15. Deve possuir uma fonte de energia em corrente alternada (AC) com capacidade de alimentação bivolt (110V/220V);
- 5.1.16. A fonte de alimentação deve ser original e adequada com as especificações do fabricante;
- 5.1.17. A fonte de alimentação deve ser fornecida pela CONTRATADA;
- 5.1.18. **Portas Ethernet:** Deve possuir 02 (duas) *interface* de rede sendo pelo menos uma de 10 Gbps;
- 5.1.19. O Ponto de Acesso rede sem fio interno deverá suportar a função de análise de spectrum, detecção de rogue APs e WIPS nas frequências 2.4GHz, 5GHz e 6GHz;
- 5.1.20. **MESH:** Possuir, permitir, garantir, prover e implementar o uso da Rede MESH em todas as frequências de 2.4 GHz, 5.0 GHz e 6 GHz;
- 5.1.21. **Fast Roaming:** Possuir e garantir o uso dos padrões, 802.11r, 802.11k e 802.11v;
- 5.1.22. Balanceamento de carga dinâmico: Possuir e garantir o uso, garantindo a distribuição eficiente de dispositivos entre APs;
- 5.1.23. *Failover* automático e tolerância a falhas: Possuir e garantir o uso, garantindo a continuidade da conexão em caso de falha de um AP ou interferência nas bandas de frequência;
- 5.1.24. **SNMP:** Possuir, permitir, garantir, prover e implementar o protocolo SNMP, para permitir o monitoramento e gerenciamento remoto do Ponto de Acesso rede sem fio pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;
- 5.1.25. **802.11e** (Enhanced Distributed Channel Access - EDCA): Possuir, permitir, garantir, prover e implementar o uso do padrão 802.11e EDCA para priorização de tráfego sensível à latência em redes Wi-Fi, permitindo a entrega eficiente de pacotes de voz e vídeo, com melhor qualidade de serviço (QoS) em ambientes de alta densidade;
- 5.1.26. **TWT (Target Wake Time):** Possuir, permitir, garantir, prover e implementar o Target Wake Time (TWT), permitindo que dispositivos negociem horários específicos de comunicação com o ponto de acesso, otimizando o consumo de energia e reduzindo o tempo de atividade necessário para dispositivos móveis e IoT, sem comprometer o desempenho de aplicações sensíveis ao tempo, como VoIP;
- 5.1.27. Possuir homologação da ANATEL válida, na entrega da proposta Técnica quando a LICITANTE vencedora do Certame, para análise da comissão Técnica do Processo Licitatório;

## 6. Serviço de Rede Sem Fio Temporário com Segurança

- 6.1. Os equipamentos SRSFT devem possuir as mesmas características técnicas dos “Ponto de Acesso rede sem fio interno (*Access point Indoor*)”.

6.2. O Serviço de Rede Sem Fio Temporária (SRSFT) deverá ser dimensionado e disponibilizado por um período de até 180 (cento e oitenta) dias na infraestrutura do Contratante Aderente, sendo interligado ao serviço de Acesso Dedicado contratado. A Ordem de Serviço que autoriza a instalação dos SRSFTs deve estabelecer o período exato de uso destes serviços temporários, não podendo exceder a 180 (cento e oitenta) dias, ficando explicitamente autorizada a desativação automática após o período exato estabelecido. Sendo a utilização em período menor que os 180 dias paga na fração correspondente ao mês;

6.3. Para o (SRSFT) não será necessário a realização do Site Survey.

## 7. Serviço de Rede Sem Fio Externo com Segurança

7.1. Requisitos específicos para o equipamento do tipo Solução unificada de segurança de rede sem fio Wi-Fi:

7.1.1. **Padrão Wi-Fi:** 802.11ax (Wi-Fi 6), com compatibilidade com os padrões anteriores: 802.11ac (Wi-Fi 5), 802.11n (Wi-Fi 4), 802.11g (Wi-Fi 3), 802.11a/b, garantindo maior capacidade de dados, melhor eficiência e menor latência;

7.1.2. **Bandas de Frequência:** Possuir um rádio 2.4 GHz e um rádio 5 GHz, *sendo que o MESH/Backhaul deverá ser disponibilizado pelo rádio de 5 GHz.*

7.1.3. **Capacidade de Dados Mínima nas Frequências e MIMO:**

7.1.3.1. 2.4 GHz — Capacidade mínima de 250 Mbps, com MIMO 2x2 (ou superior);

7.1.3.2. 5.0 GHz — Capacidade mínima de 2 Gbps, MIMO 2x2 (ou superior);

7.1.4. **Largura do Canal:**

7.1.4.1. Frequência: 2.4 GHz, bandas: mínimo de 20 MHz;

7.1.4.2. No Mínimo para frequência: 5.0 GHz, bandas: 20 MHz, 40 MHz e 80 MHz;

7.1.5. Possuir no mínimo 04 (quatro) antenas, por ser uma solução externa deve ter a necessidade de direcionar o sinal, podendo utilizar de antenas internas (built-in) ou externas (montáveis). A CONTRATADA deverá indicar a configuração mais adequada (ganho e polarização) de acordo com a necessidade do ambiente de instalação e registrado no site survey.

7.1.6. Possuir no mínimo uma antena com ganho/banda a seguir, 4 dBi para 2.4GHz e 5.5 dBi para 5 GHz;

7.1.6.1. No caso específico de equipamento que possui apenas antenas internas (built-in):

7.1.6.1.1 Não é obrigatória a presença de conectores N-type (ou equivalentes), uma vez que as antenas são parte integrante do equipamento e de sua homologação;

7.1.6.2. No caso de equipamento que possui antenas externas montáveis:

7.1.6.2.1 O equipamento deverá possuir conectores N-type (ou equivalentes);

7.1.6.2.2. Os requisitos de ganho (4 dBi em 2.4 GHz e 5.5 dBi em 5 GHz) devem ser comprovados nas especificações técnicas do fabricante, tanto para antenas internas quanto externas.

7.1.6.2.3. O fornecimento das antenas externas, quando adotadas, deverá ocorrer sem ônus adicional para a CONTRATANTE.

7.1.7. Possuir, permitir, garantir, prover e implementar a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deverá permitir e ser possível criar no mínimo 08 (oito) SSIDs por rádio;

7.1.8. Modulação: 1024 QAM nas frequências de 5.0GHz;

7.1.9. **MU-MIMO:** Possuir e garantir o uso de Multi-User MIMO em Uplink e Downlink, garantindo a comunicação simultânea com vários dispositivos;

7.1.10. **OFDMA:** Possuir e garantir o uso do Orthogonal Frequency-Division Multiple Access, garantindo que vários dispositivos compartilhem o espectro simultaneamente;

7.1.11. **BSS Coloring:** Possuir e garantir o uso de BSS Coloring para diferenciar redes Wi-Fi sobrepostas e reduzir interferências, melhorando o desempenho em ambientes de alta densidade de dispositivos.

7.1.12. Características da Potência Energética:

7.1.12.1. **PoE (Power over Ethernet):**

7.1.12.1.1. O equipamento deve possuir e garantir o uso do padrão **802.3bt**, assegurando dispositivos de alta performance e eficiência energética;

7.1.12.2. **Alternativa ao PoE 802.3bt, caso esse padrão não esteja disponível:**

7.1.12.2.1. O equipamento deve possuir e garantir o uso do padrão 802.3at (PoE+), assegurando a alimentação adequada; ou

7.1.12.2.2. O equipamento deve ser instalado ligado diretamente na rede elétrica utilizando uma fonte de energia externa. Os dispositivos precisam ter uma potência mínima entre 30W e 40W, conectando-se diretamente à rede elétrica;

7.1.12.3. **Infraestrutura de Energia:**

7.1.12.3.1. Toda a infraestrutura necessária para a alimentação de energia, incluindo fonte de alimentação, cabos, conectores, calhas, fios e demais componentes, será provida pela CONTRATADA.

7.1.12.3.2. Apenas a alimentação de energia será fornecida pela CONTRATANTE.

7.1.12.3.3. Além do padrão PoE (802.3bt/802.3at), o equipamento deve possuir uma fonte de energia em corrente alternada (AC) com capacidade de alimentação bivolt (110V/220V);

7.1.12.3.4. A fonte de alimentação deve ser original e adequada com as especificações do fabricante;

7.1.12.3.4.1. A fonte de alimentação deve ser fornecida pela CONTRATADA;

7.1.13. Deverá possuir no mínimo 01 (uma) interface de rede Multi-Gigabit (mGig) de **2.5 Gbps** (ou superior);

7.1.14. **IP67:** Deverá atender à classificação de proteção IP67, assegurando resistência total à poeira e proteção contra imersão temporária em água;

7.1.15. O Ponto de Acesso rede sem fio externo deverá suportar a função de análise de spectrum, detecção de rogue APs e WIPS nas frequências 2.4GHz e 5GHz;

7.1.16. **MESH:** Possuir e garantir o uso da Rede MESH em todas as frequências de 2.4 GHz e 5.0 GHz;

7.1.17. **Fast Roaming:** Possuir e garantir o uso dos padrões, 802.11r, 802.11k e 802.11v;

7.1.18. Balanceamento de carga dinâmico: Possuir e garantir o uso, garantindo a distribuição eficiente de dispositivos entre APs;

7.1.19. **Failover automático e tolerância a falhas:** Possuir e garantir o uso, garantindo a continuidade da conexão em caso de falha de um AP ou interferência nas bandas de frequência;

7.1.20. **SNMP:** Deverá suportar o protocolo SNMP, para permitir o monitoramento e gerenciamento remoto do Ponto de Acesso rede sem fio pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

7.1.21. **802.11e (Enhanced Distributed Channel Access - EDCA):** Possuir e garantir o uso do padrão 802.11e EDCA para priorização de tráfego sensível à latência em redes Wi-Fi, permitindo a entrega eficiente de pacotes de voz e vídeo, com melhor qualidade de serviço (QoS) em ambientes de alta densidade;

7.1.22. **TWT (Target Wake Time):** Deverá suportar ao Target Wake Time (TWT), permitindo que dispositivos negociem horários específicos de comunicação com o ponto de acesso, otimizando o consumo de energia e reduzindo o tempo de atividade necessário para dispositivos móveis e IoT, sem comprometer o desempenho de aplicações sensíveis ao tempo, como VoIP;

7.1.23. Possui homologação da ANATEL válida;

7.1.24. Prover, de acordo com a anuência da Contratante Aderente e a aprovação da ATI-PE, bridge *wireless* para interligação entre pontos de acesso.

## 8. Serviço de Rede Sem Fio switches para interligação dos Access Points (APs) e interligação com a rede Local.

### 8.1. Características Gerais:

Tabela 1 - Especificações mínimas da solução

Item	Especificação	Quantidades de portas do Switches
1	10 Gigabit Ethernet com conectores SFP+	4
2	Multigigabit Ethernet 2.5G (simultaneamente) com conectores RJ-45	8

8.1.1. Deve possuir, no mínimo, 4 portas 10 Gigabit Ethernet padrão SFP+ ou 10GBASE-T.  
8.1.1.1 O transceiver a ser fornecido dependerá dos resultados do site survey do local, de modo a garantir a melhor adequação às condições e requisitos da infraestrutura existente no PCS.

8.1.2. Deve possuir, no mínimo, 8 portas Multigigabit Ethernet 2.5G (simultaneamente) com conectores RJ-45;

8.1.3. Deverá implementar os padrões IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt com PoE budget de 180W;

8.1.4. A solução deve suportar, permitir e garantir o acesso administrativo ao equipamento.

8.1.4.1. Quando ofertada em modelo local (on-premises), a solução deverá possuir porta console para acesso à interface de linha de comando (CLI) por conexão serial, devendo ser fornecidos todos os cabos e adaptadores necessários para configuração direta e manutenção.

8.1.4.2. Quando ofertada em modelo de gerenciamento em nuvem, a solução deverá assegurar funcionalidades equivalentes de administração, rastreabilidade, segurança e controle de acesso, garantindo proteção e integridade das informações administrativas da rede, conforme os requisitos deste Termo de Referência.

8.1.5. A CONTRATADA poderá substituir a interface USB física por funcionalidades equivalentes disponibilizadas via Dashboard ou API, desde que estas permitam, de forma segura e autenticada, a execução de procedimentos de backup, captura de logs, atualização de firmware e restauração de configurações. A solução deverá garantir o mesmo nível de segurança, rastreabilidade e controle administrativo que seria obtido com o uso de uma interface USB física, atendendo integralmente a todos os requisitos técnicos e de gestão previstos neste Termo de Referência e seus Adendos.

8.1.6. Deve suportar no mínimo 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

8.1.7. Deve possuir capacidade de vazão de no mínimo 60 Gbps;

8.1.8. Deve possuir capacidade de encaminhamento de no mínimo 170 Mpps;

8.1.9. Deve possuir capacidade de armazenamento de no mínimo 16.000 (dezesesseis mil) entradas de endereços MAC;

8.1.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

8.1.11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

- 8.1.12. Deve suportar a comutação de Jumbo Frames;
- 8.1.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 8.1.14. Deve implementar serviço de DHCP Relay;
- 8.1.15. Deve suportar IGMP snooping para controle de tráfego de multicast;
- 8.1.16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 8.1.17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).
- 8.1.18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 8.1.19. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 8.1.20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- 8.1.21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
- 8.1.22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 8.1.23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 8.1.24. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 8.1.25. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;
- 8.1.26. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 8.1.27. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 8.1.28. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 8.1.29. Deve suportar autenticação por endereço MAC (MAC Authentication Bypass – MAB), inclusive sob outras nomenclaturas ou classificações adotadas por fabricantes que representem a mesma funcionalidade;
- 8.1.30. Deve implementar RADIUS CoA (Change of Authorization);
- 8.1.31. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 8.1.32. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 8.1.33. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

- 8.1.34. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
- 8.1.35. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
- 8.1.36. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
- 8.1.37. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 8.1.38. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 8.1.39. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 8.1.40. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota por meio de CLI (Command Line Interface), quando aplicável a modelos de gerenciamento local.
- 8.1.40.1. Para soluções baseadas em nuvem (Cloud Managed), a administração poderá ocorrer por interface gráfica (Dashboard) ou API segura, desde que essas ferramentas assegurem controle administrativo, rastreabilidade, autenticação, segurança e nível de governança equivalentes ao acesso via CLI, atendendo integralmente aos requisitos de gerenciamento definidos neste Termo de Referência.
- 8.1.41. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 8.1.42. Deve permitir ser gerenciado através de IPv6;
- 8.1.43. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 8.1.44. Deve suportar autenticação via RADIUS e TACACS+, ou outra tecnologia que permita acesso seguro para controle do acesso administrativo ao equipamento;
- 8.1.45. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 8.1.46. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 8.1.47. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 8.1.48. Deverá suportar ser configurado e monitorado através de REST API;
- 8.1.49. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 8.1.50. Todos os acessórios para montagem e fixação deverão ser fornecidos;

## 9. Serviço de Garantia de Qualidade Contínua do SRSF

9.1. Considerando a importância crítica do SRSF, que suporta operações essenciais como serviços de voz, vídeo e atendimento a servidores do Estado de Pernambuco e à população em geral, além da implementação de novas tecnologias, como Wi-Fi 7 e topologia Mesh, é necessário garantir que a qualidade da rede seja mantida de forma contínua. Essa garantia inclui reavaliações periódicas e ajustes, conforme necessário, para assegurar a estabilidade e o desempenho consistente da rede Wi-Fi, especialmente em aplicações críticas que exigem alta disponibilidade e confiabilidade;

9.2. O Serviço de Garantia de Qualidade Contínua do SRSF, consiste em um conjunto de atividades destinadas a assegurar que a rede Wi-Fi opere de forma otimizada e confiável ao longo do tempo. O escopo desse serviço inclui o Planejamento e Execução do Site Survey, onde é realizada uma análise detalhada do ambiente para identificar a melhor configuração da rede; Métricas de Desempenho da Solução, com a coleta e avaliação de indicadores técnicos para garantir a capacidade e eficiência do sistema; e a elaboração de um Relatório Final do Site Survey, contendo os resultados da análise e recomendações. Após isso, ocorre a Implantação, onde os equipamentos são instalados e configurados conforme o planejamento inicial, seguida por um Período de Avaliação para monitorar a performance da rede. A etapa de Validação Final do Sinal Wi-Fi verifica se o sinal está adequado em toda a área de cobertura, culminando no Recebimento Definitivo, que formaliza a conclusão do serviço com garantias de funcionamento.

### 9.3. Planejamento e Execução do Site Survey

9.3.1. A instalação dos pontos de acesso, inclusive em topologias de Wi-Fi Mesh, deverá ser precedida de uma análise técnica do ambiente real, apoiada por ferramentas e *softwares* adequados, garantindo:

9.3.1.1. Melhor posicionamento dos Pontos de Acesso, tanto principais quanto secundários (Mesh, híbrido ou cabeado), para maximização da cobertura de radiofrequência e cumprimento das métricas de qualidade;

9.3.1.2. Determinação da quantidade exata de pontos de acesso por localidade/andar, considerando a necessidade de *backhaul* eficiente;

9.3.1.3. Identificação de fontes e zonas de interferência que possam impactar a comunicação entre os pontos de acesso e o *backhaul*, seja este cabeado ou sem fio, de forma a garantir estabilidade, throughput e qualidade do enlace de retorno da rede.

9.3.1.4. Definição de canais de frequência para cada Ponto de Acesso, com especial atenção à separação dos canais de dados e do *backhaul* nas frequências adequadas (5 GHz e 6 GHz), considerando os resultados do site survey e as condições técnicas do ambiente.

9.3.1.5. Desenhos coloridos com áreas de cobertura e faixas de níveis de recepção de sinal de RF, incluindo o mapeamento da topologia Mesh e a cobertura do *backhaul*;

9.3.1.6. A realização dos serviços deve ser planejada conforme a disponibilidade da CONTRATANTE ou CONTRATANTE aderente. Caso o CONTRATANTE opte em realizar o planejamento prévio pode ser feito remotamente, por meio de *webconferência* e *videoconferência*. A CONTRATANTE fornecerá plantas baixas das edificações. Caso essas plantas não estejam disponíveis ou não contenham informações suficientes, a CONTRATADA deverá realizar visitas in loco para analisar espessuras e materiais das paredes e outros detalhes da edificação, elaborando um croqui detalhado. O site survey também deve considerar possíveis variações no ambiente, como mudanças na densidade de usuários e obstáculos que possam afetar o *backhaul* da rede Mesh;

### 9.4. Métricas de Desempenho da Solução

9.4.1. A Solução deverá ter abrangência de cobertura em todas as instalações da edificação, tanto para os pontos de acesso principais quanto para a comunicação entre nós Mesh (*backhaul*). A Solução deverá ter cobertura de 100% (cem por cento) nas áreas produtivas – onde estão distribuídas as estações de trabalho, salas de reuniões e *videoconferência*, salas de treinamentos, bibliotecas, salas de convivência, halls de entrada, corredores e escadas. Deverá existir o mínimo de sinal nas áreas de acesso externo, como estacionamento, e de acesso restrito, como por exemplo salas dos *datacenters*. Nas demais áreas, tais como: banheiros, copas, salas do ar-condicionado, geradores e elevadores, a CONTRATANTE deverá definir ou não pela cobertura;

#### 9.4.2. Características da Rede Mesh:

9.4.2.1. A topologia Wi-Fi Mesh deverá garantir cobertura ampla, redundância e alta eficiência espectral, assegurando conectividade estável mesmo em ambientes com barreiras físicas ou alta densidade de dispositivos.

9.4.2.2. Cada PCS poderá conter múltiplas malhas Mesh, compostas por até 8 (oito) Pontos de Acesso (APs), sendo 1 (um) AP raiz conectado à rede LAN por meio de interface 10 GbE (cabo Cat. 6A ou fibra óptica com conversor SFP+), e até 7 (sete) APs adicionais interligados via backhaul sem fio em 5 GHz e/ou 6 GHz, conforme melhores práticas de mitigação de interferências e balanceamento de carga.

9.4.2.3. O backhaul entre os APs deve ser dimensionado para suportar largura de banda elevada, baixa latência e alta disponibilidade, garantindo o desempenho, a resiliência e a continuidade do serviço conforme os níveis mínimos de qualidade definidos neste Termo de Referência.

#### 9.4.3. SSID para Voz

9.4.3.1. Para otimizar a qualidade de chamadas VoIP, é necessário um SSID dedicado unicamente ao tráfego de voz. Esse SSID deve possuir as seguintes características:

9.4.3.1.1. Prioridade de tráfego (QoS/WMM): Implementar mecanismos de Qualidade de Serviço (QoS), como o Wi-Fi Multimedia (WMM), que garantam a priorização do tráfego de voz em relação a outros tipos de dados, reduzindo latência, jitter e evitando a perda de pacotes.

9.4.3.1.2. Isolamento de tráfego: O SSID deve estar isolado dos SSIDs de dados e entretenimento, para evitar que o tráfego de voz seja afetado por congestionamentos ou interferências, assegurando uma comunicação fluida;

9.4.3.1.3. Canal dedicado e separação de frequências: Sempre que possível, utilizar canais de frequência dedicados para o SSID de voz, especialmente em 5 GHz ou 6 GHz, para minimizar interferências e garantir a estabilidade das chamadas;

9.4.3.2. Essa configuração de um SSID dedicado à voz permitirá que a rede suporte um grande volume de chamadas VoIP com a qualidade necessária para ambientes críticos, como instituições governamentais.

#### 9.4.4. Demais requisitos mínimos da rede Wi-Fi:

9.4.4.1. Relação Sinal/Ruído mínima de 20 dB, tanto para o tráfego de dados quanto para a comunicação do *backhaul* Mesh;

9.4.4.2. Nível de sinal mínimo de -60 dBm para 2.4 GHz e -65 dBm para 5 GHz e 6 GHz, com especial atenção à qualidade do sinal para o *backhaul*;

9.4.4.3. Utilização de CPU e memória dos ativos de rede abaixo de 70%, com exceção de casos extraordinários.

#### 9.5. Relatório Final do Site Survey

9.5.1. O planejamento dos serviços deve resultar em um documento de escopo de trabalho contendo o detalhamento dos serviços que serão executados, contendo no mínimo:

9.5.1.1. Premissas técnicas e operacionais do projeto, incluindo a topologia de implantação (Mesh, cabeada ou híbrida), arquitetura de backhaul, critérios de dimensionamento e parâmetros de desempenho mínimos exigidos;

9.5.1.1.1. Mapa detalhado de cobertura e posicionamento proposto dos Pontos de Acesso (APs), com indicação de áreas de sombra, sobreposição de sinal, densidade de usuários e interferências detectadas durante o levantamento;

9.5.1.2. Local, horários e condições de execução dos serviços;

9.5.1.3. Pontos de contato da CONTRATANTE e CONTRATADA;

9.5.1.4. Cronograma faseado do projeto, dividido em etapas, com responsáveis e data de início e fim (se aplicável);

9.5.1.5. Relação da documentação a ser entregue ao final da execução dos serviços;

9.5.1.6. Responsabilidade da CONTRATANTE e CONTRATADA;

9.5.1.7. Itens excluídos no projeto;

9.5.1.8. Termo de aceite;

**9.5.2. O relatório deve conter todas as informações coletadas, incluindo:**

9.5.2.1. Mapas de calor/cobertura em 2.4GHz, 5GHz e 6GHz, com especial ênfase na cobertura e qualidade do *backhaul* Mesh;

9.5.2.2. Localização sugerida dos pontos de acesso, relação sinal/ruído e interferências, tanto para tráfego de usuários quanto para o *backhaul* entre os nós Mesh;

9.5.2.3. Taxas de transferência esperadas, listagem de pontos de acesso, *switches*, cabos e outros elementos necessários para a infraestrutura Mesh;

9.5.2.4. Recomendações de melhorias e escalabilidade para o futuro, incluindo opções para otimização do *backhaul*;

## 9.6. Implantação e instalação

9.6.1. A CONTRATADA é integralmente responsável por fornecer, instalar e operacionalizar toda a infraestrutura necessária, incluindo cabos de Categoria 6A, fibras ópticas, os conversores de fibra para RJ45 **SFP+** com suporte a velocidades de 10 Gbps, calhas e tomadas para os pontos de acesso (APs) e os equipamentos que forem necessários energia. É imperativo que todos os componentes essenciais ao funcionamento dos APs no ambiente do Ponto Conectado Seguro (PCS) estejam contemplados. A implantação da rede Wi-Fi, incluindo a topologia Mesh, deve estritamente seguir as recomendações e o planejamento definidos no site survey, assegurando conformidade com as métricas de qualidade e cobertura estipuladas.

9.6.2. Para a instalação dos itens de serviços deste Termo de Referência e deste ADENDO IV para os pontos de acesso (APs), *switches*, cabos e demais equipamentos, a CONTRATADA deverá:

9.6.2.1. Seguir o *Layout* Planejado, garantindo que todos os pontos de acesso e nós Mesh sejam instalados nos locais definidos, respeitando o posicionamento ideal para maximização da cobertura e desempenho, inclusive do *backhaul*;

9.6.2.2. Documentar a Instalação:

9.6.2.2.1. Registrar fotos detalhadas de cada equipamento instalado, incluindo:

9.6.2.2.2. Fotos das áreas internas e externas onde os pontos de acesso foram posicionados;

9.6.2.2.3. Fotos do cabeamento utilizado, mostrando claramente as passagens e conexões;

9.6.2.2.4. Fotos dos racks e armários onde *switches* e outros equipamentos de rede foram instalados.

9.6.2.3. Validação Física:

9.6.2.3.1. Certificar-se de que os equipamentos instalados estejam configurados e operando conforme especificado no site survey, incluindo a verificação da comunicação de *backhaul* nos nós Mesh;

9.6.2.4. Testes de Funcionamento:

9.6.2.4.1. Realizar testes preliminares em cada ponto de acesso, validando sua operação antes da entrega final. Esses testes devem incluir:

9.6.2.4.1.1. Conectividade de rede e taxas de transferência, tanto para o tráfego de usuários quanto para o *backhaul*;

9.6.2.4.1.2. Verificação da energia e ventilação dos equipamentos;

9.6.2.4.1.3. Confirmação de que os canais de frequência estão configurados corretamente, incluindo a separação entre dados, voz e *backhaul*;

9.6.3. A implantação só será considerada completa após a entrega e aprovação do relatório de implantação, juntamente com a realização dos testes de conformidade descritos.

## 9.7. Período de Avaliação

9.7.1. Após a implementação, será realizado um período de avaliação de 15 dias corridos. Durante esse período, a CONTRATADA deverá ajustar quaisquer falhas ou problemas que sejam identificados. O monitoramento será feito em tempo real, com logs automáticos e testes no ambiente. O desempenho do *backhaul* Mesh será monitorado para garantir a estabilidade. Caso a implementação não resulte em um serviço adequado que atenda às métricas especificadas, será solicitada a realização presencial de site survey com auxílio de ferramentas específicas para este fim, bem como eventual adequação de instalações físicas e configurações.

## 9.8. Validação Final do Sinal Wi-Fi

9.8.1. Após a implementação e ajustes decorrentes do período de avaliação, deverá ser realizada uma validação final da cobertura e qualidade do sinal da rede Wi-Fi, tanto para os usuários quanto para o *backhaul* Mesh, em toda a área coberta pela rede, utilizando ferramentas de medição avançadas, como analisadores de espectro portáteis ou equivalentes, que permitam medições precisas e em tempo real dos seguintes parâmetros:

9.8.1.1. Níveis de Sinal (dBm) e qualidade de *backhaul*: Medição detalhada da intensidade do sinal e da qualidade do *backhaul* Mesh em cada ponto da área coberta.

9.8.1.2. Relação Sinal/Ruído (SNR), tanto para tráfego de usuários quanto para o *backhaul*.

9.8.1.3. Mapas de Calor Atualizados, refletindo a condição final da rede, incluindo a topologia Mesh e o *backhaul*.

9.8.1.4. Taxas de Transferência (Mbps) em toda a área coberta, tanto para usuários quanto para o *backhaul* Mesh.

9.8.1.5. Análise de Roaming e de continuidade de *backhaul* entre os nós Mesh.

9.8.2. A contratada deverá apresentar um relatório final de validação, contendo os resultados detalhados das medições e testes realizados, confirmando se o projeto atende plenamente às métricas de qualidade estipuladas ou se ajustes adicionais são necessários. O relatório deverá incluir, no mínimo:

9.8.2.1. Mapas de calor atualizados.

9.8.2.2. Relatório de níveis de sinal (dBm) e relação sinal/ruído (SNR), tanto para as frequências de dados quanto para as frequências do *backhaul*.

9.8.2.3. Desempenho de *throughput* para diferentes tipos de frequências.

## 9.9. Recebimento Definitivo e o Monitoramento Contínuo do Serviço.

9.9.1. Após o “Recebimento Definitivo”, a CONTRATADA continuará responsável pelo pleno funcionamento da rede, especialmente em casos de reconfigurações ou mudanças de *layout*. O replanejamento da rede, incluindo o *backhaul* Mesh, deve seguir o processo normal de site survey e será realizado sem custos adicionais a ATI-PE.

9.10. Sempre que solicitado pela CONTRATANTE, seja em decorrência de mudanças de *layout*, obras ou em caso de uma quantidade excessiva de chamados de suporte relacionados ao Wi-Fi ou ao *backhaul* Mesh, a contratada deverá executar novamente os serviços de validação, ajuste de cobertura ou replanejamento da rede, incluindo site surveys adicionais, sem custos adicionais.

## ADENDO V – SERVIÇO DE CONECTIVIDADE DE REDE LOCAL

### 1. Objetivo

1.1. Este Adendo tem como objetivo definir os requisitos e condições para a contratação de serviços necessários para a execução do novo projeto de conectividade à internet, aprimorando a infraestrutura de tecnologia da informação do Governo do Estado de Pernambuco, buscando estabelecer as diretrizes e especificações técnicas para a seleção de

fornecedores qualificados, garantindo que os serviços contratados atendam aos padrões de qualidade e eficácia esperados, em conformidade com as legislações vigentes.

## 2. Definições

**2.1. Links de Acesso (LA):** São circuitos de dados, conhecidos como links ou conexões de última milha, que deverão ter os tipos de acessos à Internet com as características e funcionalidades descritas neste adendo e serão divididos em 3 (três) tipos, de acordo com as características técnicas de cada acesso, a saber:

- a) Links de Acesso Permanente (LAP);
- b) Links Multitecnologia Especial (LME);
- c) Link de Acesso Temporário (LAT).

### 2.1.1. Links de Acesso Permanente (LAP)

2.1.1.1. São os circuitos destinados às conexões dos Pontos Conectados Seguros (PCSs) da Nova Rede Corporativa e serão disponibilizados em dois tipos: Links de Acesso Permanente Tipo 1 (**LAP Tipo 1**) e Links de Acesso Permanente Tipo 2 (**LAP Tipo 2**).

2.1.1.2. Os circuitos **LAP Tipo 1** correspondem aos **Links de Banda Larga (LBL)** com velocidade de **500 Mbps**, sendo facultado à CONTRATADA optar pela entrega de **Links Dedicados (LD)** com velocidade de **300 Mbps**.

2.1.1.3. Os circuitos **LAP Tipo 2** correspondem aos **Links de Banda Larga (LBL)** com velocidade de **1 Gbps**, sendo facultado à CONTRATADA optar pela entrega de **Links Dedicados (LD)** com velocidade de **500 Mbps**.

2.1.1.4. As definições dos **Links de Banda Larga (LBL)** e **Links Dedicados (LD)** encontram-se na sequência deste adendo. A CONTRATADA deverá garantir total conformidade com as normas e padrões técnicos aplicáveis, incluindo as regulamentações da ANATEL, bem como os requisitos estabelecidos neste Termo de Referência.

2.1.1.4.1 A equivalência entre **Links de Banda Larga (LBL)** e **Links Dedicados (LD)** se aplicam de forma equivalente aos **Links Multitecnologia Especial (LME)** e **Link de Acesso Temporário (LAT)**:

2.1.1.4.1.1 Os circuitos **LME Tipo 1** e **LAT Tipo 1** devem ser entregues com **Tecnologias satelitais (MEO ou LEO)** com velocidade de **200 Mbps**;

2.1.1.4.1.2 Os circuitos **LME Tipo 2** e **LAT Tipo 2** devem ser entregues com **Links de Banda Larga (LBL)** com velocidade de **500 Mbps**, sendo facultado à CONTRATADA optar pela entrega de **Links Dedicados (LD)** com velocidade de **300 Mbps**;

2.1.1.4.1.3 Os circuitos **LME Tipo 3** e **LAT Tipo 3** devem ser entregues com **Links de Banda Larga (LBL)** com velocidade de **1 Gbps**, sendo facultado à CONTRATADA optar pela entrega de **Links Dedicados (LD)** com velocidade de **500 Mbps**.

2.1.1.5. Na operacionalização dos LAPs devem ser utilizadas tecnologias de acesso: preferencialmente fibra ótica ou outras tecnologias desde que aprovadas pela ATI com justificativa técnica.

2.1.1.6. Pelo menos 92% (noventa e dois por cento) dos Links de Acesso (LA) devem ser compostos por circuitos do tipo LAP. Percentuais inferiores devem ser expressamente aprovados pela Agência Estadual de Tecnologia da Informação (ATI).

### 2.1.1.7. Links Banda Larga (LBL)

2.1.1.7.1. São circuitos destinados às conexões dos Pontos Conectados Seguros (PCSs) da Nova Rede Corporativa, utilizando conexões de banda larga fixa. Esses circuitos devem atender às regulamentações vigentes da Agência Nacional de Telecomunicações (Anatel) ([Banda Larga — Agência Nacional de Telecomunicações — https://www.gov.br/anatel/pt-br/consumidor/conheca-seus-direitos/banda-larga](https://www.gov.br/anatel/pt-br/consumidor/conheca-seus-direitos/banda-larga)), especialmente a Resolução nº

614/2013, que regulamenta o Serviço de Comunicação Multimídia (SCM), permitindo o acesso à Internet de forma assimétrica e oferecer condições adequadas para suportar as demandas de conectividade previstas no contrato, com estabilidade e desempenho contínuos.

2.1.1.7.2. O serviço Links de Banda Larga (LBL) poderá ser contratado nas velocidades iniciais de 500 Mbps e 1 Gbps, por meio dos itens de serviço correspondentes aos Links de Acesso Permanente (LAP) Tipo 1 ou Tipo 2, conforme as demandas específicas de cada Ponto Conectado Seguro (PCS).

#### 2.1.1.8. Links Dedicados (LD)

2.1.1.8.1. São circuitos utilizados nas conexões dos Pontos Conectados Seguros (PCSs) da Nova Rede Corporativa, caracterizados por fornecerem links simétricos (taxa de download igual à taxa de upload) e uma conexão dedicada entre o provedor de serviços de internet (ISP) e a CONTRATANTE. Esses circuitos devem garantir largura de banda constante, com 100% de garantia da banda contratada, sem qualquer degradação de desempenho.

2.1.1.8.2. A taxa de transmissão de dados instantânea, tanto para download quanto para upload, deve corresponder integralmente à banda contratada, sem variações ou limitações que comprometam a capacidade exigida.

2.1.1.8.3. A CONTRATADA deve assegurar que a conexão seja exclusiva e não compartilhada, garantindo que a largura de banda contratada esteja sempre disponível para a CONTRATANTE, mesmo em períodos de alta demanda.

2.1.1.8.4. O serviço Link Dedicado (LD) poderá ser contratado nas velocidades iniciais de 300 Mbps e 500 Mbps, por meio dos itens de serviço correspondentes aos Links de Acesso Permanente (LAP) Tipo 1 ou Tipo 2, conforme as demandas específicas de cada Ponto Conectado Seguro (PCS).

2.1.1.8.5. As tecnologias de acesso utilizadas devem atender aos seguintes requisitos:

2.1.1.8.5.1. Conexão Simétrica: Taxa de upload igual à de download;

2.1.1.8.5.2. Garantia de Banda: 100% da capacidade contratada;

#### 2.1.2. Links Multitecnologia Especial (LME)

2.1.2.1. Estes links poderão ser usados nas conexões com os PCSs da Nova Rede Corporativa para permitir a comunicação de acesso à Internet, quando a CONTRATADA comprovar inviabilidade de atendimento do acesso com a tecnologia de banda larga e/ou dedicado.

2.1.2.1.1. Para comprovar a inviabilidade de atendimento referida no item, a CONTRATADA deverá apresentar toda e qualquer documentação solicitada pela ATI, no prazo estipulado pela própria ATI, para que a área técnica responsável possa elaborar parecer técnico.

2.1.2.1.2. A área técnica da ATI responsável pela gerência da rede corporativa emitirá parecer técnico aprovando a contratação do LME com base nos documentos e normativos que achar necessário.

2.1.2.1.3. O CONTRATANTE precisará formalizar a anuência ao parecer técnico da ATI para que a CONTRATADA possa seguir com os procedimentos necessários ao atendimento do PCS através de LME.

2.1.2.1.4. Com exceção do LME tipo 1, os links de acesso LME não deverão ultrapassar 8% (oito por cento) do total de circuitos contratados através da Nova Rede Corporativa, quando a finalidade for a substituição da obrigatoriedade do atendimento do LAP.

2.1.2.1.5. Caso, durante a implantação ou operação da rede, seja identificada pela CONTRATADA a necessidade técnica de ultrapassar o limite percentual estabelecido, esta deverá apresentar justificativa técnica formal, devidamente fundamentada e acompanhada de documentação comprobatória, para análise e posicionamento da ATI.

2.1.2.2. A CONTRATANTE poderá contratar os serviços LME Tipo 2 e 3 escolhendo a tecnologia que melhor se adeque às suas demandas específicas. Essa contratação poderá ocorrer sem se submeter às limitações de quantitativos estabelecidos no item 2.1.2.1.4, quando houver necessidade de:

- Conexões redundantes (além das já previstas neste Termo de Referência);
- Interconexões ponto-a-ponto;
- Outras aplicações consideradas especiais pela CONTRATANTE.

2.1.2.3. O serviço **Link Multitecnologia Especial (LME)** poderá ser contratado em três categorias, conforme as especificações abaixo:

2.1.2.3.1. **LME Tipo 1:** Velocidade inicial de **200 Mbps**, podendo ser fornecido por tecnologias satelitais (MEO ou LEO).

2.1.2.3.2. **LME Tipo 2:** Velocidade inicial de **500 Mbps**, podendo ser provido por qualquer uma das tecnologias de acesso permitidas neste Adendo ou mediante aprovação técnica da ATI.

2.1.2.3.3. **LME Tipo 3:** Velocidade inicial de **1 Gbps**, podendo ser provido por qualquer uma das tecnologias de acesso permitidas neste Adendo ou mediante aprovação técnica da ATI.

2.1.2.4. Os LMEs, para aplicações especiais, podem ser providos a partir de tecnologias e recursos diversos de telecomunicações apropriados para esses fins a exemplo de Satélites do tipo MEO ou LEO, Banda Larga, Dedicado e tecnologia 5G FWA.

2.1.2.5. **Atendimento ao Distrito Estadual de Fernando de Noronha:**

2.1.2.5.1. Para os PCSs localizados no Distrito Estadual de Fernando de Noronha, os Links Multitecnologia Especial (LME) poderão ser providos por soluções baseadas em tecnologia satelital (LEO ou MEO), considerando as características geográficas e limitações de infraestrutura da localidade.

2.1.2.5.2. Para esses casos, será adotado o LME Tipo 1, independentemente da comprovação de inviabilidade prevista no item 2.1.2.1, sendo considerada solução estrutural adequada à localidade;

2.1.2.5.3. O atendimento aos PCSs poderá ser realizado por uma das seguintes arquiteturas, a critério da CONTRATADA:

2.1.2.5.3.1. Atendimento direto ao PCS, por meio de terminal satelital(LEO ou MEO) instalado na própria localidade do ponto de acesso;

2.1.2.5.3.2. Atendimento por meio de concentrador ou ponto de presença local, no qual a CONTRATADA receba capacidade satelital (LEO ou MEO), realizando a distribuição aos PCSs por meio de infraestrutura terrestre, tais como fibra óptica, rádio ou tecnologia equivalente;

2.1.2.5.4. A CONTRATADA poderá propor outras tecnologias ou arquiteturas de atendimento, desde que apresente justificativa técnica fundamentada, a qual deverá ser previamente submetida à análise e aprovação da Agência Estadual de Tecnologia da Informação (ATI);

2.1.2.5.5. Caberá exclusivamente à CONTRATADA a responsabilidade por toda a infraestrutura necessária à prestação do serviço, incluindo, mas não se limitando a:

2.1.2.5.5.1. obtenção de licenças regulatórias e ambientais;

2.1.2.5.5.2. implantação de infraestrutura física e lógica;

2.1.2.5.5.3. contratação de terceiros ou parceiros;

2.1.2.5.5.4. custos de transporte, instalação, operação e manutenção.

2.1.2.5.6. A CONTRATANTE não será responsável por qualquer custo adicional além da contraprestação pelos serviços contratados.

**2.1.3. Link de Acesso Temporário (LAT)**

2.1.3.1. Serão usados nas conexões com os PCSs da Nova Rede Corporativa, de unidades administrativas que precisam ter acesso à internet durante eventos sazonais e/ou especiais, podendo ser providos a partir de tecnologias e recursos diversos da área de telecomunicações, as quais devem ser apropriadas para tais finalidades.

2.1.3.2. O serviço denominado de Link Acesso Temporário (LAT) terão períodos máximos de funcionamento e de comercialização de até 180 (cento e oitenta) dias a partir da data de instalação efetivamente atestada pelo Gestor do Órgão CONTRATANTE aderente. A Ordem de Serviço que autoriza a instalação dos LATs deve estabelecer o período exato de uso destes serviços temporários, ficando explicitamente autorizada a desativação automática após o período exato estabelecido na contratação.

2.1.3.3. As Ordens de Serviço serão formalizadas no mínimo com 15 (quinze) dias antes do início do período de utilização deste serviço.

2.1.3.4. O serviço Link de Acesso Temporário (LAT) poderá ser contratado em três categorias, conforme as especificações abaixo:

2.1.3.4.1. **LAT Tipo 1:** Velocidade inicial de **200 Mbps**, podendo ser fornecido por tecnologias satelitais (MEO ou LEO).

2.1.3.4.2. **LAT Tipo 2:** Velocidade inicial de **500 Mbps**, podendo ser provido por qualquer uma das tecnologias de acesso permitidas neste Adendo ou mediante aprovação técnica da ATI.

2.1.3.4.3. **LAT Tipo 3:** Velocidade inicial de **1 Gbps**, podendo ser provido por qualquer uma das tecnologias de acesso permitidas neste Adendo ou mediante aprovação técnica da ATI.

2.1.3.5. Na operacionalização dos LATs podem ser utilizadas tecnologias de acesso diversas (de acordo com a tecnologia disponível na localidade), tais como fibra ótica, 5G FWA, rádios e satélites.

2.1.3.5.1. A CONTRATADA deverá instalar preferencialmente as tecnologias de acesso de fibra óptica.

2.1.3.5.2. A ATI poderá solicitar esclarecimentos sobre o motivo do não atendimento pelas tecnologias de fibra óptica.

2.1.3.6. Condições Específicas para o Serviço de Link de Acesso Temporário (LAT)

2.1.3.6.1. Tendo em vista a natureza eventual e transitória do Serviço de Link de Acesso Temporário (LAT), o faturamento mínimo, para fins de cobrança, será sempre correspondente a 30 (trinta) dias corridos de serviço, ainda que o período efetivo de uso do link seja inferior a esse prazo — como nos casos de atendimento a eventos, ações emergenciais ou demandas temporárias de curta duração.

2.1.3.6.2. A cada ativação de serviço LAT, será obrigatória a implantação de Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 ou Tipo 2, conforme a capacidade da banda contratada. O faturamento da respectiva solução de segurança seguirá a mesma regra prevista no subitem anterior, com valor mínimo equivalente a 30 (trinta) dias corridos de uso, independentemente do tempo efetivo de operação do equipamento.

2.1.3.6.3. Em função da característica excepcional deste serviço, não se aplicará a regra geral de carência mínima de 6 (seis) meses estabelecida para os demais serviços previstos no Termo de Referência. Assim, o LAT e sua respectiva solução de segurança poderão ser contratados por períodos inferiores, respeitado o faturamento mínimo indicado nos subitens 2.1.3.6.1 e 2.1.3.6.2.

2.1.3.6.4. Para o atendimento da solução de segurança associada ao LAT, será permitida a utilização de equipamentos com uso prévio, desde que estejam em perfeito estado de funcionamento, livres de danos aparentes e atualizados com as versões mais recentes de firmware.

2.1.3.6.5. Os equipamentos utilizados deverão atender, integralmente, às exigências técnicas, funcionais e de segurança descritas no ADENDO III – SEGURANÇA DE REDE LOCAL.

2.1.3.6.6. As condições excepcionais dispostas neste subitem aplicam-se exclusivamente ao serviço de Link de Acesso Temporário (LAT) e à Solução Unificada de Segurança de Rede de Última Milha que o acompanha, não produzindo efeitos ou extensões para os demais serviços e soluções integrantes do escopo da Nova Rede Corporativa.

### 3. Disposições Gerais

3.1. Os Links de Acesso devem ser fornecidos a partir de tecnologias e recursos diversos da área de telecomunicações, apropriados para as finalidades contratadas, garantindo os níveis mínimos especificados neste Termo de Referência.

3.2. A CONTRATADA deverá prover, de forma total e exclusiva, toda a infraestrutura e os equipamentos necessários para o perfeito funcionamento dos serviços contratados, incluindo:

3.2.1. A infraestrutura física (cabos, conectores, entre outros) e elétrica será restrita aos serviços contratados e aos equipamentos da CONTRATADA que integram o Ponto Conectado Seguro (PCS), devendo atender integralmente às especificações e normas descritas no **ADENDO I - OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE**.

3.2.2. O fornecimento, instalação, manutenção e suporte de todos os equipamentos necessários para a prestação dos serviços, bem como da infraestrutura física e elétrica mencionada no subitem 3.2.1, incluindo sua configuração e gerenciamento, serão de total responsabilidade da CONTRATADA.

3.2.3. A garantia de que a infraestrutura interna e os equipamentos sejam disponibilizados exclusivamente para o atendimento das necessidades dos serviços contratados, respeitando as normas e especificações técnicas previstas no contrato e seus anexos.

3.2.4. O CONTRATANTE proverá apenas o espaço físico e a energia elétrica no PCS.

3.3. A solução de conectividade deverá ser flexível e escalável, permitindo ao CONTRATANTE a inclusão de novos sites em qualquer localidade do Estado de Pernambuco, em localidades até 30 km das suas fronteiras, quando necessário, e no Distrito de Fernando de Noronha.

3.4. É de responsabilidade da CONTRATADA instalar e manter, nas dependências do CONTRATANTE, todos os equipamentos e meios de transmissão necessários à prestação do serviço. Isso inclui o dimensionamento adequado de capacidade e desempenho para garantir o pleno funcionamento. A aquisição, configuração, manutenção e gerenciamento dos equipamentos são de total responsabilidade da CONTRATADA.

3.5. Os links de acesso à Internet deverão ser fornecidos em conformidade com as especificações estabelecidas neste Termo de Referência e, subsidiariamente, em atendimento às regulamentações vigentes da Agência Nacional de Telecomunicações (ANATEL), bem como às diretrizes estabelecidas por órgãos e normativas aplicáveis, tais como:

- Ministério das Comunicações (MCOM), para diretrizes estratégicas e normativas aplicáveis ao setor de telecomunicações;
- Comissão Nacional de Assuntos Espaciais (CONAE) e União Internacional de Telecomunicações (UIT), para regulamentação e padrões técnicos aplicáveis a serviços satelitais (MEO, LEO e GEO);
- 3rd Generation Partnership Project (3GPP), para normas internacionais relacionadas às redes 5G FWA;
- Internet Engineering Task Force (IETF) e Institute of Electrical and Electronics Engineers (IEEE), para protocolos e padrões de interconectividade, segurança e qualidade de serviço;
- Regulamentos do Comitê Gestor da Internet no Brasil (CGI.br), para diretrizes de governança e boas práticas na prestação de serviços de conectividade.

3.6. A validação e homologação do serviço, para fins de início de faturamento e término de contabilização de prazos/NMS para fins de glosa e multa, somente ocorrerá após a implementação da solução unificada de segurança deste serviço.

3.7. A CONTRATADA poderá subcontratar o fornecimento dos links de acesso descritos neste Adendo. Contudo, todas as interações e solicitações serão tratadas exclusivamente com a CONTRATADA, que será a única responsável pela prestação integral dos serviços descritos neste Termo de Referência.

3.7.1. Os links deverão ser fornecidos por prestadores devidamente autorizados pela ANATEL para exploração deste serviço. A CONTRATANTE poderá, a qualquer momento durante a vigência do contrato, solicitar a comprovação desta autorização.

#### 4. Fornecimento dos Serviços

4.1. A Nova Rede Corporativa de conectividade incluirá, preferencialmente, a prestação do Serviço de LAP para atendimento de aproximadamente 3.000 endereços/sites, conforme ordem de serviço emitida por CONTRATANTE Aderente no período de Assunção.

4.2. A CONTRATADA deve apresentar na Proposta de preços a descrição de como será a prestação dos serviços, incluindo uma descrição do Serviço de Links de Acesso (LAs) para Nova Rede Corporativa, atendendo aos princípios gerais e requisitos contidos neste Termo de Referência e respeitando as premissas obrigatórias abaixo elencadas, de responsabilidade da CONTRATADA:

4.2.1. Todos os equipamentos utilizados na implantação do serviço devem ser novos, sem uso anterior, garantindo a longevidade e a eficiência da infraestrutura.

4.3. A CONTRATADA deverá apresentar preços fixos unitários mensais para todos os serviços de Links de Acesso (LAs) nas suas respectivas velocidades e localidades previstas na abrangência da Nova Rede Corporativa.

4.4. O volume de dados, o tempo de utilização dos serviços e as informações trafegadas via rede, não deverão impactar na precificação dos Links de Acesso.

4.5. O Serviço deverá ser composto do link de comunicação que integre a localidade à Internet, com capacidade de expansão modular e flexível, garantindo ainda recursos de segurança adequados.

4.6. Ampliação de Capacidade dos Links de Acesso (LA)

4.6.1. A CONTRATADA deverá realizar um incremento de 100% da velocidade dos Links de Acesso (LA), tanto upload quanto download, de forma que o novo patamar de capacidade esteja plenamente implementado e em operação **até a data de início do terceiro ano contratual**, tomando como base a respectiva capacidade inicialmente definida neste Termo de Referência para cada item de serviço.

4.6.2. No início do terceiro ano contratual, todos os serviços de Links de Acesso já deverão estar implementados com a velocidade ampliada, conforme a Tabela 01.

Banda Contratada	Velocidade no Início do Contrato (Primeiro Ano)	Segundo Ano Contratual	Terceiro Ano Contratual	Quarto Ano Contratual
Links de 200 Mbps	200 Mbps	200 Mbps	400 Mbps	400 Mbps
Links de 300 Mbps	300 Mbps	300 Mbps	600 Mbps	600 Mbps
Links de 500 Mbps	500 Mbps	500 Mbps	1,00 Gbps	1,00 Gbps
Links de 1 Gbps	1,00 Gbps	1,00 Gbps	2,00 Gbps	2,00 Gbps

Tabela 01 - Incrementos de Velocidade dos Links de Acesso (LA)

4.6.3. Em caso de **renovação contratual**, deverão ser observadas as seguintes condições de ampliação:

4.6.3.1. No **início do sexto ano contratual (primeira renovação)**, todos os links contratados deverão sofrer incremento adicional de 50% sobre a capacidade originalmente definida neste Termo de Referência, tanto em upload quanto em download, devendo o novo patamar estar plenamente implementado e operacional até essa data.

4.6.3.2. No **início do nono ano contratual (segunda renovação)**, todos os links contratados deverão sofrer novo incremento adicional de 50% sobre a capacidade originalmente definida neste Termo de Referência, tanto em upload quanto em download, devendo o novo patamar estar plenamente implementado e operacional até essa data.

4.6.3. No início de cada etapa contratual prevista (terceiro, sexto e nono anos), todos os serviços de Links de Acesso deverão estar devidamente implementados com as velocidades ampliadas, conforme as tabela 02 de evolução de capacidade constantes deste Adendo.

Banda Contratada Inicial	Contrato 48 meses				1ª Renovação Contratual - 36 meses			2ª Renovação Contratual - 36 meses		
	Velocidade no Início do Contrato (Primeiro Ano)	Segundo Ano Contratual	Terceiro Ano Contratual	Quarto Ano Contratual	Quinto Ano Contratual	Sexto Ano Contratual	Sétimo Ano Contratual	Oitavo Ano Contratual	Novo Ano Contratual	Décimo Ano Contratual
Links de 200 Mbps	200 Mbps	200 Mbps	400 Mbps	400 Mbps	400 Mbps	500 Mbps	500 Mbps	500 Mbps	600 Mbps	600 Mbps
Links de 300 Mbps	300 Mbps	300 Mbps	600 Mbps	600 Mbps	600 Mbps	750 Mbps	750 Mbps	750 Mbps	900 Mbps	900 Mbps
Links de 500 Mbps	500 Mbps	500 Mbps	1,00 Gbps	1,00 Gbps	1,00 Gbps	1,25 Gbps	1,25 Gbps	1,25 Gbps	1,5 Gbps	1,5 Gbps
Links de 1 Gbps	1,00 Gbps	1,00 Gbps	2,00 Gbps	2,00 Gbps	2,00 Gbps	2,5 Gbps	2,5 Gbps	2,5 Gbps	3 Gbps	3 Gbps

Tabela 02 - Incrementos de Velocidade dos Links de Acesso (LA) em caso de renovação contratual

4.6.4. Caso a tecnologia utilizada não permita a implementação do incremento previsto, a CONTRATADA deverá apresentar, **de forma antecipada**, justificativas técnicas e propostas de solução alternativa que assegurem capacidade equivalente, a serem submetidas à análise e deliberação da ATI/SAD, **de modo a evitar o descumprimento dos prazos de ampliação contratual**, quando caracterizada inviabilidade técnica.

4.6.5. A efetivação da instalação dos Links de Acesso, bem como os incrementos de capacidade, deverão ser submetidos à validação formal do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), mediante testes e relatórios técnicos fornecidos pela CONTRATADA. O aceite pelo CIISC constituirá a homologação oficial do atendimento às exigências deste ADENDO.

4.6.6. A CONTRATADA deverá garantir as ampliações de capacidade sem qualquer custo adicional para a CONTRATANTE, seja por meio do aumento da capacidade do link originalmente contratado ou pela agregação, no CPE, de múltiplos links.

4.6.7. Durante toda a vigência contratual e suas eventuais renovações, todos os novos links implantados deverão ser entregues já em conformidade com as velocidades correspondentes ao período vigente, observando-se os prazos e percentuais de ampliação definidos neste Termo de Referência.

4.7. A CONTRATADA deverá prover as conexões do serviço através de fibra óptica, prioritariamente, ou outros meios previstos no Termo de Referência ou autorizado pela Agência Estadual de Tecnologia da Informação - ATI, fornecendo todos os equipamentos materiais e infraestrutura necessária ao perfeito funcionamento;

4.8. O serviço contratado não deverá conter limites, franquias de uso ou consumo, nem qualquer política de restrição baseada em volume de dados trafegados, independentemente da tecnologia de acesso empregada, incluindo, mas não se limitando a, acessos baseados em tecnologias satelitais, rádio ou 5G FWA.

4.8.1. Considera-se vedada a adoção de franquias de dados, políticas de uso justo (Fair Use Policy – FUP), redução automática de velocidade, priorização negativa de tráfego, bloqueio de aplicações ou cobrança adicional em função do volume de dados consumido.

4.8.2. As exigências deste item não se confundem com limitações técnicas inerentes às características físicas ou operacionais da tecnologia de acesso utilizada (tais como enlaces satelitais, rádio ou 5G FWA), desde que tais limitações não resultem em restrições comerciais de consumo, não impliquem corte, degradação automática ou tarifação adicional, e não impeçam o cumprimento integral dos Níveis Mínimos de Serviço (NMS) e SLAs contratuais estabelecidos neste Termo de Referência

4.8.3. Em quaisquer hipóteses, a CONTRATADA deverá garantir a entrega contínua do serviço, observando os parâmetros de desempenho, disponibilidade, latência, jitter, perda de pacotes e garantia de banda definidos neste Termo de Referência e seus Adendos, sendo vedada a utilização de mecanismos que condicionem a qualidade ou a continuidade do serviço ao volume de tráfego consumido.

4.8.4. A eventual utilização de mecanismos de gestão de tráfego deverá restringir-se exclusivamente a fins técnicos de estabilidade, segurança e integridade da rede, não podendo, em nenhuma hipótese, caracterizar limitação de consumo, franquia de dados ou política comercial restritiva ao CONTRATANTE.

4.9. Não deverá existir nenhum bloqueio de portas e/ou serviços, visando permitir livre comunicação entre sistemas utilizados CONTRATANTE.

4.10. A CONTRATADA deverá implementar e garantir o acesso de consulta via SNMP (versões 2 e 3 ou superior, caso disponível) aos equipamentos que forem fornecidos para prestação do serviço para permitir o monitoramento de desempenho e o gerenciamento dos serviços;

4.11. A CONTRATADA deverá garantir o acesso remoto à ATI-PE, e a quem ela determinar/ liberar, de consulta via SNMP (versões 2 e 3 ou superior, caso disponível) aos equipamentos que forem fornecidos para prestação do serviço;

4.12. A CONTRATADA deverá disponibilizar para ATI-PE credenciais de acesso de leitura a todas as soluções, e a todos os seus recursos, que compõem este serviço e a quem a ATI-PE autorizar;

4.13. O Serviço de Internet deverá ser prestado em consonância com os serviços especificados em todos os ADENDOS deste Termo.

#### **4.14. Instalar, operacionalizar e manter os serviços de Links de Acesso (LAs) nos PCs.**

4.14.1. Garantir nos PCs o funcionamento dos serviços de dados instalados.

4.14.2. Quando for adotada uma solução técnica por radiofrequência, para prover os serviços de Links de Acesso (LAs), não poderá ser utilizado Radiofrequência por Espalhamento Espectral, tecnologia esta não permitida na nova Rede corporativa;

4.14.3. Cada LAP, LME e LAT, deve ser disponibilizado de forma integrada e gerenciável pela equipe de operação/gerenciamento da Nova Rede Corporativa, aos serviços de dados, suportados pelo protocolo TCP/IPV6. Este serviço inclui todos os recursos de conectividade da Nova Rede Corporativa;

4.14.4. Garantir o sigilo e a integridade dos dados transmitidos através dos LAPs, LMEs e LATs nos padrões exigidos na Nova Rede Corporativa;

4.14.5. Garantir na solução adotada que todos os LAs sejam gerenciados tecnicamente pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, através do protocolo SNMP (versões 2 e 3 ou superior, caso disponível). O sistema de gerência técnica deve ser integrado, para o controle e monitoramento dos recursos e serviços providos via a Nova Rede Corporativa;

4.14.6. Priorizar todo o tráfego de voz, quando aplicável, nos túneis configurados nos equipamentos SD-WAN nas dependências da CONTRATANTE, em toda a solução fornecida, garantindo os requisitos e Níveis Mínimos de Serviço descritos nos adendos deste Termo de Referência.

4.14.7. Garantir a implantação do aumento de velocidade como previsto neste Termo de Referência. A implantação será de forma transparente, isto é, sem gerar impacto, interrupções e custos adicionais de reinstalações. O serviço apenas será considerado concluído quando for formalmente validado pelo Centro Integrado de Inteligência e Segurança Cibernética e pela Gestão Técnica da Nova Rede Corporativa - ATI. Os recursos e equipamentos envolvidos nestes aumentos de velocidade deverão suportar as atualizações tecnológicas previstas nesta facilidade;

4.14.8. A CONTRATADA deverá fornecer todos os recursos, instalar, configurar e operacionalizar todos os equipamentos da solução (Firewalls, switches, modems, ONUs, roteadores, conversores de interface, cabos dentre outros), onde todos devem estar devidamente homologados pela ANATEL, e demais acessórios necessários à operação do serviço, bem como a manutenção e atualização do sistema operacional dos equipamentos, sem ônus adicionais para a CONTRATANTE, inclusive ponto(s) elétrico(s) estabilizado(s), e toda a infraestrutura de rede (cabeamento, calhas, racks, etc.) imprescindível para seu pleno funcionamento dentro da velocidade requerida, garantindo e obedecendo todos os requisitos de segurança estabelecidos nos adendos deste Termo de Referência;

4.14.9. A CONTRATADA será responsável pelo desempenho dos equipamentos fornecidos, cabendo a substituição ou correção, em caso de perda de desempenho ou ameaça à segurança da CONTRATANTE;

4.15. A solução instalada deverá ser compatível com a velocidade CONTRATADA (largura de banda) dos Links de Acesso (LAs), possuir todos os recursos (memória, processamento, I/O e portas de comunicação) necessários ao pleno funcionamento com todas as funcionalidades exigidas pela CONTRATANTE, com o desempenho (performance) satisfatório para atendimento de todo o tráfego gerado no PCS onde o LA esteja instalado.

4.16. Todas as especificações para solução de segurança dos Links de Acesso estão descritas nos ADENDOS de Segurança deste Termo de Referência.

## 5. Especificações Técnicas

### 5.1. Do Endereçamento IPv4 e IPv6

5.1.1. A CONTRATADA deverá, preferencialmente, utilizar os blocos de endereçamento IPv4 e IPv6 fornecidos pela CONTRATANTE, provenientes do ASN 10938 da ATI-PE. Alternativamente, poderá prover endereçamento IPv4 e IPv6 fixo, válido e público para todos os Links de Acesso contratados previstos neste Adendo, devendo, em qualquer hipótese, assegurar conformidade com as boas práticas de conectividade IP reconhecidas nacional e internacionalmente. Não será permitido o uso de endereçamentos privados (RFC 1918) para comunicação com redes externas.

5.1.2. A CONTRATADA, na hipótese de optar pela utilização dos blocos IPv4 e IPv6 fornecidos pela CONTRATANTE, provenientes do ASN 10938 da ATI-PE, deverá realizar todas as configurações técnicas necessárias, assegurando que o serviço seja prestado em conformidade com as melhores práticas de conectividade, roteamento e operação de redes IP.

5.1.3. Caso a CONTRATADA faça uso do plano de endereçamento fornecido pela ATI-PE, deverá respeitar integralmente a distribuição de endereços definida para cada localidade e garantir que os links de acesso à Internet estejam configurados conforme o plano aprovado pela CONTRATANTE.

5.1.4. A CONTRATADA será responsável por todas as configurações de endereçamento e roteamento necessárias para o funcionamento pleno do serviço contratado, incluindo, mas não se limitando, à configuração de VPNs e redes locais que atendam às necessidades da CONTRATANTE.

5.1.5. Configurações específicas para publicação de serviços, redes locais ou integração com sites externos que exijam segurança adicional deverão ser realizadas exclusivamente por meio do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), respeitando os procedimentos e normas estabelecidos pela CONTRATANTE.

### 5.2. DO GERENCIAMENTO E DOCUMENTAÇÃO

5.2.1. Manter documentação técnica atualizada de todo o plano de endereçamento implementado, incluindo topologia lógica da rede, configurações aplicadas e mudanças realizadas;

5.2.2. Registrar em sistema próprio todas as alterações realizadas no esquema de endereçamento, mantendo histórico das modificações;

5.2.3. Documentar todas as configurações de roteamento implementadas, incluindo políticas de BGP e regras de firewall aplicadas.

### 5.3. DA SEGURANÇA E PROTEÇÃO

5.3.1. Implementar e manter atualizados filtros de bogons para bloquear endereços IP inválidos;

5.3.2. Configurar e gerenciar *Access Control Lists* (ACLs) apropriadas para proteção da infraestrutura;

5.3.3. Implementar mecanismos de proteção contra *spoofing* de endereços IP;

5.3.4. Configurar o protocolo BGP seguindo as melhores práticas de segurança, incluindo filtros de prefixos adequados.

## 5.4. Especificações Técnicas e Parâmetros de Qualidade

### 5.4.1.1. Definições dos Parâmetros Técnicos

#### 5.4.1.1.1. Latência Máxima:

5.4.1.1.1.1. Tempo máximo que um pacote de dados leva para ir de um ponto da rede a outro, medido em milissegundos (ms). A medição deve ser realizada em intervalos periódicos, conforme metodologia definida no **ADENDO II - Níveis Mínimos de Serviço**.

Fonte: ITU-T G.114 – "One-way Transmission Time" (Tempo de Transmissão Unidirecional).

#### 5.4.1.1.2. Jitter Máximo:

5.4.1.1.2.1. Variação no tempo de chegada dos pacotes na rede, medido em milissegundos (ms). Impacta diretamente a qualidade de serviços em tempo real, como streaming e chamadas de voz.

Fonte: ITU-T G.1050 – "Network Jitter Models for Simulation" (Modelos de Rede para Simulação de Jitter).

#### 5.4.1.1.3. Perda de Pacotes:

5.4.1.1.3.1. Porcentagem máxima de pacotes de dados que podem ser perdidos durante a transmissão. Afeta a integridade dos dados e a experiência do usuário.

Fonte: ITU-T Y.1541 – "Network Performance Objectives for IP-based Services" (Objetivos de Desempenho de Rede para Serviços baseados em IP).

#### 5.4.1.1.4. Disponibilidade:

5.4.1.1.4.1. Porcentagem mínima do tempo em que o serviço deve estar disponível para uso dentro de um período mensal. Um valor maior reflete maior confiabilidade do serviço.

Fonte: ITU-T E.800 – "Definitions of Terms Related to Quality of Service" (Definições de Termos Relacionados à Qualidade de Serviço).

#### 5.4.1.1.5. Garantia de Banda (Download e Upload):

5.4.1.1.5.1. A CONTRATADA deverá garantir, tanto para download quanto para upload, os seguintes parâmetros de desempenho para cada link contratado:

##### 5.4.1.1.5.1.1. Garantia de Velocidade Instantânea Contratada:

5.4.1.1.5.1.1.1. **Banda Larga (LBL e LAT/LME Banda Larga):** Mínimo de 40% para download e upload da velocidade contratada em 95% das medições realizadas no período do respectivo regime de manutenção.

5.4.1.1.5.1.1.2. **Links Dedicados (LD e LAT/LME Dedicado):** 100% da velocidade contratada.

5.4.1.1.5.1.1.3. **LAT/LME 5G FWA:** 80% da velocidade contratada.

5.4.1.1.5.1.1.4. **Links Satelitais (LAT/LME LEO e MEO):** Mínimo de 80% para download e 10% para upload da velocidade contratada.

##### 5.4.1.1.5.1.2. Garantia de Velocidade Média Contratada:

5.4.1.1.5.1.2.1. **Banda Larga (LBL e LAT/LME Banda Larga):** Mínimo de 80% para download e upload da velocidade contratada, como média de todas as medições realizadas no período entre 7h e 19h.

5.4.1.1.5.1.2.2. **Links Dedicados (LD e LAT/LME Dedicado):** 100% da velocidade contratada.

5.4.1.1.5.1.2.3. **LAT/LME 5G FWA:** 80% da velocidade contratada.

5.4.1.1.5.1.2.4. Links Satelitais (LAT/LME LEO e MEO): Mínimo de 80% para download e 10% para upload da velocidade contratada.

5.4.1.1.5.1.3. Os parâmetros acima estão alinhados às diretrizes da Anatel para o Serviço de Comunicação Multimídia (SCM), conforme descrito na Resolução nº 717/2019 e nas orientações disponíveis no portal da agência (gov.br).

#### 5.4.1.2. Tabela Consolidada de Parâmetros Técnicos

5.4.1.2.1. A CONTRATADA deverá garantir os seguintes parâmetros técnicos para cada tipo de link contratado, de acordo com o acesso utilizado e a velocidade contratada, conforme especificado na tabela abaixo:

Parâmetro Técnico	LA						
	LAP		LAT/ LME				
	Banda Larga (LBL)	Dedicado (LD)	Banda Larga	Dedicado	5G FWA	LEO (Satélite)	MEO (Satélite)
Latência Máxima	80 ms	50 ms	80 ms	50 ms	30 ms	100 ms	270 ms
Jitter Máximo	40 ms	5 ms	40 ms	5 ms	5 ms	20 ms	30 ms
Perda de Pacotes	≤ 2%	≤ 0,5%	≤ 2%	≤ 0,5%	≤ 0,5%	≤ 1%	≤ 1,5%
Disponibilidade	≥ 98%	≥ 99,5%	≥ 98%	≥ 99,5%	≥ 98,5%	≥ 98,5%	≥ 98,5%
Cumprimento de Prazo	Tabela Limites de Tempos para Correções de Falhas						
Garantia de Banda (Download)	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	80% da contratada	80% da contratada	80% da contratada
Garantia de Banda (Upload)	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	Média ≥ 80% / Inst. ≥ 40%	100% da contratada	80% da contratada	10% da contratada	10% da contratada

Tabela 03 - Parâmetros Técnicos

#### 5.4.1.2.2. Legenda para Parâmetros Técnicos:

5.4.1.2.2.1. **Média ≥ 80%:** Refere-se à Garantia de Velocidade Média Contratada, que é o percentual médio da velocidade contratada que deve ser entregue durante o período de medição, com um valor mínimo de 80% da velocidade contratada, conforme estabelecido pela Anatel.

5.4.1.2.2.2. **Inst. ≥ 40%:** Refere-se à Garantia de Velocidade Instantânea Contratada, que é o percentual mínimo da velocidade contratada que deve ser entregue em medições instantâneas realizadas, com um valor mínimo de 40%, conforme estabelecido pela Anatel.

#### 5.4.2. Garantia de Serviço

5.4.2.1. A CONTRATADA deverá garantir a qualidade e o desempenho dos serviços conforme os Níveis Mínimos de Serviço (NMS) estabelecidos no **ADENDO II – Níveis Mínimos de Serviço**, incluindo tempos máximos de resposta e resolução de falhas.

#### 5.4.3. Suporte Técnico

5.4.3.1. A CONTRATADA deverá oferecer suporte padrão de 12x5 (12 horas por dia, 5 dias por semana) para todas as localidades atendidas.

5.4.3.2. Opcionalmente, a CONTRATANTE poderá contratar regimes adicionais de manutenção, como 24x7 (24 horas por dia, 7 dias por semana) ou 12x7 (12 horas por dia, 7 dias por semana), conforme descrito no ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO.

#### 5.4.4. Gerenciamento, Monitoramento e Emissão de Relatórios

5.4.4.1. A CONTRATADA deverá fornecer relatórios mensais consolidados, contendo informações detalhadas sobre a qualidade dos serviços contratados, incluindo:

5.4.4.1.1. Disponibilidade dos links;

5.4.4.1.2. Tempos de resposta e resolução de incidentes;

5.4.4.1.3. Perdas de pacotes, latência e jitter;

5.4.4.1.4. Desempenho em relação aos parâmetros técnicos estabelecidos;

5.4.4.1.5. Eventos de degradação de serviço e indisponibilidades registradas;

5.4.4.1.6. Conformidade com os SLAs estipulados no contrato.

5.4.4.2. Os relatórios deverão ser emitidos de forma automatizada e auditável, permitindo exportação em formatos padronizados (CSV, JSON, XML) para integração com os sistemas da CONTRATANTE. Os relatórios serão utilizados como base para avaliação da conformidade da CONTRATADA com os parâmetros técnicos e de desempenho estabelecidos neste Termo de Referência.

5.4.4.3. O Centro Integrado de Inteligência e Segurança Cibernética (CIISC) será responsável pelo gerenciamento e monitoramento centralizado da infraestrutura de conectividade da Nova Rede Corporativa, incluindo:

5.4.4.3.1. Supervisão e controle contínuo da operação dos links de acesso (LAP, LAT/LME);

5.4.4.3.2. Monitoramento proativo da performance e integridade dos links;

5.4.4.3.3. Correlação de incidentes e falhas na conectividade, com detecção de anomalias;

5.4.4.3.4. Auditoria dos relatórios apresentados pela CONTRATADA e validação dos SLAs;

5.4.4.3.5. Execução de diagnósticos técnicos e suporte avançado para resolução de problemas;

5.4.4.3.6. Coordenação da resposta a incidentes de rede e segurança, conforme os protocolos estabelecidos;

5.4.4.3.7. Gerenciamento e comando do consórcio da CONTRATADA, garantindo a aderência dos serviços ao contrato.

#### 5.4.5. Referências Normativas

5.4.5.1. Os padrões de qualidade devem seguir o estabelecido na Resolução nº 717/2019 da Anatel, além de boas práticas internacionais aplicáveis ao tipo de tecnologia utilizada, como:

- ITU-T E.800-E809: Modelos de medição de qualidade de serviços de telecomunicação;
- ITU-T G.1050: Modelos de simulação de rede para jitter e latência;
- ETSI TR 103 273: Indicadores de qualidade para serviços multimídia;
- ITU-T G.114: Diretrizes de latência para serviços de voz e dados;
- ETSI TS 102 519: Critérios de avaliação para perda de pacotes;
- 3GPP Release 15 e posteriores: Padrões para redes 5G.

#### 5.5. Tecnologias de Atendimento

5.5.1. A implantação dos serviços de Links de Acesso (LAs) para a Nova Rede Corporativa deverá utilizar tecnologias modernas e de alta eficiência, capazes de garantir alta capacidade de transmissão, confiabilidade operacional e conformidade com padrões internacionais de qualidade e desempenho.

5.5.2. As tecnologias de atendimento descritas a seguir são permitidas neste Termo de Referência e deverão ser implementadas de acordo com suas respectivas características técnicas e normas que as regem. A adoção dessas tecnologias visa assegurar que os serviços contratados atendam aos critérios de desempenho, segurança, escalabilidade e eficiência necessários para atender às demandas da CONTRATANTE.

5.5.3. A CONTRATADA poderá sugerir e utilizar novas ou outras tecnologias, desde que:

5.5.3.1. Garantam os parâmetros técnicos exigidos neste Termo de Referência.

5.5.3.2. Apresentem documentação técnica detalhada da solução proposta.

5.5.3.3. Sejam aprovadas formalmente pela ATI, após análise técnica da viabilidade e impacto na rede.

5.5.4. A CONTRATADA será responsável pela implementação, manutenção e suporte contínuo das tecnologias utilizadas. Abaixo seguem as tecnologias permitidas, suas respectivas características e os padrões técnicos que devem ser seguidos:

### 5.5.5. Tecnologias de Fibra Óptica

5.5.5.1. **FTTH (Fiber to the Home):** Modelo de provimento de última milha através do uso de fibra óptica até o local de instalação do PCS, proporcionando alta capacidade de transmissão de dados, baixa latência e alta confiabilidade. Adequada para conexões de 500 Mbps a 20Gbps.

**Normas/Padrões:** ITU-T G.984.x (GPON), ITU-T G.987.x (XG-PON), ITU-T G.9807.x (XGS-PON).

5.5.5.1.1. **GPON (Gigabit Passive Optical Network):** Rede óptica passiva que permite compartilhar a mesma fibra óptica entre múltiplos usuários, reduzindo custos de infraestrutura enquanto fornece alta velocidade. Adequada para conexões de até 2,5Gbps.

**Normas/Padrões:** ITU-T G.984.x.

5.5.5.1.2. **XG-PON (10 Gigabit Passive Optical Network):** Evolução do GPON, oferecendo maior capacidade de transmissão, chegando até 10Gbps.

**Normas/Padrões:** ITU-T G.987.x.

5.5.5.1.3. **XGS-PON (10 Gigabit Simetric Passive Optical Network):** Tecnologia avançada de rede óptica passiva que suporta até 10Gbps.

**Normas/Padrões:** ITU-T G.9807.x.

5.5.5.2. **DWDM (Dense Wavelength Division Multiplexing):** Tecnologia que aumenta a capacidade da fibra óptica existente, suportando múltiplos canais de 500 Mbps a 20Gbps simultaneamente.

**Normas/Padrões:** ITU-T G.694.1, ITU-T G.872, G.709 (interfaces); G.692 (Interfaces multichannel); G.798 (transporte ótico).

5.5.5.3. **Metro Ethernet:** Tecnologia que utiliza a infraestrutura Ethernet para fornecer conexões de alta velocidade em áreas metropolitanas, adequada para conexões de 300Mbps a 20Gbps.

**Normas/Padrões:** IEEE 802.3, IEEE 802.1Q.

5.5.5.4. **DOCSIS 3.1 (Data Over Cable Service Interface Specification):** Padrão de transmissão de dados via cabos coaxiais, utilizado principalmente em áreas urbanas, oferecendo alta velocidade de transmissão com baixa latência, adequada para conexões de até 10Gbps.

**Normas/Padrões:** ANSI/SCTE 201 2017.

### 5.5.6. Tecnologias Sem Fio e Rádio Digital

**5.5.6.1. Rádio Digital de Alta Capacidade (PtP – Ponto a Ponto):** Tecnologia de conexão sem fio dedicada para locais sem infraestrutura de fibra, garantindo conectividade de baixa latência.

**Normas/Padrões:** ITU-R F.1497, ITU-R F.1702, ETSI EN 302 217.

**5.5.6.2. 5G FWA (Fixed Wireless Access):** Utilização da tecnologia 5G para fornecer conexões de alta velocidade em locais fixos, oferecendo velocidades de até 1Gbps. Aplicável principalmente em LAT/LME, como alternativa a soluções cabeadas.

**Normas/Padrões:** 3GPP Release 15 e posteriores.

**5.5.6.2.1. A CONTRATADA** deverá fornecer o modem 5G FWA ou equipamento equivalente, configurado para permitir a conexão direta via interface LAN com dispositivos como firewalls, roteadores ou outros equipamentos de rede previstos no projeto.

**5.5.6.2.2. O equipamento** fornecido deverá atender aos seguintes requisitos técnicos mínimos:

- Velocidade nominal de até 1Gbps, com garantia mínima de 80% da banda contratada para download e upload.
- Permitir a configuração de IPv4 e IPv6 de forma simultânea (dual stack).
- Operar nas bandas 5G autorizadas pela ANATEL, garantindo compatibilidade com a infraestrutura nacional.
- Latência máxima inferior a 30ms.
- Pelo menos 1 porta LAN gigabit para conexão com dispositivos locais.
- Fallback automático para 4G LTE em caso de indisponibilidade do sinal 5G.
- Permitir a gestão remota centralizada pelo Centro Integrado de Inteligência e Segurança Cibernética (CIISC), assegurando monitoramento e configuração contínuos conforme os requisitos do projeto.

**5.5.6.3. SD-WAN (Software-Defined Wide Area Network):** Tecnologia que otimiza a rede WAN, utilizando múltiplas conexões de internet para melhorar o desempenho e a segurança.

**Normas/Padrões:** MEF 70 (SD-WAN Service Attributes and Service Framework).

## 5.5.7. Atendimento por Satélite:

A fim de garantir a máxima cobertura e disponibilidade dos serviços de banda larga, a CONTRATADA poderá utilizar tecnologias de satélite. Estas tecnologias incluem satélites de baixa órbita (LEO) e órbita média (MEO). Cada uma dessas tecnologias possui características específicas que devem ser levadas em consideração para garantir a qualidade e a eficiência do serviço. Todos os equipamentos e infraestrutura necessários para o serviço satelital serão fornecidos e mantidos integralmente pela CONTRATADA, devendo estar homologados pela Anatel.

### 5.5.7.1. Tipos de Satélites e Especificações Técnicas

#### 5.5.7.1.1. Satélites de Baixa Órbita (LEO)

- **Características:** Satélites em órbitas de aproximadamente 500 a 2.000 km de altitude.
- **Velocidades Médias Atingidas:** Até 250 Mbps *download* por link.
- **Normas/Padrões:** ITU-R S.1001, ETSI EN 302 340.
- **Parâmetros Técnicos e Indicadores de Qualidade:**

- **Latência** Máxima:  $\leq 100\text{ms}$

o Referência: ITU-T G.114, ETSI TR 102 374-1.

- **Jitter** Máximo:  $\leq 20\text{ ms}$

o Referência: ITU-T G.1050, ETSI GS QKD 011.

- **Perda de Pacotes:**  $\leq 1\%$ .

o Referência: ITU-T Y.1541, ETSI TS 102 519.

- **Disponibilidade do Serviço:**  $\geq 98,5\%$  ao mês.

o Referência: ITU-T E.800-E809, ETSI TR 103 273.

#### 5.5.7.1.2. Satélites de Órbita Média (MEO)

- **Características:** Satélites em órbitas de aproximadamente 8.000 a 20.000 km de altitude.
- **Velocidades Médias Atingidas:** Até 500 Mbps *download* por link.
- **Normas/Padrões:** ITU-R S.1001, ETSI EN 302 340.
- **Parâmetros Técnicos e Indicadores de Qualidade:**

- **Latência Máxima:**  $\leq 270\text{ms}$ .

o Referência: ITU-T G.114, ETSI TR 102 374-1.

- **Jitter Máximo:**  $\leq 30\text{ms}$ .

o Referência: ITU-T G.1050, ETSI GS QKD 011.

- **Perda de Pacotes:**  $\leq 1,5\%$ .

o Referência: ITU-T Y.1541, ETSI TS 102 519.

- **Disponibilidade do Serviço:**  $\geq 98,5\%$  ao mês.

o Referência: ITU-T E.800, ETSI TR 103 273.

#### 5.5.7.2. Particularidades e Normas/Regras

- **Antenas e Equipamentos de Solo:** Todos os equipamentos de solo, incluindo antenas, modems e amplificadores, devem ser compatíveis com a tecnologia do satélite escolhido e devem ser fornecidos, instalados e mantidos pela CONTRATADA. As antenas devem seguir as normas ETSI EN 301 459 e ETSI EN 301 427.
- **Aprovação/Homologação pela ANATEL:** Todos os equipamentos utilizados devem ter aprovação/homologação pela ANATEL.
- **Interferência e Proteção de Sinal:** Deve ser garantida a proteção contra interferências, conforme ITU-R S.1432 e ETSI EN 302 340.
- **Manutenção e Suporte:** A CONTRATADA deve garantir manutenção e suporte técnico, com tempos máximos de resposta e resolução de incidentes claramente definidos no SLA.
- **Segurança:** Implementação de medidas de segurança para proteger a integridade e a confidencialidade dos dados transmitidos via satélite, conforme ISO/IEC 27001.
- **Flexibilidade de Contratação:** Será permitido a flexibilidade para alternar entre diferentes tipos de satélites conforme necessário para atender às condições específicas de cada localidade.
- **Medição e Relatórios:** Relatórios periódicos sobre a qualidade do serviço, incluindo latência, jitter, perda de pacotes e disponibilidade, devem ser fornecidos à CONTRATANTE para monitoramento e avaliação contínua, conforme especificações no **ADENDO II de Nível Mínimo de Serviço**.

- **Atualizações Tecnológicas:** A CONTRATADA deve estar preparada para incorporar atualizações tecnológicas à medida que novas tecnologias de satélite se tornem disponíveis, garantindo a melhoria contínua do serviço.

## 5.6. Infraestrutura Resiliente e Redundante no PCS

5.6.1. A CONTRATADA deverá implementar infraestrutura resiliente e redundante no âmbito do Ponto Conectado Seguro (PCS), quando solicitada pela CONTRATANTE, com o objetivo de garantir a continuidade dos serviços de conectividade, observando, obrigatoriamente, as regras de redundância, topologia, segregação e roteamento definidas neste Adendo.

5.6.2. A fim de garantir a continuidade dos serviços e minimizar o tempo de indisponibilidade, as soluções de redundância deverão assegurar a continuidade automática dos serviços em caso de falha de qualquer dos Links de Acesso, respeitando os Níveis Mínimos de Serviço (NMS) estabelecidos no ADENDO II, independentemente da tecnologia de acesso empregada. A seguir, são detalhadas as especificações e responsabilidades da CONTRATADA para assegurar a resiliência da infraestrutura:

### 5.6.2.1. Redundância e Topologia dos Links de Acesso nos PCSs

5.6.2.1.1. Qualquer modalidade de Link de Acesso (LAP, LME ou LAT) poderá ser contratada com redundância, mediante solicitação expressa do CONTRATANTE ou por necessidade técnica devidamente caracterizada e validada pela ATI.

5.6.2.1.2. Os Links de Acesso instalados em um PCS poderão ser contratados em qualquer combinação entre as modalidades previstas neste Adendo, incluindo, mas não se limitando a: LAP com LAP, LAP com LME, LAP com LAT ou outras combinações tecnicamente viáveis.

5.6.2.1.3. Sempre que houver dois ou mais Links de Acesso instalados em um mesmo Ponto Conectado Seguro (PCS), estes deverão operar obrigatoriamente em regime de redundância, salvo por expressa determinação do CONTRATANTE ADERENTE, previamente validada pela ATI, garantindo a continuidade automática do serviço em caso de falha de qualquer dos acessos.

5.6.2.1.4. Quando configurados em redundância, os links deverão ser implantados com:

5.6.2.1.4.1. meios de acesso distintos, admitindo-se, por exemplo, a utilização de duas fibras ópticas distintas ou dois enlaces de rádio distintos; a utilização de tecnologias satelitais ou 5G como enlaces redundantes dependerá de autorização expressa da ATI;

5.6.2.1.4.2. quando utilizadas múltiplas conexões por fibra óptica, estas deverão ser completamente independentes, incluindo rotas físicas separadas e sem compartilhamento de dutos ou caminhos de infraestrutura;

5.6.2.1.4.3. rotas físicas independentes;

5.6.2.1.4.4. infraestrutura de última milha segregada;

5.6.2.1.4.5. inexistência de compartilhamento de elementos críticos de acesso.

5.6.2.1.5. A CONTRATADA deverá implementar mecanismos de roteamento automático e eficiente entre os links instalados no PCS, assegurando:

5.6.2.1.5.1. failover transparente;

5.6.2.1.5.2. priorização adequada do tráfego;

5.6.2.1.5.3. continuidade dos serviços;

5.6.2.1.5.4. atendimento aos níveis mínimos de serviço estabelecidos neste Termo de Referência.

5.6.2.1.6. A solução de roteamento e redundância adotada deverá observar as melhores práticas de engenharia de redes e estará sujeita à validação técnica da ATI, independentemente da tecnologia empregada.

5.6.2.1.7. A instalação de mais de dois Links de Acesso em um mesmo PCS poderá ser autorizada, de forma excepcional, quando caracterizada necessidade de interesse público ou necessidade técnica/operacional específica, hipótese em que a CONTRATADA deverá:

5.6.2.1.7.1. apresentar viabilidade técnica para atendimento com mais de dois links de acesso no PCS, indicando alternativas técnicas distintas das já implantadas;

5.6.2.1.7.2. em caso de inviabilidade técnica e econômica, apresentar justificativa técnica fundamentada;

5.6.2.1.7.3. submeter, em qualquer dos casos, a proposta à aprovação formal da ATI;

5.6.2.1.7.4. formalizar situação na Ordem de Serviço específica da contratação.

5.6.2.1.8. A CONTRATADA deverá registrar e informar à CONTRATANTE ADERENTE e à ATI os PCSs que não possuam entradas ou tubulações redundantes;

5.6.2.1.9. Os links deverão ser fornecidos, preferencialmente, por operadoras distintas, não configurando exigência mandatória, desde que a CONTRATADA entregue solução que assegure a total segregação física da rede de acesso (incluindo última milha, meios e rotas de chegada ao PCS) e a segregação lógica dos acessos, sem compartilhamento de elementos críticos da infraestrutura de acesso.

5.6.2.1.9.1. A CONTRATADA deverá, sempre que solicitada pela CONTRATANTE ou pela ATI, apresentar topologia técnica, diagramas de atendimento ou informações detalhadas da solução implantada, de forma a demonstrar o atendimento aos requisitos de segregação e redundância previstos neste Adendo.

5.6.2.1.9.2. Normas/Padrões aplicáveis: NBR 14565 (Cabeamento de telecomunicações para edifícios comerciais) e ITU-T G.652 (Características de uma fibra óptica monomodo).

5.6.2.1.10. Considera-se que a infraestrutura de backbone das operadoras de telecomunicações, por sua própria natureza técnica, é composta por múltiplos caminhos, mecanismos de roteamento e engenharia de tráfego, não sendo exigida, para fins deste Termo de Referência, a disponibilização de backbone dedicado, exclusivo ou com rotas físicas totalmente segregadas para o presente contrato.

5.6.2.1.10.1. A CONTRATADA deverá assegurar que eventuais falhas internas de sua infraestrutura de backbone não comprometam o atendimento aos Níveis Mínimos de Serviço (NMS) estabelecidos neste Termo de Referência, permanecendo integralmente responsável pela continuidade, desempenho e disponibilidade dos serviços contratados.

#### 5.6.2.2. Monitoramento e Gerenciamento Proativo

5.6.2.2.1. A CONTRATADA deverá implementar sistemas de monitoramento contínuo para detectar falhas e anomalias em tempo real. Esses sistemas devem ser capazes de iniciar processos de *failover* automaticamente, garantindo a rápida recuperação dos serviços.

5.6.2.2.2. Normas/Padrões aplicáveis: ISO/IEC 27002 (Práticas de Segurança da Informação).

#### 5.6.2.3. Equipamentos Redundantes

5.6.2.3.1. Todos os equipamentos envolvidos em soluções redundantes deverão possuir unidades redundantes, suportando configurações em modo ativo-passivo ou ativo-ativo, bem como SD-WAN, e, se solicitado, a configuração de Alta Disponibilidade (HA). A CONTRATADA será responsável por todos os insumos necessários para essa configuração (cabos, módulos SFP, fontes de alimentação redundantes, etc.).

5.6.2.3.2. Normas/Padrões aplicáveis: IEC 62351 (Normas de segurança para redes de comunicação), IEEE 802.1Q (VLAN) e RFC 4193 (Endereçamento de Redes Privadas IPv6).

#### 5.6.2.4. Teste de Redundância:

5.6.2.4.1. A CONTRATADA deverá realizar testes regulares de *failover* e recuperação para garantir que todos os mecanismos de redundância estejam plenamente funcionais e aptos a entrar em operação automaticamente em caso de necessidade, devendo cumprir os requisitos abaixo:

5.6.2.4.1.1 A periodicidade de realização testes regulares deve ser previamente acordada com a CONTRATANTE Aderente;

5.6.2.4.1.2 A realização dos testes regulares deve ser previamente agendada e autorizada pela CONTRATANTE Aderente;

5.6.2.4.1.3 O relatório com os resultados dos testes regulares deve ser apresentado à CONTRATANTE Aderente;

5.6.2.4.2. Normas/Padrões aplicáveis: ISO/IEC 20000 (Gestão de Serviços de TI).

#### 5.6.2.5. Planos de Contingência:

5.6.2.5.1. A CONTRATADA deverá elaborar e apresentar planos de contingência detalhados, especificando os procedimentos de resposta e recuperação para diversos cenários de falha. Esses planos deverão ser revisados e atualizados regularmente, sendo apresentados à ATI para avaliação e aprovação.

5.6.2.5.2. Normas/Padrões aplicáveis: ISO 22301 (Gestão de Continuidade de Negócios).

5.6.3. A CONTRATADA será integralmente responsável por todas as necessidades de hardware e software necessários à implementação, manutenção e operação das redundâncias contratadas.

5.6.4. As disposições deste item tratam exclusivamente da resiliência e redundância dos Links de Acesso e da infraestrutura de conectividade no PCS, não se confundindo com o serviço de Alta Disponibilidade da Solução Unificada de Segurança de Rede, cujos requisitos técnicos, configurações e obrigações específicas estão definidos no ADENDO III – Segurança de Rede Local.

### ADENDO VI – SEGURANÇA DE DATACENTER

#### 1. Implantação, prestação dos serviços e manutenibilidade do contrato

##### 1.1. Implantação dos equipamentos e serviços de segurança:

1.1.1. A CONTRATANTE aderente deverá contratar o serviço de configuração de Alta Disponibilidade (HA) juntamente com a solução unificada de segurança para *datacenters*, assegurando a alta disponibilidade do serviço desde o início da vigência do contrato, um dos pilares fundamentais da segurança da informação;

1.1.2. Todos os equipamentos utilizados na implantação do serviço devem ser novos, sem uso anterior, garantindo a longevidade e a eficiência da infraestrutura;

##### 1.2. Condições para renovação do contrato:

1.2.1. A cada renovação do contrato, e como condição para a renovação, a CONTRATADA deverá realizar uma análise prévia das Soluções Unificadas de Segurança de Rede, para determinar se será necessário realizar a atualização, substituindo-as por modelos mais recentes ou versões atualizadas que atendam, no mínimo, às especificações originais deste Termo de Referência e aos requisitos adicionais decorrentes do crescimento e evolução da rede ao longo do período, a ser validado pela CONTRATANTE técnica ATI;

1.2.2. Nos casos em que a análise mostrar que o equipamento está atendendo ao perfil de tráfego da localidade, essa obrigatoriedade poderá ser revogada pela comissão de auditoria;

1.2.3. Esta atualização deve assegurar a continuidade da proteção e o desempenho adequado para a infraestrutura, considerando as demandas de tráfego, ameaças cibernéticas e requisitos técnicos vigentes à época;

1.2.4. A substituição dos equipamentos deverá ser realizada sem ônus adicional para a CONTRATANTE, respeitando o cronograma previamente acordado e garantindo a mínima interrupção dos serviços;

### 1.3. Instalação, Operação e Manutenção:

1.3.1. A CONTRATADA vencedora do LOTE 01 deverá fornecer dois racks de 42U para cada um dos três *Datacenters* previstos no projeto (ATI, SEE e SEFAZ), totalizando seis racks. Cada par de racks deverá ser instalado em posições físicas distintas dentro de cada *Datacenter*, garantindo a configuração em Alta Disponibilidade (HA) da Solução Unificada de Segurança (firewall). Além disso, toda a infraestrutura necessária para a instalação dos equipamentos será de responsabilidade da CONTRATADA, incluindo, mas não se limitando a:

1.3.1.1. Infraestrutura física: fornecimento e instalação de cabos UTP e ópticos, fibras ópticas, patch cords, transceivers, bandejamento, dutos, canaletas, suportes, organizadores de cabos, acessórios de fixação e etiquetagem.

1.3.1.2. Infraestrutura elétrica: provisionamento de quadros elétricos dedicados, disjuntores exclusivos, cabeamento elétrico adequado, PDUs (Power Distribution Units) com proteção contra surtos e sobrecargas, conectores elétricos compatíveis com os equipamentos, aterramento adequado e redundância elétrica conforme a norma NBR 5410.

1.3.1.3. A instalação deverá seguir as normas técnicas aplicáveis e boas práticas do setor, garantindo que todos os componentes estejam corretamente organizados, identificados e plenamente funcionais para atender às exigências operacionais e de segurança do ambiente de *Datacenter*.

1.3.2. Poderão ser instalados links multitecnologias de qualquer fonte, que atendam aos requisitos mínimos deste Termo de Referência, desde que previamente aprovados pela CONTRATANTE técnica (ATI), garantindo flexibilidade e adequação às necessidades específicas da Nova Rede Corporativa;

1.3.3. A CONTRATADA deve garantir e implementar a conexão com os links L2L - Lan to Lan, LIT1 e LIT2 especificados no Adendo VII - Serviço de Conectividade para *Datacenter*, e com os links disponibilizados pela REPEPE - Rede Pernambucana de Pesquisa e Educação;

1.3.4. Para cada solução unificada de segurança para *datacenter*, deve ser entregue um *appliance* de segurança *Sandbox*, que pode ser virtual ou físico de responsabilidade da CONTRATADA;

1.3.5. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (*appliance*), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, *hardware* e *software* devem ser integrados em um único equipamento;

1.3.6. Caso a solução ofertada não implemente nativamente todas as funcionalidades requeridas no Termo de Referência, será aceito o uso de composições com outras soluções, desde que seja garantido e comprovado o atendimento integral a todos os requisitos técnicos exigidos neste Termo de Referência, assegurando ainda a plena interoperabilidade entre os componentes da solução ofertada;

1.3.7. Possuir quantidade de memória e processamento suficientes para atendimento de todas as funcionalidades e desempenho, de acordo com a velocidade do Link contratado, solicitados neste Termo de Referência;

1.3.8. A infraestrutura do equipamento disponibilizado pela CONTRATADA, que não esteja em uso para atender aos serviços contratados pela CONTRATANTE, poderá ser integralmente utilizada pela CONTRATANTE, caso necessário;

1.3.9. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de *Next Generation Firewall* - NGFW);

1.3.10. Permitir, garantir e realizar na solução monitorar falhas de *hardware*, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, *status* do cluster, ataques e estatísticas de uso das *interfaces* de rede;

1.3.11. Garantir o envio dos logs para os sistemas de monitoramento do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa em tempo real.

## 2. Serviço de fornecimento e implantação de Solução unificada de segurança de rede – **DATACENTER**

Tabela 1 - Especificações mínimas da solução

Item	Especificação	Solução unificada de segurança de <i>datacenters</i>
1	<i>Throughput</i> de Firewall (Gbps)	140
2	Conexões simultâneas (milhões)	20
3	Novas conexões por segundo (mil)	900
4	<i>Throughput</i> de IPSec (Gbps)	50
5	Proteção combinada contra ameaças (Gbps) *	20
6	Qtd mínima de <i>interfaces</i> (100 Gbps)	4
7	Quantidade de Instâncias Virtuais Licenciadas	20

\* Na proteção combinada contra ameaças, a solução instalada deverá ter os recursos de controle de aplicação, *IPS*, proteção contra *malware* e *antivírus* habilitados simultaneamente, considerando tráfego *enterprise mix*. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.

2.1. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH, software cliente ou WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD.

2.2. Requisitos mínimos da funcionalidade de Sandbox:

2.2.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada de malwares não conhecidos (*APT Advanced Persistent Threat e Zero-Day Threats*), *ransomwares* com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de *callbacks*;

2.2.2. A solução deve possuir mecanismo para identificar hosts infectados tentando acessar endereços de DNS de domínios maliciosos;

2.2.3. Deve selecionar através de política quais tipos de arquivos sofrerão esta análise e prevenção;

2.2.4. A solução deverá implementar e identificar existência de *malware* em anexos de *e-mail* e *URL's* conhecidas;

2.2.5. Deve implementar detecção e bloqueio imediato de *malwares* que utilizem mecanismo de exploração em arquivos no formato PDF. O bloqueio poderá ser na própria solução de *Sandboxing* ou em conjunto com dispositivos de segurança compatíveis e integrados tais como *Firewall*, *e-mail secure gateway*, *endpoint* ou *web Application Firewall*.

2.2.6. A solução deve suportar integração com as ferramentas utilizadas na Nova Rede Corporativa;

2.2.7. Deverá suportar recurso de bloqueio em tempo real integrado com a solução unificada de segurança para *datacenter*, isto é, que a entrega do arquivo suspeito, seja pausada, até o veredito da plataforma de *Sandbox* definir se deverá ser transmitido ou bloqueado. Será aceito integração via API, SDKs ou conectores disponibilizados pelo fabricante;

2.2.8. A solução deverá ter suporte a *YARA rules* como padrão de criação de regras para detecção de *malware*;

2.2.9. Permitir a criação de assinaturas em tempo real para ameaças detectadas mediante a análise de comportamento em *sandbox* com distribuição da assinatura local entre os dispositivos integrados, tais como *Firewall*, *e-mail secure gateway*, *endpoint* ou *web Application Firewall*. Possibilitando assim uma proteção imediata contra novas ameaças todos os dispositivos integrados a solução de *sandbox*;

2.2.10. Deverá possibilitar, garantir e disponibilizar que o administrador da solução fazer o *download* do arquivo original, analisado pela solução de *sandbox*;

- 2.2.11. Deve suportar, garantir e realizar a análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX);
- 2.2.12. Deve suportar, garantir e realizar análise de documentos em PDF;
- 2.2.13. Deve suportar, garantir e realizar análise de arquivos compactados (ZIP, BZ2, RAR.7Z);
- 2.2.14. Deve suportar, garantir e realizar configurações GUI e CLI
- 2.2.15. Deve suportar, garantir e realizar criação de várias contas de administrador;
- 2.2.16. Deve suportar, garantir e realizar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB ou CIFS.
- 2.2.17. A solução deve garantir, realizar a inspeção do tráfego criptografado SSL em conjunto com dispositivos integrados de segurança perimetral como *Next-Generation Firewalls*;
- 2.2.18. Deve permitir, garantir e realizar atualizações automáticas de assinatura frequentes;
- 2.2.19. Deve suportar, permitir, garantir e realizar alta disponibilidade;
- 2.2.20. Deverá apresentar um detalhamento do comportamento máquina comprometida, contendo pelo menos informações sobre Tipo de Arquivo, IP de Origem do *Malware* para fins de auditoria;
- 2.2.21. Deve possuir, garantir, realizar e implementar a capacidade de diferenciar arquivos analisados, como por exemplo: por nível de risco baixo, médio e alto, ou em malicioso, não malicioso.
- 2.2.22. Deve possuir, garantir, realizar e implementar *Dashboard* com *Widgets* para conectividade e serviços, *status* de licença, desempenho, recursos do sistema e monitoramento em tempo real;
- 2.2.23. Deve ser integrado com a solução unificada de segurança para *datacenter*, onde o arquivo será executado e simulado em ambiente controlado. Permitindo o recebimento de artefatos para avaliação como também enviando resultados de detecção de ameaças e assinaturas;
- 2.2.24. Deverá possuir, garantir, realizar e implementar e estar licenciado todos os recursos/funcionalidades descritas nesta especificação durante toda a vigência do contrato de todos os itens da solução;
- 2.3. Requisitos mínimos das funcionalidades de Rede e *Firewall* dos *Datacenters*:
- 2.3.1. Ter, garantir, realizar e implementar tecnologia de *Firewall* do tipo *Statefull*;
- 2.3.2. Ser otimizada para análise de conteúdo de aplicações em camada 7;
- 2.3.3. Permitir, para o gerenciamento da solução, interface de administração via web ou cliente próprio no próprio dispositivo integrada com bases de usuários LDAP, LDAP/AD;
- 2.3.4. Realizar *VLAN* com *Tags* padrão 802.1q;
- 2.3.5. Possuir, garantir, realizar e implementar suporte a agregação de links 802.3ad e LACP;
- 2.3.6. Realizar e implementar política baseada em roteamento (*Policybasedrouting*) ou política baseada em encaminhamento (*policybasedforwarding*);
- 2.3.7. Realizar *DHCP Relay* e *DHCP Server*;
- 2.3.8. Possuir, garantir, realizar e implementar suporte a sub-*interfaces* ethernet lógicas;
- 2.3.9. Funcionar com tradução de endereços de rede (NAT) dinâmico (*Many-to-1* e *Many-to-Many*);
- 2.3.10. Funcionar com NAT estático (1-to-1, *Many-to-Many*, bidirecional 1-to-1);
- 2.3.11. Funcionar com tradução de porta (PAT);
- 2.3.12. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 2.3.13. Implementar e suportar NAT64 e NAT46;

- 2.3.14. Implementar NAT66, quando solicitado pela ATI ou o CONTRATANTE aderente;
- 2.3.15. Implementar o protocolo ICMP;
- 2.3.16. Implementar balanceamento de link por hash do IP de origem, como também por hash do IP de origem e destino;
- 2.3.17. A solução deve suportar, garantir, realizar e implementar o balanceamento de, no mínimo, três circuitos (links) simultaneamente, distribuindo o tráfego de forma equilibrada entre eles. Deve permitir a configuração de critérios de balanceamento, como percentual, peso ou prioridade, para direcionamento do tráfego conforme a necessidade da operação;
- 2.3.18. Possuir, garantir, realizar e implementar proteção contra falsificação de endereços (anti-spoofing);
- 2.3.19. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.3.20. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 2.3.21. Suportar, garantir, realizar e implementar OSPF *gracefulrestart*;
- 2.3.22. Suportar, garantir, realizar e implementar Modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.3.23. Ter a capacidade, garantir, realizar e implementar a operação de forma simultânea em uma única instância de *Firewall*, mediante o uso de suas *interfaces* físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 2.3.24. Suportar, garantir, realizar e implementar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 2.3.25. Suportar, garantir, realizar e implementar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default *gateway* das redes protegidas;
- 2.3.26. Suportar, garantir, realizar e implementar Modo misto de trabalho Sniffer, L2 e L3 em diferentes *interfaces* físicas;
- 2.3.27. Possuir, garantir, realizar e implementar suporte à criação de sistemas virtuais no mesmo equipamento (*appliance*);
- 2.3.28. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 2.3.29. Possuir, garantir, realizar e implementar controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (*Inbound*) e saída (*Outbound*), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 2.3.30. Realizar e implementar controles de políticas por porta e protocolo;
- 2.3.31. Realizar e implementar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 2.3.32. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 2.3.33. Realizar e implementar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 2.3.34. Realizar e implementar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (*Inbound*) e saída (*Outbound*);
- 2.3.35. A solução deve realizar a inspeção de conexões SSL de entrada (*Inbound*);
- 2.3.36. De-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.3;
- 2.3.37. Realizar e implementar controle de inspeção e de-criptografia de SSH ou SSL por política;

- 2.3.38. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 2.3.39. Realizar e implementar no mínimo três tipos de negação de tráfego nas políticas de *Firewall*:
- 2.3.39.1. Drop sem notificação do bloqueio ao usuário;
- 2.3.39.2. Drop com notificação do bloqueio ao usuário;
- 2.3.39.3. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 2.3.39.4. TCP-Reset para o cliente;
- 2.3.39.5. TCP-Reset para o server ou para os dois lados da conexão.
- 2.3.39.6. Serão aceitas outras nomenclaturas e classificações que representem as mesmas ações.
- 2.3.40. Realizar e implementar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 2.4. A solução deve possuir mecanismos de integração com ambientes de nuvem pública e privada, por meio de APIs, conectores ou integrações nativas, que permitam a identificação e atualização dinâmica de endereços IP, instâncias, workloads ou grupos lógicos, possibilitando sua utilização em políticas de firewall;
- 2.5. Requisitos mínimos da funcionalidade de Controle de Aplicações dos *Datacenters*:
- 2.5.1. Possuir, garantir, realizar e implementar a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 2.5.2. Realizar, garantir e implementar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 2.5.3. Possuir, garantir, realizar e implementar o reconhecimento de no mínimo 5.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, atualização de *software*, protocolos de rede, VOIP, áudio, vídeo, *proxy*, mensageiros instantâneos, compartilhamento de arquivos, *e-mail*, entre outros;
- 2.5.4. Possuir, garantir, realizar e implementar a inspeção de *payload* de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;
- 2.5.5. Possuir, garantir, realizar e implementar a detecção de aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;
- 2.5.6. Possuir, garantir, realizar e implementar a identificação do uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da *deep web* (ex.: rede Tor);
- 2.5.7. Possuir, garantir, realizar e implementar descryptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 2.5.8. Possuir, garantir, realizar e implementar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 2.5.9. Possuir, garantir, realizar e implementar atualização da base de assinaturas de aplicações automaticamente;
- 2.5.10. Possuir, garantir, realizar e implementar a limitação de banda (*download/upload*) usada por aplicações (*trafficshaping*), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;

2.5.11. Possuir, possuir, garantir, realizar e implementar a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

2.5.12. Possuir, garantir, realizar e implementar em adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

2.5.13. Possuir, garantir, realizar e implementar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;

2.5.14. Possuir, garantir, realizar e implementar em manter a segurança da rede eficiente, realizando o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

2.5.15. Possuir, garantir, realizar e implementar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria *interface* gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

2.5.16. A solução deverá permitir a criação e aplicação de regras ou assinaturas personalizadas de segurança;

2.5.17. Possuir, permitir, garantir, realizar e implementar a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

2.5.18. Possuir, permitir, garantir, realizar e implementar a configuração de alertas quando uma aplicação for bloqueada;

2.5.19. Possuir, permitir, garantir, realizar e implementar o controle de portas seja aplicado para todas as aplicações;

2.5.20. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;

2.5.21. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;

2.5.22. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o *chat* e bloquear a chamada de vídeo;

2.5.23. Possuir, permitir, garantir, realizar e implementar a diferenciação de aplicações Proxies e permitir a aplicação de políticas de controle adequadas;

2.5.24. Possuir, permitir, garantir, realizar e implementar a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (*Client-Server*, *BrowseBased*, *Network Protocol* etc.), Nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

2.6. Requisitos mínimos da funcionalidade de Prevenção de Ameaças dos *Datacenters*:

2.6.1. Possuir, permitir, garantir, realizar e implementar módulos de IPS, Antivírus e *Anti-Spyware* integrados no próprio *appliance* de *Firewall*;

2.6.2. Possuir, permitir, garantir, realizar e implementar a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware*);

2.6.3. Possuir, permitir, garantir, realizar, implementar e sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, *Anti-Spyware* quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

2.6.4. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

2.6.5. Possuir, permitir, garantir, realizar e implementar ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;

- 2.6.6. Possuir, permitir, garantir, realizar e implementar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 2.6.7. Possuir, permitir, garantir, realizar e implementar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 2.6.8. Possuir, permitir, garantir, realizar e implementar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do *Firewall*, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 2.6.9. Possuir, permitir, garantir, realizar e implementar o uso de exceções por IP de origem ou de destino nas regras e assinatura;
- 2.6.10. Possuir, permitir, garantir, realizar e implementar e suportar granularidade nas políticas de IPS, Antivírus e Anti-*Spyware*, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 2.6.11. Possuir, permitir, garantir, realizar e implementar o bloqueio de vulnerabilidades;
- 2.6.12. Possuir, permitir, garantir, realizar e implementar o bloqueio de programas exploradores de vulnerabilidades (*exploits*) conhecidos;
- 2.6.13. Possuir, permitir, garantir, realizar e implementar e incluir proteção contra ataques de negação de serviços (DoS);
- 2.6.14. Possuir, permitir, garantir, realizar e implementar assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 2.6.15. Possuir, permitir, garantir, realizar e implementar os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 2.6.16. Possuir, permitir, garantir, realizar e implementar imunidade com capacidade de impedir ataques básicos como: *Synflood*, *ICMP flood*, *UDP flood* etc.;
- 2.6.17. Possuir, permitir, realizar, implementar e garantir detectar e bloquear a origem de programas de varredura de portas (*portscans*);
- 2.6.18. Possuir, permitir, realizar, implementar e garantir bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões;
- 2.6.19. Possuir, permitir, garantir, realizar e implementar assinaturas para bloqueio de ataques de buffer overflow;
- 2.6.20. Possuir, permitir, garantir, realizar e implementar usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-*Spyware*, permitindo a criação de exceções com granularidade nas configurações;
- 2.6.21. Possuir, permitir, garantir, realizar e implementar o bloqueio de vírus e *Spywares* em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.6.22. Possuir, permitir, garantir, realizar e implementar: Identificar, alertar e bloquear comunicação com *botnets*;
- 2.6.23. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.6.24. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou anti-malware;
- 2.6.25. Possuir, permitir, garantir, realizar e implementar que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

2.6.26. Possuir, permitir, garantir, realizar e implementar a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

2.6.27. Possuir, permitir, garantir, realizar, implementar e identificar nos eventos o país de onde partiu a ameaça;

2.6.28. Possuir, permitir, garantir, realizar, implementar e incluir proteção contra vírus em conteúdo HTML e javascript, *software* espião (*Spyware*) e worms;

2.6.29. Possuir, permitir, garantir, realizar e implementar a proteção contra *downloads* involuntários usando HTTP de arquivos executáveis e maliciosos.

2.6.30. Possuir, permitir, garantir, realizar e implementar recursos de automação, com a finalidade de facilitar a operação diária dos *Firewalls*. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de *e-mails*, notificações via *webhooks* e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

2.6.31. A solução de *Firewall* deve possuir, permitir, garantir, realizar e implementar a integração com *threat feeds* externos. Suportar ao menos listas de IPs, *mac address*, *hashes* de malwares e domínios;

2.7. Requisitos mínimos da funcionalidade de Filtro de Conteúdo dos *Datacenters*:

2.7.1. Possuir, permitir, garantir, realizar e implementar no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;

2.7.2. Possuir, permitir, garantir, realizar e implementar especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.7.3. Possuir, permitir, garantir, realizar e implementar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.7.4. Possuir, permitir, garantir, realizar e implementar criação de políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/*Active directory*) e base de dados local;

2.7.5. Possuir, permitir, garantir, realizar e implementar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.7.6. Possuir, permitir, garantir, realizar e implementar a criação de categorias de URLs customizadas;

2.7.7. A solução deve possuir, permitir, garantir, realizar e implementar forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;

2.7.8. Possuir, permitir, garantir, realizar e implementar base ou cache de URLs local no *appliance* ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;

2.7.9. Deve possuir, permitir, garantir, realizar e implementar a função de exclusão de URLs do bloqueio, por categoria;

2.7.10. Possuir, permitir, garantir, realizar e implementar a customização de página de bloqueio;

2.8. Requisitos mínimos da funcionalidade de Identificação de Usuários dos *Datacenters*:

2.8.1. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, *Active directory*, e base de dados local;

2.8.2. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on; essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

2.8.3. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- 2.8.4. Permitir o controle de acesso, para saída de Internet, sendo habilitado o *captive portal*, de forma integrada com a solução proposta;
- 2.8.5. Permitir e implementar o controle de acesso, habilitando o *captive portal*, baseados em políticas definidas pela CONTRATANTE aderente;
- 2.8.6. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.8.7. Implementar a criação de grupos customizados de usuários no *Firewall*, baseado em atributos do LDAP e LDAP/AD;
- 2.8.8. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 2.8.9. A solução deverá permitir a integração com serviços de diretório e provedores de identidade (IdP), possibilitando a autenticação centralizada de usuários. A integração poderá ocorrer de forma direta ou por meio de soluções intermediárias de gerenciamento de identidade, devendo utilizar protocolos e padrões amplamente aceitos pelo mercado;
- 2.8.10. A solução deverá garantir o registro adequado e detalhado dos logs de acesso à internet, contemplando, no mínimo, a identificação do usuário autenticado, data e hora do acesso, endereço IP de origem, destino acessado e ação realizada. A identificação do usuário deverá estar associada à identidade fornecida pelo serviço de diretório ou provedor de identidade integrado à solução;
- 2.9. Requisitos mínimos das funcionalidades de Qualidade de Serviço (QoS) e Modelagem de Tráfego dos *Datacenters*:
- 2.9.1. Realizar Traffic Shaping para a solução de segurança dos Acessos Dedicados;
- 2.9.2. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 2.9.3. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 2.9.4. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 2.9.5. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo *web* ou CLI (Command Line *Interface*);
- 2.9.6. Realizar QoS (Traffic Shapping) em *interface* agregadas ou redundantes.
- 2.10. Requisitos mínimos da funcionalidade de Filtro de Dados dos *Datacenters*:
- 2.10.1. Identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 2.10.2. Identificar arquivos criptografados e aplicar políticas sobre esses tipos de arquivos;
- 2.10.3. Identificar e prevenir a transferência de informações definidas como sensíveis pela CONTRATANTE (por exemplo, número de cartão de crédito etc.) possibilitando a criação de novos tipos de dados via expressão regular.
- 2.11. Requisitos mínimos da funcionalidade de Geolocalização dos *Datacenters*:
- 2.11.1. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 2.11.2. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 2.11.3. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela *interface* gráfica e criar políticas utilizando as mesmas.
- 2.12. Requisitos mínimos da funcionalidade de Redes Virtuais Privadas (VPNs) dos *Datacenters*:
- 2.12.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 2.12.2. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 2.12.3. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-Hellman Groups 15, 16, 19, 20 ou 21;

- 2.12.4. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv2);
- 2.12.5. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;
- 2.12.6. A solução deve suportar interoperabilidade VPN com equipamentos de diferentes fabricantes, mediante a implementação de padrões abertos amplamente utilizados no mercado, incluindo suporte aos protocolos IPsec, IKEv2, AES, SHA-2, Diffie-Hellman e NAT-T, garantindo a compatibilidade com quaisquer soluções que adotem tais padrões;
- 2.12.7. Habilitar, desabilitar, reiniciar e atualizar IKE *gateways* e túneis de VPN IPsec a partir da *interface* gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 2.12.8. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 2.12.9. Realizar atribuição de DNS nos clientes remotos de VPN;
- 2.12.10. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 2.12.11. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.12.12. Permitir que a conexão com a VPN seja estabelecida antes ou após do usuário autenticar na estação;
- 2.12.13. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 2.12.14. Manter uma conexão segura com o portal durante a sessão;
- 2.12.15. Garantir e prover solução IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 2.12.16. Garantir e prover solução de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS;
- 2.13. Funcionalidade de Virtualização
- 2.13.1. Deve possuir, permitir, garantir, realizar e implementar a criação de administradores independentes para cada uma das instâncias virtuais;
- 2.13.2. Deve possuir, permitir, garantir, realizar e implementar a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 2.14. Funcionalidade de SD-WAN
- 2.14.1. A solução SD-WAN deve possuir, permitir, garantir, realizar e implementar e ser viabilizada com recursos de segurança integrados de: *Firewall*, VPN, Antivírus, IPS e Filtro de Segurança *Web*;
- 2.14.2. A solução SD-WAN deve possuir, permitir, garantir, realizar e implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 2.14.3. A solução SD-WAN deve possuir, permitir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 2.14.4. A configuração VPN IPSEC deve possuir, permitir, garantir, realizar, implementar e oferecer suporte para *DH Group*: 14 e 15;
- 2.14.5. Possuir, permitir, garantir, realizar e implementar reconhecimento em camada 7 totalmente segregado da camada 4;
- 2.14.6. Deve possuir, permitir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 2.14.7. O reconhecimento de aplicações deve possuir, permitir, garantir, implementar e realizar independente de porta e protocolo, inspecionando o *payload* de pacote de dados;

2.14.8. Ainda sobre o reconhecimento de Aplicações, a solução deve possuir, permitir, garantir, realizar e implementar e fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);

2.14.9. A solução deve possuir, permitir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;

2.14.10. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

2.14.11. Deve haver mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN para que ocorra o chaveamento do tráfego para outro link;

2.14.12. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da *Interface* SD-WAN;

2.14.13. Deverá permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

2.14.14. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;

2.14.15. A solução de SD-WAN deve ser compatível com o uso de túneis VPN dinâmicos;

2.14.16. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar pelo menos um dos métodos descritos abaixo:

2.14.16.1. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;

2.14.16.2. Passivo: uso do tráfego real para as medições.

### 3. **Serviço de configuração das soluções unificadas de segurança em Alta Disponibilidade (HA) para *DATACENTER* com fornecimento dos equipamentos necessários para ativação do serviço**

3.1. O serviço consiste em configurar os *Firewalls* para operar em modo de Alta Disponibilidade (HA), garantindo que um dispositivo possa assumir automaticamente as funções do outro em caso de falha;

3.2. A CONTRATANTE aderente deverá solicitar no início da vigência do contrato, o serviço de Alta Disponibilidade (HA) para a Solução Unificada de Segurança para *Datacenter*;

3.3. A configuração deve garantir a continuidade do serviço de rede e a integridade dos dados durante e após o processo de *failover*;

3.4. Para o serviço, deverão ser disponibilizados todos os transceivers, cabos e conectores, bem como dois switches necessários para complementar a infraestrutura para alta disponibilidade (HA);

3.5. Requisitos mínimos dos switches para o serviço de alta disponibilidade (HA):

**Tabela 2 - Especificações mínimas da solução**

Item	Especificação	Quantidades de portas do Switches
1	25G/10G SFP28/SFP+	24
2	40G/100G QSFP+/QSFP28	6

3.5.1. Deve possuir no mínimo 24 (vinte e quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 10GbE ou slots SFP+28 para conexão de fibras ópticas do tipo 25GBase-X. Sendo que a escolha do tipo

de transceiver a ser fornecido deverá depender da arquitetura do datacenter e quantidade de links a ser instalado, garantindo a melhor adequação às condições e requisitos da infraestrutura.

3.5.2. Deve possuir no mínimo 6 (seis) slots QSFP+/QSFP28 para conexão de fibras ópticas do tipo 100GBase-X. A escolha do tipo de transceiver a ser fornecido deverá depender da arquitetura do datacenter a ser instalado, garantindo a melhor adequação às condições e requisitos da infraestrutura.

3.5.3. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

3.5.4. Deve possuir interface para gerenciamento local do tipo. Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

3.5.5. Deve possuir capacidade de comutação de no mínimo 840 Gbps e ser capaz de encaminhar no mínimo 1.000 Mpps;

3.5.6. Deve suportar no mínimo o modo de encaminhamento de tráfego store-and-forward;

3.5.7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

3.5.8. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;

3.5.9. Deve possuir tabela MAC com suporte a 64.000 endereços;

3.5.10. Deve operar com latência igual ou inferior à 1us (microsegundo);

3.5.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

3.5.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

3.5.13. Deve suportar Multi-Chassis Link Aggregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;

3.5.14. Deve suportar a comutação de Jumbo Frames;

3.5.15. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

3.5.16. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

3.5.17. Deverá possuir hardware com capacidade de suportar roteamento dinâmico utilizando os protocolos RIP, BGP e OSPF para IPv4, bem como OSPF para IPv6, ou suas versões mais recentes. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

3.5.18. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM ou PIM-SSM MAP (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;

3.5.19. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

3.5.20. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

3.5.21. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;

3.5.22. Deve implementar serviço de DHCP Server e DHCP Relay;

3.5.23. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 4000 (quatro mil) grupos;

- 3.5.24. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);
- 3.5.25. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN ou ERSPAN;
- 3.5.26. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;
- 3.5.27. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
- 3.5.28. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
- 3.5.29. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- 3.5.30. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
- 3.5.31. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
- 3.5.32. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
- 3.5.33. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo ToS ou CoS e VLAN ID;
- 3.5.34. Deve permitir de forma nativa ou através de composição de soluções a definição de dias e horários que a ACL deverá ser aplicada na rede;
- 3.5.35. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 3.5.36. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;
- 3.5.37. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection), Deficit Weighted Round Robin (DWRR) ou Weighted Fair Queuing (WFQ);
- 3.5.38. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 3.5.39. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
- 3.5.40. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
- 3.5.41. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- 3.5.42. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 3.5.43. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

- 3.5.44. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
- 3.5.45. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- 3.5.46. Deve suportar autenticação por endereço MAC (MAC Authentication Bypass – MAB), inclusive sob outras nomenclaturas ou classificações adotadas por fabricantes que representem a mesma funcionalidade;
- 3.5.47. Deve implementar RADIUS CoA (Change of Authorization);
- 3.5.48. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 3.5.49. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
- 3.5.50. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 3.5.51. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
- 3.5.52. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 3.5.53. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 3.5.54. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 3.5.55. Deve implementar Netflow, sFlow ou similar;
- 3.5.56. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 3.5.57. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1/v2c e v3;
- 3.5.58. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 3.5.59. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 3.5.60. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 3.5.61. Deve permitir ser gerenciado através de IPv6;
- 3.5.62. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 3.5.63. Deve suportar autenticação via RADIUS e TACACS+;
- 3.5.64. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 3.5.65. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 3.5.66. Deverá suportar ser configurado e monitorado através de REST API;
- 3.5.67. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;

3.5.68. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

3.5.69. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

3.5.70. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

#### 4. Solução de segurança de confiança zero - ZTNA

4.1. A solução deve garantir acesso seguro a aplicações hospedadas em qualquer local, independentemente de os usuários estarem em trabalho remoto ou nas dependências da instituição. Em conformidade com o modelo de Confiança Zero (Zero Trust), usuários e dispositivos deverão ser considerados confiáveis somente após verificação e autenticação adequadas;

4.2. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas, que poderá ser implantado em ambiente on-premises ou em nuvem;

4.3. Deve ser compatível e do mesmo fabricante da Solução unificada de segurança de rede – *DATACENTER*;

4.4. O controle de acesso deve ser dinâmico e baseado em contexto (usuário, dispositivo, aplicação, localização e postura de segurança), conforme modelo adaptativo de confiança zero (ZTNA);

4.5. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;

4.6. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal *web* SSL a ser acessado por cada usuário;

4.7. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;

4.8. Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows, Microsoft Windows Server, Mac OS e Linux;

4.9. É imprescindível que o agente seja atualizado periodicamente para garantir a compatibilidade contínua com novas versões dos sistemas operacionais. Caso qualquer versão do sistema operacional atinja o fim do suporte, o fornecedor deverá manter o suporte do agente por um período adicional de 6 meses, assegurando que o cliente tenha tempo suficiente para transitar para uma versão compatível, minimizando impactos operacionais;

4.10. A solução de ZTNA deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.

4.11. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;

4.12. A solução deve exigir a utilização obrigatória de autenticação multifator (MFA) para todos os usuários, independentemente do uso do agente. O mecanismo de MFA deve ser aplicado em todas as etapas do processo de autenticação, garantindo maior segurança no acesso aos recursos corporativos;

4.12.1. Requisitos mínimos da solução de MFA:

4.12.1.1. Deve permitir o download gratuito nas lojas de aplicativos separado do seu provisionamento

4.12.1.2. O aplicativo deve suportar exclusão e adição de novos tokens

- 4.12.1.3. Deve ser instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota
- 4.12.1.4. Deve garantir a privacidade do dispositivo móvel, ou seja, não deve ser capaz de consultar histórico de navegação
- 4.12.1.5. Deve requerer a permissão proprietário para envio de notificações ou qualquer tipo de alteração nas configurações
- 4.12.1.6. Deve suportar as principais plataformas de mobile do mercado (iOS (iPhone, iPod Touch, iPad), Android)
- 4.12.1.7. Deve suportar a geração dinâmica das sementes de token, minimizando a exposição online.
- 4.12.1.8. Deve suportar ativação através da utilização de QR Codes e manual
- 4.12.1.9. Deve criptografar o armazenamento de sementes utilizadas na geração do token
- 4.12.1.10. Deve ser capaz de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH
- 4.12.1.11. Deve suportar a ocultação do token para tokens baseados em tempo (TOTP)
- 4.12.1.12. Deve ser capaz de proteger abertura do aplicativo através de PIN ou Impressão Digital ou Face Security
- 4.12.1.13. Deve exibir o intervalo de tempo OTP
- 4.12.1.14. Deve exibir o número de série do token
- 4.12.1.15. Deve suportar que a senha gerada possa ser copiada para a área de transferência
- 4.12.1.16. Deve suportar detalhes de login enviados ao telefone para aprovação com um toque
- 4.12.1.17. Deve usar um serviço de provisionamento dinâmico, onde apenas na atribuição de um token a um usuário a semente é criada e é removida durante o download ou após um tempo limite configurável.
- 4.12.1.18. Deve ser compatível e integrável com o item Solução de gerenciamento de identidade de acesso deste termo.
- 4.12.1.19. Deve estar de acordo com as seguintes RFCs para especificações OTP: RFC6238 e RFC4226
- 4.12.1.20. Deve ser capaz de realizar vinculação com o dispositivo móvel
- 4.12.1.21. Deve suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor Radius
- 4.12.1.22. Deve ser compatível com Google, Amazon e outros tokens TOTP (Time-based One-Time Password) compatíveis com OAT.
- 4.13. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único pelo agente e deverá ainda ser compartilhado com o proxy de acesso;
- 4.14. Deve ser possível revogar o certificado de um agente por meio da console central;
- 4.15. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;
- 4.16. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados estejam diferentes, o acesso deverá ser bloqueado por padrão;
- 4.17. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;

- 4.18. A solução deve prover *backup* automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;
- 4.19. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;
- 4.20. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;
- 4.21. Deve ser possível exportar os logs diretamente a nível de agente;
- 4.22. Deve ser possível exigir uma senha para desconectar o agente da console central;
- 4.23. Deve existir a possibilidade de restringir o usuário de realizar *backup* da configuração do agente;
- 4.24. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;
- 4.25. Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir *tags* aos *endpoints* de acordo com o índice de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal;
- 4.26. Deve ser possível configurar o agente para usar Proxy;
- 4.27. O agente deve permitir a configuração local via XML (eXtensible Markup Language);
- 4.28. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;
- 4.29. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;
- 4.30. Deverá ser possível enviar uma notificação por *e-mail* contendo o código de registro para os usuários finais informados, bem como um link para *download* do instalador do agente;
- 4.31. Deve ser possível especificar a validade do código de registro;
- 4.32. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net.
- 4.33. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;
- 4.34. Deve ser possível agrupar agentes em grupos;
- 4.35. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;
- 4.36. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política
- 4.37. A console central deve apresentar um resumo das informações de cada *endpoint*, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust *tags* associadas, detalhes da conexão de rede cabeada e Wi-Fi, detalhes do *hardware* como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão do agente está em uso em um respectivo *endpoint*, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;
- 4.38. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;
- 4.39. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;

- 4.40. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do *endpoint* visando criar entradas DNS;
- 4.41. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
- 4.42. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os *endpoints* e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;
- 4.43. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;
- 4.44. As regras de conformidade devem gerar *tags* que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado *endpoint* diretamente no proxy de acesso;
- 4.45. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;
- 4.46. Deve ser possível construir *tags* com verificações no *endpoint*, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o *endpoint* está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;
- 4.47. A console central deve permitir exportar e importar *tags* entre sistemas diferentes por meio de um arquivo JSON;
- 4.48. Deve ser possível verificar quais *endpoints* estão associadas com cada *tag*;
- 4.49. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma *tag* simultaneamente, caso a política possua vínculo com diversas *tags*;
- 4.50. Deve ser possível criar regras no proxy de acesso vinculando *interface* de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;
- 4.51. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;
- 4.52. Deve possibilitar definir funções administrativas relacionadas às permissões dos *endpoints*, de políticas e de configurações gerais;
- 4.53. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn ou Google, podendo ainda notificá-los para que esse vínculo possa ser realizado;
- 4.54. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de *endpoint*, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;
- 4.55. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;
- 4.56. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;
- 4.57. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;
- 4.58. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;

- 4.59. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;
- 4.60. O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário;
- 4.61. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;
- 4.62. Deve suportar a criação de várias versões de pacotes de instalação;
- 4.63. Deve possuir módulo para execução de filtro *web* a nível de *endpoint* mediante uso do agente local, realizando a filtragem diretamente no *endpoint*, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego *web* com base na categoria de URL ou filtro de URL customizado;
- 4.64. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;
- 4.65. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;
- 4.66. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;
- 4.67. Deve ser possível verificar as violações de filtro *web* diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;
- 4.68. Deve ser possível determinar quando o filtro *web* entrará em ação no agente, se ele deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;
- 4.69. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;
- 4.70. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução;
- 4.71. Deve permitir visibilidade unificada de usuários, dispositivos, aplicações e ameaças por meio de dashboards de telemetria e Zero Trust Analytics.
- 4.72. A solução deve suportar políticas de prevenção contra perda de dados (DLP) baseadas em conteúdo e contexto, com mecanismos de identificação e proteção de informações sensíveis.
- 4.73. A solução deve prover mecanismos de integração com o SIEM e o SOAR fornecidos no ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CIISC, por meio de APIs abertas, conectores nativos ou exportação de logs em formato padrão (como Syslog ou JSON), permitindo o envio em tempo real de eventos de autenticação, acesso e postura de dispositivos para monitoramento e análise centralizada.
- 4.74. A solução deve possuir mecanismos de hardening do agente, impedindo modificações, desinstalação ou desativação por usuários não autorizados. Deve permitir que o administrador configure restrições de segurança e políticas de proteção que garantam a integridade e o funcionamento contínuo do agente, mantendo registro de tentativas de alteração no portal de administração.

## 5. Solução de proteção, detecção e resposta para servidores - EDR

### 5.1. Requisito do Agente (Coletor)

- 5.1.1. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows Server, Linux RedHat, Oracle Linux OL (antigo OEL), CentOS e Ubuntu;
- 5.1.2. É imprescindível que o agente seja atualizado periodicamente para garantir a compatibilidade contínua com novas versões dos sistemas operacionais. Caso qualquer versão do sistema operacional atinja o fim do suporte, o

fornecedor deverá manter o suporte do agente por um período adicional de 6 meses, assegurando que o cliente tenha tempo suficiente para transitar para uma versão compatível, minimizando impactos operacionais;

5.1.3. A solução proposta deve consumir menos de 1 GB de espaço em disco;

5.1.4. A solução proposta deve oferecer suporte à implantação em massa e automatizada por meio de ferramentas de gerenciamento e distribuição de software amplamente utilizadas no mercado, tais como MS System Center, JAMF, Red Hat Satellite, ou mecanismos equivalentes, incluindo controladores de domínio Active Directory;

5.1.5. A solução proposta deve ter a capacidade de atualizar o terminal sem interação do usuário e sem exigir uma reinicialização;

5.1.6. A solução proposta deve ter proteção "Anti-violação" no Agente;

5.1.7. A solução proposta deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos;

5.1.8. A solução proposta deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o conhecimento do usuário associado aos eventos;

5.1.9. A solução proposta deve ter a opção de definir a senha para desinstalar o agente no terminal

5.1.10. A solução proposta deve ser capaz de gerar um instalador Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração do usuário;

5.1.11. O coletor que será instalado nos terminais da solução proposta deve ser capaz de trabalhar por trás de um proxy.

## 5.2. Requisito - Detecção de *malware*

5.2.1. A solução proposta deve ser capaz de funcionar no modo "offline" sem que o Agente esteja conectado à rede corporativa

5.2.2. A solução proposta deve ser capaz de detectar processos em execução, inícios de processos, paradas de processos e interações entre processos.

5.2.3. A solução proposta deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do PC.

5.2.4. A solução proposta deve ser capaz de detectar as solicitações de DNS enviadas do dispositivo.

5.2.5. A solução proposta deve ser capaz de detectar conexões de rede a partir do dispositivo.

5.2.6. A solução proposta deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL.

5.2.7. A solução proposta deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção.

5.2.8. A solução proposta deve ser capaz de incorporar as técnicas MITER ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas.

5.2.9. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como: nome do arquivo e hash do arquivo etc.

5.2.10. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a arquivos (Criação, Exclusão, Renomear).

5.2.11. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis)

5.2.12. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Brind);

5.2.13. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas aos logs do Windows (Log de eventos);

5.2.14. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Windows (criação de chave, exclusão de chave, conjunto de valores);

5.2.15. A solução proposta deve ter a capacidade de realizar consultas de texto livre para filtrar as informações disponíveis para a caça de ameaças;

5.2.16. A solução proposta deve ter a capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro;

5.2.17. A solução proposta deve ter a capacidade de agendar pesquisas armazenadas

5.2.18. A solução proposta deve identificar atividades maliciosas conhecidas

5.2.19. A solução proposta deve ter a capacidade de receber atualizações diárias de inteligência

5.2.20. A solução proposta deve ter a capacidade de categorizar os eventos detectados em diferentes categorias (Ex: Malicioso, Suspeito, Inconclusivo, Provavelmente Seguro)

5.2.21. A solução proposta deve ter a capacidade de coexistir com outras soluções de segurança de *endpoint* do tipo de antivírus tradicional ou de nova geração.

5.2.22. A solução deve permitir a inserção de listas do tipo allow list e block list, de forma que, se o hash do artefato estiver em alguma lista, ele será considerado limpo ou malicioso, de forma correspondente. Evitando que seja desnecessariamente analisado pela solução.

### 5.3. Requisito - Prevenção de *malware*

5.3.1. A solução proposta deve ter a capacidade de prevenir a execução de arquivos maliciosos

5.3.2. A solução proposta deve incorporar um mecanismo de antivírus de última geração (Next-Generation Antivírus) baseado no kernel do sistema operacional, com capacidade de "Aprendizado de Máquina" (Machine Learning).

5.3.3. A solução proposta deve ter a capacidade de controlar dispositivos USB

5.3.4. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo

5.3.5. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo

5.3.6. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo.

5.3.7. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série

5.3.8. A solução proposta deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados

5.3.9. A solução proposta deve ser capaz de bloquear o tráfego de comunicação malicioso para C&C (Comando e Controle);

5.3.10. A solução proposta deve ser capaz de impedir violações de segurança e tentativas de *ransomware* em tempo real;

5.3.11. A solução proposta deve ser capaz de evitar a criptografia causada por *ransomware* e modificação de arquivos ou registro de dispositivos, caso isso ocorra, a solução deverá restaurar os arquivos afetados/modificados para o seu estado original em tempo real

5.3.12. A solução proposta deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: Ativo, desativado ou apenas criar "logs" para as regras de segurança contidas nestes;

5.3.13. A solução proposta deve ser capaz de ser configurada em modo de simulação onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas.

5.3.14. A solução proposta deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio;

5.3.15. A solução proposta deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o Agente instalado;

5.4. Requisito - Difusão (Pós-infecção);

5.4.1. A solução proposta deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada uma atividade causada por *malware*.

5.4.2. A solução proposta deve permitir alterar as políticas atribuídas de um dispositivo onde uma atividade causada por *malware* foi encontrada

5.4.3. A solução proposta deve permitir o bloqueio de atividades realizadas por arquivos maliciosos

5.4.4. A solução proposta deve ter a capacidade de criar exceções para processos com base na localização do arquivo (Caminho do Arquivo)

5.4.5. A solução proposta deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado pelo processo.

5.4.6. A solução proposta deve ter a capacidade de criar exceções para os processos baseados no usuário que o processo executou

5.4.7. A solução proposta deve ter a capacidade de criar exceções manualmente para falsos positivos para marcar a atividade como um falso positivo e evitar a ocorrência de falhas futuras

5.4.8. A solução proposta deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes.

5.5. Requisito - Resposta ao Incidente

5.5.1. A solução proposta deve permitir o armazenamento de histórico dos eventos.

5.5.2. A solução proposta deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses.

5.5.3. A solução proposta deve permitir a integração com plataformas SIEMs (Security Information and Event Management) através de um *syslog*

5.5.4. A solução proposta deve ter a capacidade de obter instantâneos de memória ou "dumps" de memória que permitam a realização de processos forenses.

5.5.5. A solução proposta deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA

5.5.6. A solução proposta deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data / hora ocorrida, atividade suspeita etc.) para permitir a integração via API

5.5.7. A solução proposta deve ter a capacidade de encerrar um processo com base em sua classificação

5.5.8. A solução proposta deve ter a capacidade de excluir um arquivo com base em sua classificação

5.5.9. A solução proposta deve ter a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida

5.5.10. A solução proposta deve ter a capacidade de isolar os dispositivos infectados da rede.

5.5.11. A solução proposta deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (Malicioso, suspeito etc.) do processo detectado

5.5.12. A solução proposta deve obter visibilidade total da cadeia de ataques e alterações maliciosas

5.5.13. A solução proposta deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo.

5.5.14. A solução proposta deve permitir a assinatura de serviços opcionais de detecção e resposta a incidentes (Ex: serviços gerenciados de detecção e resposta)

5.5.15. A solução proposta deve permitir o envio de executáveis para análise em um *sandbox*, a fim de determinar se são maliciosos ou inofensivos.

5.5.16. A solução proposta deve possuir integração com *Active directory* a fim de possibilitar a utilização de *playbooks* para contenção e resposta à incidentes de segurança

5.5.17. A solução proposta deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso, o bloqueio de uma conexão de rede.

#### 5.6. Requisito - Controle de Vulnerabilidade e Comunicação

5.6.1. A solução proposta deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o terminal

5.6.2. A solução proposta deve ter capacidade para realizar um patch virtual, através da restrição de acessos de comunicação nas aplicações vulneráveis.

5.6.3. A solução proposta deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter.

5.6.4. A solução proposta deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede.

5.6.5. A solução proposta deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado.

5.6.6. A solução proposta deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede.

5.6.7. A solução proposta deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo.

5.6.8. A solução proposta deve ser capaz de visualizar e entregar informações sobre o uso dos aplicativos de rede mostrando informações como os destinos IP do tráfego gerado pelo aplicativo.

#### 5.7. Requisito - Cenários de Ataque

5.7.1. A solução proposta deve identificar e prevenir tentativas de perseguição de privilégios

5.7.2. A solução proposta deve bloquear ataques de *ransomware* conhecidos

5.7.3. A solução proposta deve detectar *malware* desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do *malware* e não de uma assinatura

5.7.4. A solução proposta deve proteger contra scripts Powershell maliciosos

5.7.5. A solução proposta deve proteger contra scripts CScript maliciosos

5.7.6. A solução proposta deve proteger contra macros maliciosas do Office

5.7.7. A solução proposta deve ter controle sobre dispositivos USB.

#### 5.8. Requisito - Console de Administração

- 5.8.1. A Solução deve conter políticas de segurança e *playbooks* básicos pré-definidos, sem que haja a necessidade de criação manual logo após a instalação da solução
- 5.8.2. A solução proposta deve estar em conformidade com os padrões de segurança de dados da indústria de cartões de pagamento (PCI DSS)
- 5.8.3. A solução proposta deve estar em conformidade com o padrão HIPAA
- 5.8.4. A solução proposta deve estar em conformidade com o padrão GDPR
- 5.8.5. O console de gerenciamento da solução proposta deve permitir a integração com o "*Active directory*" para garantir o cumprimento dos requisitos da política de senhas da empresa.
- 5.8.6. O console de administração da solução proposta deve permitir o uso de autenticação de dois fatores (2FA) para acessá-la.
- 5.8.7. O console de administração da solução proposta deve permitir a integração com SAML para autenticação do usuário no console de gerenciamento
- 5.8.8. O console de administração da solução proposta deve permitir o uso de funções granulares para administradores
- 5.8.9. O console de administração da solução proposta deve permitir o gerenciamento de ambientes multilocatários.
- 5.8.10. O console de administração da solução proposta deve permitir o gerenciamento por meio da API Full Restful
- 5.8.11. A solução proposta deve permitir integração com soluções de NGFW, SIEM e *Sandbox*.
- 5.8.12. A solução proposta deve suportar integração com base de dados do fabricante do produto com atualizações de inteligência de ameaças contra malwares;
- 5.8.13. A solução proposta deve suportar integração NGFW onde um controle de ZTNA (Zero Trust Network Access) possa ser amplamente estabelecido por intermédio de verificação de postura do endpoint, de forma que, ao identificar um processo potencialmente malicioso no endpoint alvo, a solução possa enviar informações de restrição/bloqueio ao NGFW e/ou componentes de Zero Trust para tomada de ação automatizada, a fim de não permitir o acesso desse ativo a aplicações e sistemas críticos a partir da máquina com suspeita ou até mesmo comprometida.
- 5.8.14. Deve-se também ser possível integrar-se a arquitetura de Zero Trust, a validação da instalação do agente de EDR dentro do dispositivo dos usuários e servidores, de modo a conseguir definir que apenas dispositivos com postura validada e que possuam a solução de EDR previamente instalada no *endpoint* alvo possam ter seus acessos permitidos pelas políticas de ZTNA do *Firewall*.
- 5.8.15. O console de administração da solução proposta deve permitir a visualização dos eventos registrados nos dispositivos que requerem atenção.
- 5.8.16. O console de administração da solução proposta deve permitir a visualização da saúde dos Agentes instalados
- 5.8.17. O console de administração da solução proposta deve permitir a desinstalação remota do Agente instalado nos dispositivos;
- 5.8.18. O console de administração da solução proposta deve permitir a desativação / ativação remota do Agente instalado nos dispositivos;
- 5.8.19. O console de administração da solução proposta deve permitir a atualização remota do Agente instalado nos dispositivos
- 5.8.20. O console de administração da solução proposta deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o *status* do sistema.
- 5.8.21. O console de administração da solução proposta deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais.

5.8.22. O console de administração da solução proposta deve permitir a exportação dos logs locais gerados pelos Agentes a partir do mesmo console

5.8.23. O console de administração da solução proposta deve permitir a criação de relatórios de inventário dos Agentes implantados contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, *Status* do Agente, último dia visto pelo console

5.8.24. O console de gerenciamento da solução proposta deve ter a visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado.

5.8.25. O console de administração da solução proposta deve permitir a integração de um SMTP externo para envio de alertas por *e-mail*.

5.8.26. O console de administração da solução proposta deve permitir auditorias de alterações feitas por administradores / operadores. Essas auditorias também devem ser baixadas em formato CSV ou XML.

5.8.27. A solução deve permitir o isolamento do endpoint em caso de incidente, diretamente ou por integração com a solução de NAC, assegurando a contenção automática ou manual do ativo comprometido.

5.8.28. A solução proposta deve permitir adicionar endereços IP maliciosos detectados em um ou mais *Firewalls* remotos integrados.

5.8.29. A solução proposta deve permitir a configuração de perfis nas informações coletadas para a função de caça a ameaças.

5.8.30. A solução proposta deve permitir exclusões de informações que não serão coletadas na função de caça a ameaças.

5.8.31. A solução proposta deve entregar informações geradas pelos serviços de inteligência para a tomada de decisão na nuvem sobre o evento detectado.

5.8.32. A solução proposta deve permitir que os serviços em nuvem recategorizem uma classificação de evento

5.8.33. A solução proposta deve permitir que os administradores desabilitem as notificações para um evento de descoberta.

## 6. Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede - NDR

### 6.1. Características Gerais da Solução

6.1.1. Deve possuir licenciamento e garantia do fabricante durante todo o período do contrato.

6.1.2. Deve ser capaz de detectar anomalias de tráfego e detecção de *malware*, de forma passiva na rede.

6.1.3. Deve através de recursos como *Machine Learning* (supervisionado e não supervisionado) e Inteligência Artificial, a solução deve permitir a detecção de anomalias, provendo visibilidade ao órgão a respeito do tráfego de rede.

6.1.4. Deve realizar classificação de malwares baseando-se nas características detectadas no artefato analisado.

6.1.5. Deve identificar o paciente zero, a origem do incidente.

6.1.6. Deverá integrar-se com as demais soluções do projeto para fins de automação na resposta a incidentes, reduzindo a dependência do fator humano.

6.1.7. A solução deve estar devidamente licenciada para atender em sua totalidade o fluxo de rede da CONTRATANTE, garantindo minimamente as seguintes características:

6.1.7.1. A solução deve suportar no mínimo 65536 IPs.

6.1.7.2. Deve ser capaz de processar no mínimo 9 Gbps de tráfego HTTP;

6.1.8. A Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede (NDR) deve ser fornecida e mantida por meio de um *appliance*, que poderá ser implementado em formato virtual, físico ou baseado em Nuvem. A responsabilidade pela operação, atualização e manutenção ficará exclusivamente a cargo da CONTRATADA;

6.1.9. Qualquer solução implementada pela CONTRATADA, dentre as diversas opções sugeridas, deve ser disponibilizada em alta disponibilidade, garantindo a continuidade dos serviços sem interrupções, sempre que forem contratadas duas unidades pelos órgãos aderentes ou pela própria ATI-PE;

6.1.10. A solução deve ser atualizada constantemente pelo fabricante, de forma que esteja atualizada com as *engines* mais eficiente e updates de assinaturas que a tornem mais eficiente;

6.2. Funcionalidades de Detecção de Malwares e Anomalia de Tráfego

6.2.1. Deve possuir engine para inspeção de arquivos e assegurar a compatibilidade com os NGFWs fornecidos;

6.2.2. Caso seja um arquivo comprimido (Ex: ZIP), a solução deve ser capaz de realizar a extração do arquivo original (em até 3 camadas) para que, dessa forma, possa ser analisado.

6.2.3. Todos os arquivos devem passar por uma análise multicamadas.

6.2.4. A solução deve realizar inspeções conforme abaixo:

6.2.4.1. Análise estática, pela *engine* de antivírus;

6.2.4.2. Análise dinâmica, baseada em Inteligência Artificial;

6.2.5. Deve suportar uma grande quantidade de extensões de arquivo. Minimamente: EXE, PDF, HTML, ZIP, VBS, DOCX, MP3, DLL, DOC, POWERSHELL, PPTX, JAR, APK, RTF, MIME, BAT, TOR, AVI, BMP, PNG, GIF, JPEG, CLASS e PETITE

6.2.6. Mediante identificação de *malware*, a solução, em conjunto com *Firewalls* de mercado, deve suportar o bloqueio *inline* da transferência, impedindo que o usuário final tenha contato com o *malware*

6.2.7. Deve permitir a detecção de arquivos maliciosos em compartilhamentos de rede SMB e NFS, de forma nativa ou por meio de integração com soluções de segurança complementares. Deve suportar a aplicação de ações automatizadas, incluindo quarentena ou isolamento, de forma customizada, considerando a criticidade do risco identificado;

6.2.8. O *scan* de compartilhamentos de rede deve funcionar de forma agendada e manual.

6.2.9. Como resultado, o *scan* de compartilhamento deve apontar o nome do arquivo, local e criticidade.

6.2.10. Para cada arquivo detectado no *scan* de compartilhamentos de rede, a solução deve expor detalhes, tais como: URL, nome do arquivo, *malware* encontrado e hash.

6.2.11. A solução deverá permitir integração com mecanismos externos de inspeção de conteúdo, análise de malware ou prevenção contra vazamento de dados (DLP), de forma nativa ou mediante integração com soluções especializadas do mercado, utilizando protocolos ou mecanismos amplamente adotados;

6.2.12. A solução deve prover contexto sobre as intenções do *malware*, indo além de uma simples análise do artefato.

6.2.13. Deve organizar os incidentes de segurança por tipo e criticidade, informando o quantitativo para cada situação. *Phishing*, *Data Leak*, *DoS*, *Backdor*, pequeno, médio, alto e criticidade alta.

6.2.14. Deve usar recursos de inteligência artificial (AI) para localizar a origem do ataque (paciente zero).

6.2.15. Deve criar uma linha do tempo, evidenciando, passo a passo, como o incidente/tentativa ocorreu.

6.2.16. Deve prover uma visão do *malware*, informando: veredito, tipo de *malware*, URL, hash, características do artefato, técnicas utilizadas e ações tomadas por ele

6.2.17. Deve informar ao administrador sobre possíveis anormalidades identificadas por meio de *Machile Learning* (ML), envolvendo combinações de características pouco usuais no tráfego e que fujam ao baseline mapeado. Deve também permitir que o usuário dê um feedback para cada anomalia identificada.

6.2.18. Deve ser possível realizar *upload* de artefatos, para teste sob demanda.

6.2.19. Deve permitir ao administrador buscar por incidentes de segurança que contenham determinadas características. Minimamente: hash, cópia do *malware*, nome do incidente ou família do antivírus.

6.2.20. Deve permitir buscas recursivas, indo além das informações previamente fornecidas.

6.2.21. Deve possuir recursos de Machine Learning para detecção de tráfego anômalo. A *engine* deve ser treinada, de forma que aprenda o comportamento padrão da rede.

6.2.22. Deve utilizar, como parte do processo de aprendizado, características como: IP de origem e destino, endereços mac, geolocalização, categoria do elemento, fabricante, protocolo (rede e aplicação), tamanho de pacote, porta de destino e versão de TLS.

6.2.23. Deve possuir mecanismo que impeça novas análises caso a fila esteja demasiadamente grande.

### 6.3. Características de Visibilidade

6.3.1. Deve prover *Dashboards* customizáveis

6.3.2. Deve prover diversas estatísticas: tipos de elementos encontrados na rede, padrões de ataques mais comuns, anomalias encontradas por risco e tipo, ataques detectados x quantidade, ataques criptografados, aplicações em uso, origens detectadas e botnets encontradas.

6.3.3. Deve informar a quantidade de arquivos detectados e processados. E, como parte do processo de autoaprendizado, quantificar os recursos aprendidos com eles

6.3.4. O painel deve exibir informações básicas: *uptime*, *firmware*, *hostname*, ocupação do disco, licenças aplicadas, CPU, memória e fila de processamento de arquivos

6.3.5. Deve realizar inventário, de acordo com os elementos descobertos na rede, permitindo o enriquecimento a partir de: endereços mac, *hashes*, *hostname* e definições do usuário

6.3.6. Deve informar sobre *botnets* identificadas na rede

6.3.7. Deve informar sobre URLs e IPs nocivos identificados (IOCs). Deve, ainda, informar se fazem parte de alguma campanha

6.3.8. Deve prover *Widgets* que evidenciem ataques a nível de rede, tentativas de exploração de vulnerabilidade

6.3.9. Deve informar sobre eventual uso de criptografia fraca na rede

6.3.10. Deve ser capaz de identificar ataques em tráfego criptografado, através de análise JA3.

6.3.11. Deve gerar relatórios sobre os artefatos analisados. PDF, CSV ou STIX

6.3.12. Deve permitir o *download* do sample do *malware*, protegido com senha

6.3.13. Deve possuir abas separadas para conferir logs de *malware* e de anomalias de tráfego

6.3.14. Deve possuir aba de inventário, que evidencie os elementos de rede detectados pela solução e que permita uma análise aprofundada, considerando: nível de confiança, data em que foi descoberto, anomalias descobertas por criticidade e janela de tempo, eventos de segurança relacionados e consumo de banda.

### 6.4. Funcionalidades de Resposta a Incidente e Integrações

6.4.1. A solução, além de detectar anomalia em tráfego e análise de malwares deve, também, permitir a execução de resposta a incidente, agindo rapidamente para mitigar gaps de segurança

6.4.2. Como triggers para execução de *playbook*, a solução deve considerar: *malware* e botnet detectado, ataque criptografado, ataque de rede, IOC identificado, criptografia baixa e uso de protocolo vulnerável

6.4.3. Como triggers para execução de *playbook*, a solução deve considerar: severidade do evento, tanto para tráfego anômalo quanto para *malware*, bem como nível de assertividade.

6.4.4. Deve permitir a exclusão de origens pré-determinadas, evitando eventual falso positivo

6.4.5. Havendo "match" em alguma regra de automação, a solução deve executar resposta pré-definida, tomando ações diferentes componentes de rede, visando mitigar o incidente

6.4.6. Deve permitir ação para efetivar uma mitigação, bem como para desfazer uma ação

6.4.7. Deve suportar interações com *Firewalls*, NAC e qualquer solução da Nova Rede Corporativa que permita interações via API

6.4.8. Caso a solução demande licenciamento para utilizar o recurso de resposta a incidente, será de responsabilidade da CONTRATADA, sem ônus adicional a CONTRATANTE durante todo o período do contrato;

6.4.9. Deve prover log a respeito de cada ação tomada pela solução, informando quando ela é feita com sucesso, falha, duplicada e omitida

6.4.10. Deve integrar-se com soluções de *sandbox*, permitindo aumentar a taxa de detecção de malwares bem como velocidade na análise

6.5. Serviço de Gerenciamento e Atualizações

6.5.1. Deve permitir gerência da solução usando contas locais ou remotas. Nesse caso, LDAP e radius

6.5.2. Deve permitir a criação de perfis diversos, com diferentes níveis de permissão, de forma granular

6.5.3. Deve permitir configurar o horário via NTP e de forma manual

6.5.4. A solução deve combinar bases locais e em cloud para detecção de tráfego ou malwares maliciosos

6.5.5. Deve permitir *backup* e *restore*

6.5.6. Deve permitir envio de alertas por *e-mail*

6.5.7. Deve suportar sniffer de tráfego

6.5.8. A solução deve dispor de APIs para facilitar integrações. Ex: submissão de arquivos.

## 7. Solução para gerenciamento de acessos à rede datacenter - NAC

7.1. Este item deve incluir o licenciamento da controladora, se aplicável, durante todo o período do contrato, e as unidades serão contratadas individualmente de forma granular;

7.2. Todas as funcionalidades descritas devem estar devidamente licenciadas, com suporte do fabricante e com a possibilidade de atualização para novas versões para o período total do contrato;

7.3. A Solução de Gerenciamento de Acessos à Rede (NAC) deverá ser fornecida e mantida integralmente pela CONTRATADA. A solução poderá ser implementada em formato virtual, físico ou em Nuvem, conforme necessidade. Toda a responsabilidade pela operação, atualização e manutenção será exclusiva da CONTRATADA;

7.4. Deve funcionar, com todas as funcionalidades ativas, em camada de rede Layer 3.

7.5. A solução deve ser entregue em alta disponibilidade;

7.6. Possuir plataforma unificada que combina AAA e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas, permitindo licenciamento futuro das funções de NAC e BYOD;

7.7. Suporte a seguintes fontes para autenticação:

7.7.1. Microsoft *Active directory*;

7.7.2. Kerberos;

7.7.3. LDAP;

7.7.4. Radius;

7.7.5. HTTP;

7.7.6. Lista estática de endereços MAC;

- 7.8. Deve possuir integração com a Solução unificada de segurança de *datacenter* para possibilitar "Single Sign-on" (SSO) para os usuários identificados.
- 7.9. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
- 7.9.1. Atributos do usuário autenticado,
- 7.9.2. Hora do dia, dia da semana,
- 7.9.3. Tipo de dispositivo utilizado,
- 7.9.4. Localização do usuário;
- 7.9.5. Tipo de autenticação utilizado;
- 7.10. Permitir a visualização de todas as informações relativas a cada transação/autenticação em uma única tela, como:
- 7.10.1. Data e Hora;
- 7.10.2. Mac Address do dispositivo;
- 7.10.3. Classificação do dispositivo;
- 7.10.4. Usuário;
- 7.10.5. Equipamento que requisitou a autenticação (origem);
- 7.10.6. Método de autenticação utilizado;
- 7.10.7. Fonte de autenticação utilizada para validação;
- 7.10.8. Perfil de acesso aplicado;
- 7.11. Todos os atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Logs já filtrados para a requisição em análise;
- 7.12. Deve possuir *Dashboard* customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
- 7.13. Lista com os últimos Alertas do sistema;
- 7.14. Gráfico com o *status* das autenticações aceitas e rejeitadas;
- 7.15. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
- 7.16. Deve implementar funcionalidade de classificação automática de dispositivos ("Device profiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 7.17. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora etc.), por sistema operacional (ex. Windows, Linux, MacOS etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server etc.);
- 7.18. Deve suportar a coleta de informações, para classificação, usando no mínimo:
- 7.18.1. DHCP fingerprint,
- 7.18.2. HTTP,
- 7.18.3. MAC OUI,
- 7.18.4. SNMP,
- 7.18.5. Subnet Scanner,
- 7.18.6. MDM;

- 7.18.7. TCP Fingerprinting;
- 7.19. Deve possuir base de regras e categorias de dispositivos pré-configurada;
- 7.20. Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;
- 7.21. Deve suportar a integração com soluções de MDM (Mobile Device Management) de forma nativa ou por meio de API;
- 7.22. Suporte a RADIUS CoA ou mecanismo equivalente de alteração dinâmica de autorização, e Web authentication.
- 7.23. Deve suportar os seguintes métodos de autenticação:
- 7.23.1. TLS
- 7.23.2. TTLS
- 7.23.3. PEAP
- 7.23.4. MD5
- 7.23.5. GTC
- 7.23.6. MSCHAPV2
- 7.23.7. WPA
- 7.23.8. Online Certificate *Status* Protocol (OCSP)
- 7.23.9. *WEB* Authentication;
- 7.24. Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP);
- 7.25. Suporte a aplicação de políticas em ambiente multi vendor de *Wireless*, LAN e VPN;
- 7.26. Deve suportar integração com no mínimo os seguintes provedores de infraestrutura de segurança: CheckPoint, Cisco/SourceFire, Fortinet, FireEye, Juniper/Netscreen, Sonicwall e Tenable;
- 7.27. Deve suportar integração com no mínimo os seguintes sistemas operacionais: Android, Apple MAC OSX e iOS, Linux Ubuntu, Microsoft Windows;
- 7.28. Deve ser capaz de implementar políticas de segurança baseadas em no mínimo:
- 7.28.1. Localidade;
- 7.28.2. Usuários e ou grupo de Usuários;
- 7.28.3. Hosts ou grupo de Hosts;
- 7.28.4. Usuário temporário,
- 7.28.5. Guest;
- 7.29. Deve implementar resposta automática a incidente com a Solução unificada de segurança de *datacenter* deste edital, ou seja, os incidentes detectados pela Solução unificada de segurança de *datacenter* devem ser utilizados para resposta automática ao incidente, como, por exemplo, mover o host afetado para uma VLAN de quarentena;
- 7.30. Deve fazer a checagem de compliance dos *Endpoints* (Hosts). Os *Endpoints* (Hosts) são computadores, dispositivos móveis ou qualquer outro equipamento que necessite se conectar à rede. A checagem de compliance deve verificar se os *Endpoints* (Hosts) seguem as políticas de segurança definidas pelo ABC.
- 7.31. Deve realizar a checagem de compliance dos Endpoints (Hosts) por meio de mecanismos de verificação devendo suportar, no mínimo, a verificação com agente permanente, bem como a verificação temporária, a qual poderá ser implementada por meio de agente temporário ou de forma agentless.
- 7.32. Deve fazer a checagem de compliance dos *Endpoints* (Hosts), verificando no mínimo os seguintes itens:

- 7.32.1. Atualização de segurança do sistema operacional, Windows, MacOS ou Linux;
- 7.32.2. Antivírus;
- 7.32.3. Informações do sistema operacional;
- 7.33. Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptação da comunicação.
- 7.34. Deve suportar EDUROAM.
- 7.35. Suporte à integração com plataforma de terceiros usando HTTP/RESTful API.
- 7.36. Suporte aos seguintes recursos através de IPv6:
- 7.37. Administração via *WEB* e CLI.
- 7.38. Acesso a servidores com endereçamento IPv6 para contexto de *endpoints*;
- 7.39. A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam à mesma "zona".
- 7.40. A solução deve permitir a geração e o envio através de *e-mail* ou SMS de alertas relativos às seguintes atividades anormais detectadas na rede:
  - 7.40.1. Autenticações;
  - 7.40.2. Acesso a dispositivos de rede;
  - 7.40.3. Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios;
  - 7.40.4. Atividades irregulares nos servidores da solução;
- 7.41. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por *e-mail* em formato de no mínimo PDF;
- 7.42. Deve possuir ferramentas para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal *web* seguro.
- 7.43. Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
- 7.44. Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;
- 7.45. Deve permitir que o visitante crie sua própria credencial temporária ("self- service") através do portal *web*, sem a necessidade de um autorizador;
- 7.46. Deve realizar o caching de endereço MAC dos usuários visitantes;
- 7.47. Deve fornecer os certificados SSL válidos para o *captive portal* ou necessária para qualquer outra interação usuário e sistemas, tais como AD e servidores de *e-mail*;
- 7.48. Todas as licenças devem ser fornecidas durante todo o período do contrato;

## 8. Solução de segurança de identidade privilegiada - PAM

- 8.1. Deve permitir o gerenciamento centralizado de acessos privilegiados;
  - Entende-se por acessos privilegiados os tipos de acesso a ativos e a sistemas de tecnologia, além dos acessos realizados por um usuário comum, geralmente realizados por administradores de redes, administradores de servidores e administradores de sistemas;

8.2. A solução deve controlar o acesso baseado em função, com recursos de auditoria e de segurança, provendo no mínimo as seguintes funcionalidades:

8.2.1. Cofre de credenciais: funcionalidade onde os usuários não precisam ter conhecimento das credenciais, reduzindo-se o risco de vazamento, incluindo o rotacionamento automático dessas credenciais;

8.2.2. Controle de acesso a contas privilegiadas: funcionalidade onde é possível estabelecer níveis de privilégios de cada usuário, incluindo funcionalidades de fluxo de aprovação de acessos a determinados recursos;

8.2.3. Monitoramento e registro de eventos: funcionalidade onde é possível monitorar, registrar e auditar as atividades dos usuários privilegiados, incluindo informações das sessões tais como pressionamento de teclas, eventos de mouse etc.;

8.3. A Solução para Gerenciamento de Acessos Privilegiados (PAM) deve ser fornecida e mantida integralmente nas dependências da CONTRATADA, por meio de um *appliance*, que poderá ser implementado em formato virtual, físico ou em nuvem. A responsabilidade pela operação, atualização e manutenção ficará exclusivamente a cargo da CONTRATADA;

8.4. As chaves criptográficas devem ser armazenadas internamente na solução e protegidas por tecnologia TPM, vTPM ou através de integração nativa utilizando o protocolo PKCS#11;

8.5. A solução deve ter a possibilidade de integração com o item “SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO” e com o item “SOLUÇÃO DE ZTNA” deste processo, sendo possível, portanto, o uso da autenticação centralizada e de *tags* Zero-Trust;

8.6. A solução deve prover *interface* de API para integração com sistemas ou soluções de terceiros;

8.7. A solução deve diferenciar os usuários da plataforma entre:

8.7.1. Usuários comuns: aqueles que apenas executam as tarefas de gerenciamento dos sistemas de destino, como por exemplo a equipe de TI, um contratado da TI, um administrador de banco de dados (DBA). Geralmente estes usuários são Gerentes de TI e Administradores de Sistemas de TI.

8.7.2. Usuários administradores: aqueles que são responsáveis pelas tarefas de gerenciamento da solução.

8.8. A solução deve operar pelo menos nos seguintes modos:

8.8.1. Modo Proxy: toda conexão aos sistemas de destino é interceptada pela solução, que fica responsável pela conexão final ao sistema de destino. Nesse modo, a máquina cliente não tem acesso direto as credenciais de acesso e o administrador da solução pode interromper conexões se um comportamento estranho for detectado;

8.8.2. Modo Não-Proxy: toda conexão aos sistemas de destino parte diretamente da máquina cliente e a solução fornece ao cliente as credenciais para esse acesso;

8.9. A solução deve armazenar de forma segura o nome de usuário e a senha/chave dos servidores como segredos. Os segredos podem conter informações sobre login, credenciais e o endereço IP do servidor de destino. O usuário final pode usar o segredo para acessar os servidores;

8.10. As credenciais reais devem ser protegidas e os usuários da solução não podem acessar as credenciais, exceto em alguns casos configuráveis pelo administrador. As credenciais de login podem ser alteradas automaticamente e manualmente, a depender dos diferentes casos de uso;

8.11. A solução deve permitir a configuração de políticas comuns e um sistema de fluxo de aprovação hierárquico e auditável para acesso a informações sensíveis;

8.12. Os critérios de gerenciamento de senha devem ser configuráveis para atender à política organizacional de frequência de alteração de senha/controle de aprovação de uso/alteração após o uso;

8.13. Deve incluir, mas não se limitar, aos seguintes recursos de sistemas, protocolos e ferramentas: Active Directory (AD), Windows, Linux/Unix, Oracle DB, Microsoft SQL (MS SQL), Microsoft SQL Shell, MySQL CLI, MySQL Shell, PostgreSQL CLI, VNC, Web SMB, Web SSH, Web RDP e Web SFTP;

- 8.14. Deve permitir a construção de um conector de plataforma personalizado e integração A2A;
- 8.15. Deve oferecer suporte para aprovação de credencial dupla, exigindo aprovações de usuários designados antes de permitir o acesso a credenciais para contas gerenciadas;
- 8.16. Deve oferecer suporte a funcionalidades de fluxo de trabalho para controles de liberação de senha e sessão, incluindo suporte para vários níveis de autorização, capacidade de agrupar autorizadores;
- 8.17. Deve suportar a capacidade de expirar a solicitação de aprovação após um período;
- 8.18. Deve fornecer a capacidade de permitir recursos de check-out e check-in para secrets;
- 8.19. Deve permitir a autenticação de uma sessão sem revelar a senha por meio da máquina do usuário final;
- 8.20. Sessões privilegiadas devem ser transmitidas por proxy por meio de um *hardware* seguro ou dispositivo virtual;
- 8.21. O proxy de sessão deve ser capaz de entrar em uma conta sem liberar uma senha para o usuário privilegiado;
- 8.22. A solução deve permitir o uso do modo cliente, com o uso de agentes, e deve oferecer suporte ao modo somente navegador, onde nenhum *software* cliente/agente é necessário;
- 8.23. Os seguintes modos de cliente e navegador devem ser suportados:
- 8.23.1. Modo cliente: PuTTY, Windows Remote Desktop, RealVNC, TightVNC e WinSCP etc;
- 8.23.2. Modo de navegador: *Web* SSH, *Web* RDP, *Web* VNC, *Web* SMB, *Web* SFTP e *Web* Account;
- 8.23.3. No modo navegador, deve possibilitar o uso de pelo menos as seguintes funcionalidades: acesso a senhas, sessões e administração da solução;
- 8.24. Deve possuir iniciadores de conexão para pelo menos: MySQL (CLI e Shell), Microsoft SQL CLI, PostgreSQL CLI, SSH (PuTTY, SSH CLI e SecureCRT), Remote Desktop e VNC (TightVNC e VNC Viewer);
- 8.25. As sessões devem permitir a inclusão ou exclusão de comandos executados durante uma sessão sem a necessidade de um agente;
- 8.26. Deve suportar registro/monitoramento de sessões registrando o nome de usuário, endereço IP, duração da sessão, volume de tráfego, data e hora do último login;
- 8.27. Deve permitir a auditoria das atividades administrativas da própria solução;
- 8.28. As solicitações de acesso privilegiado devem ser feitas usando um modelo de solicitação/liberação, no mínimo;
- 8.29. Não deve permitir que um administrador da solução realize o bypass do fluxo de aprovação para obter uma senha ou ativar uma sessão;
- 8.30. A solução deve oferecer suporte à sessão remota de auditoria no modo não transparente ou transparente, sem alteração no fluxo de trabalho para acessar a sessão remota usando ferramentas nativas do cliente, incluindo injeção direta de credencial;
- 8.31. Deve suportar monitoramento e gravação de sessão (para análise posterior) e seu monitoramento em tempo real (para vigilância em tempo real), permitindo que o administrador encerre as sessões, caso necessário;
- 8.32. As gravações do vídeo da sessão devem usar formatos disponíveis publicamente, devendo ser armazenadas pelo período mínimo de 06 (seis) meses;
- 8.33. Deve ser possível gerar alertas de *e-mail* quando um usuário executa um comando restrito e a detecção de tais comandos não devem depender do uso de agentes;
- 8.34. Deve suportar diferentes métodos de autenticação e integração com sistemas corporativos como: *Active directory*, LDAP, SAML, RADIUS;
- 8.35. Deve suportar no mínimo múltiplo fator de autenticação (MFA);
- 8.36. Deve permitir a configuração de OTP (One Time Password) via *e-mail*;

- 8.37. Deve permitir a verificação de arquivos transferidos entre o *endpoint* e os ativos protegidos, realizando-se a varredura contra conteúdos maliciosos;
- 8.38. Deve suportar o uso de verificações contra vazamento de dados (DLP) nos arquivos transferidos;
- 8.39. Deve suportar o bloqueio da área de transferência dos ativos privilegiados, para impedir a cópia de informações desses ativos;
- 8.40. Deve fornecer a funcionalidade de Break Glass para acesso emergencial as credenciais armazenadas na solução;
- 8.41. Deve restringir o acesso a console dos ativos protegidos pela solução;
- 8.42. Deve proteger o acesso à rede dos ativos protegidos pela solução;
- 8.43. Deve armazenar todas as senhas em um cofre seguro com criptografia AES-256;
- 8.44. Deve permitir que qualquer login/senha usado para acesso a ativos protegidos seja armazenado internamente e com segurança e deve permitir que os usuários se conectem aos ativos protegidos sem o conhecimento do login/senha utilizado;
- 8.45. Deve alterar automaticamente as senhas para um grupo de recursos;
- 8.46. Deve estabelecer acesso granular às senhas;
- 8.47. Deve impedir os usuários vejam a senha em texto puro;
- 8.48. Deve permitir que as credenciais sejam injetadas diretamente nos sistemas, dando acesso aos usuários sem que eles vejam ou forneçam credenciais;
- 8.49. Deve suportar o controle de acesso sem o uso de VPN;
- 8.50. Deve permitir que as sessões sejam mantidas e compartilhadas com os auditores para interação (colaboração de sessão);
- 8.51. Deve permitir que os auditores monitorem usuários privilegiados sob demanda e em tempo real;
- 8.52. Deve integrar um sistema de fluxo de trabalho para permitir o acesso administrativo às máquinas identificadas;
- 8.53. A solução deve permitir acesso ao recurso de destino, sem agente, pelo menos nos protocolos RDP, SSH, TELNET, VNC, HTTPS;
- 8.54. Deve possibilitar o bloqueio do usuário no caso de uma execução de uma ação restrita;
- 8.55. Deve permitir rastreabilidade das conexões;
- 8.56. Deve permitir visualizar todas as conexões ativas;
- 8.57. Deve permitir rastreabilidade e controle de transferências de arquivos;
- 8.58. Deve permitir a configuração de notificações de *e-mail* em um determinado número de indicadores, como eventos relacionados ao tráfego (falha de conexão, falha de autenticação etc.);
- 8.59. Deve permitir integração com soluções SIEM para relatórios avançados e processamento em tempo real de detecção de comportamento malicioso;
- 8.60. Deve possuir logs de auditoria completos e pesquisas avançadas, como pesquisas de texto para isolar incidentes;
- 8.61. Os logs de auditoria da solução devem mostrar claramente quem acessou qual dispositivo de destino, bem como a duração (hora de início e hora de término);
- 8.62. Deve fornecer logs para o histórico de aprovação de sessões privilegiadas;
- 8.63. Deve possuir um painel para exibir os usuários conectados no momento;
- 8.64. Deve permitir relatórios personalizáveis.

9. **Solução de Filtro de Aplicações WEB - WAF**

9.1. A Solução de Filtro de Aplicações Web deverá ser fornecida através de *appliance* que poderá ser implementado em formato virtual, físico ou em nuvem, sob total responsabilidade da CONTRATADA. A solução deve atender aos seguintes requisitos mínimos:

9.1.1. Deve suportar no mínimo 8 (oito) *interfaces* virtuais;

9.1.2. Suportar área de armazenamento interno de no mínimo 02 (dois) Terabytes;

9.1.3. Deve suportar no mínimo 03 (Três) instâncias administrativas independentes entre si, permitindo criar níveis diferentes de privilégios de acesso dos administradores;

9.1.4. Deve suportar no mínimo para 08 (Oito) vCPU;

9.1.5. Deve possuir capacidade de tratamento para um *Throughput* HTTP de no mínimo, 2,8 (dois virgula oito) Gbps.

9.2. Sempre que forem contratadas duas unidades pelos órgãos aderentes ou pela própria ATI-PE, a solução deverá obrigatoriamente ser implementada em Alta Disponibilidade (HA), garantindo a continuidade dos serviços sem interrupções, garantindo a continuidade ininterrupta dos serviços e atendendo aos requisitos de capacidade definidos nesta especificação. A CONTRATADA será integralmente responsável por assegurar suporte contínuo para tráfego, conectividade, conexões, requisições de nível 7, requisições SSL e transações.

9.3. Durante toda a vigência do contrato, a solução deve implementar e manter, no mínimo, as seguintes funcionalidades ativas e em pleno funcionamento: Reputação de IP, Defesa contra Preenchimento de Credenciais e Análise Avançada de Ameaças (*Sandbox*)

9.4. Durante a operação não impor degradação no tempo de resposta da aplicação que possa implicar em Timeout da operação do usuário ou degradação na experiência do usuário – qualquer diferença no tempo de resposta para a atuação do WAF deve ser imperceptível para o usuário final da aplicação protegida.

9.5. Deve ser capaz de funcionar no mínimo como Proxy reverso de aplicações;

9.6. Deve preservar e encaminhar o endereço IP real do visitante para aplicação/ativo protegido pelo WAF, podendo ser adicionado em campo de cabeçalho X-Forwarded-For ou X-Real-IP;

9.7. Deve suportar a granularidade de criação de configurações/regras/políticas específicas por subdomínio;

9.8. Deve suportar endereçamento IPv4 e IPv6;

9.9. Sobre os *softwares* e licenciamentos: devem ser fornecidos todos os *softwares* e licenciamentos de forma a permitir a plena utilização e operação dos requisitos previstos para a solução durante todo o período do contrato, contemplando todos os itens abaixo descritos:

9.9.1. Deve oferecer *interface* gráfica *web* para a configuração de todas as funções do produto, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS. Não deve exigir nenhum tipo de instalação de algum *software* proprietário, Driver, Plugin ou semelhante, ou mesmo protocolo proprietário para qualquer operação relacionada ao serviço de gestão do produto na estação/navegador do cliente.

9.9.2. Deve possuir administração baseada em *interface web* HTTPS, de forma centralizada, devidamente protegida por autenticação;

9.9.3. Deve ter a capacidade de alertar/notificar em sua console em tempo real qualquer ocorrência de um ataque;

9.9.4. Deverá armazenar, minimamente, para cada evento detectado: endereço IP de origem, porta TCP de origem, dados relativos ao destino do ataque (domínio, IP, porta), data e hora da mensagem e identificador relativo ao tipo de ataque/regra/política, bem como nível de severidade do ataque.

9.9.5. Deverá possuir ferramenta, na *interface* gráfica de gerência (*Dashboard*) que permita visualizar os últimos Logs de ataque detectados/bloqueados;

- 9.9.6. Deve prover as seguintes informações, na *interface* de gráfica de gerência: estatísticas de *Throughput* HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP/HTTPS em tempo real e últimos Logs de eventos do Sistema;
- 9.9.7. Deve ser capaz de exportar Logs para servidor externo via protocolo *SYSLOG*;
- 9.9.8. Deve ser capaz de enviar alertas por *e-mail* de eventos baseados em severidades e/ou categorias;
- 9.9.9. Deve possuir dados analíticos contendo localização geográfica dos clientes *web*;
- 9.9.10. Deve possuir dados analíticos, sendo possível visualizar a *contagem* total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (Hits) e percentual de cada país de origem;
- 9.9.11. Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;
- 9.9.12. Deve ser possível visualizar através da *interface* gráfica de gerência as informações de licenças e assinaturas;
- 9.9.13. Realizar configuração da ferramenta, registrando as alterações realizadas, permitindo auditoria de data/hora e autoria de qualquer modificação realizada;
- 9.9.14. Deve ser possível executar e restaurar *backup* de configurações;
- 9.9.15. Deve prover as funcionalidades e customizações nos relatórios:
- 9.9.15.1. Permitir que sejam gerados relatórios com base em filtros dos campos dos Logs. Por exemplo: filtrar os ataques com a ação de alertar/bloquear, com base no nome de políticas.
- 9.9.15.2. Tipos de relatórios: de ataque, de tráfego, de evento;
- 9.9.15.3. Mostrar os tops ataques nos últimos minutos ou nas últimas 24 (vinte e quatro) horas;
- 9.9.15.4. Registrar eventos para melhor detalhamento com data, horário com precisão de segundos (ou maior precisão) e especificação do Tempo Universal Coordenado (UTC) equivalente ou de acordo com o timezone do sistema;
- 9.10. No caso de equipamentos servidores que ofereçam diversas aplicações por um mesmo endereço IP, toda proteção deve ser baseada na URL das aplicações e não no endereço IP, independente do protocolo HTTP ou HTTPS.
- 9.11. Permitir a criação de novas regras sem interrupção de conexões estabelecidas;
- 9.12. Produto deve oferecer RESTful API para gerenciamento de configurações e integrações;
- 9.13. A configuração de administração da solução deve possibilitar a criação e customização de perfis, para gestão e operação da solução, permissão de leitura de relatórios, escrita e implementação de políticas.
- 9.14. Suportar múltiplos administradores logados ao mesmo tempo na *interface* de administração;
- 9.15. Características de bloqueio/tratamento:
- 9.15.1. Para funcionamento do WAF, não depender de Plugins, agentes ou Softwares na aplicação protegida;
- 9.15.2. Deve ser capaz de suportar a configuração e proteção de aplicações configuradas em HTTPS;
- 9.16. A solução deve oferecer proteção contra ameaças e técnicas de ataque definidas pelo OWASP (owasp.org), contemplando no mínimo o que consta no relatório TOP 10 (<https://owasp.org/Top10/> - mínimo relatório ano 2021), tanto para aplicações *web* quanto APIs através do OWASP API TOP10
- 9.17. Inspeção de tráfego HTTP/HTTPS, em diferentes versões;
- 9.18. Suporte ao TLS 1.0, 1.1, 1.2 e 1.3;
- 9.19. Gestão do certificado digital das aplicações na ferramenta;
- 9.20. Permitir importar certificados digitais de CA's;

- 9.21. Possibilitar configuração para recodificar em SSL/TLS a requisição ao enviar para o servidor, permitindo otimização em um ambiente 100% criptografado;
- 9.22. Deve ser capaz de redirecionar requisições HTTP para HTTPS;
- 9.23. Deve suportar redirecionamento e reescrita de requisições e respostas HTTP;
- 9.24. Deve permitir redirecionar requisições para outro *web* site;
- 9.25. Deve permitir customizar conteúdo da resposta e *Status Code* para requisições HTTP com erro (minimamente *status* 50X e 40X);
- 9.26. Deve permitir a customização das telas de resposta de bloqueios implementados pelo WAF;
- 9.27. Deve possuir mecanismo de aprendizado automático capaz de criar proteções e detectar padrões a partir de qualquer conteúdo presente na requisição:
- 9.27.1. O conteúdo das requisições;
- 9.27.2. Partes das URLs;
- 9.27.3. Parâmetros em URLs e seus tipos de dados;
- 9.27.4. Campos de formulários e seus tipos de dados;
- 9.28. Para o mecanismo de aprendizado automático, deverá possuir pelo menos 2 camadas de linguagem de máquina a fim de diminuir o número de falso positivos e diminuir atrito com a aplicação, no momento de instalação. Caso a solução possua apenas 1 camada de linguagem de máquina, deverá ser considerado outra solução WAF secundária, com os mesmos recursos apresentados neste termo, para contemplar o atendimento a este item a fim de ajustar a ferramenta em relação aos falsos positivos.
- 9.29. Deve implementar recursos de Sandbox para análise de malware moderno, de forma nativa ou integrada;
- 9.29.1. Deve permitir a configuração para que todos os arquivos que correspondem às regras de restrição sejam submetidos a uma solução de *Sandbox*.
- 9.29.2. A solução de *Sandbox* deve avaliar se os arquivos representam uma ameaça e retornar os resultados ao Filtro de Aplicações *WEB*.
- 9.29.3. Se a solução *Sandbox* determinar que o arquivo é malicioso, o sistema deve realizar as seguintes ações:
- 9.29.3.1. Gerar uma mensagem de log de ataque contendo o resultado (por exemplo, mensagens com a ação Alerta).
- 9.29.3.2. Executar a ação especificada na política de segurança de arquivos. Durante este período, o sistema não deve reenviar o arquivo para a solução de *Sandbox*.
- 9.30. Deve implementar recursos de antivírus para análise de arquivos, detecção e bloqueio de malwares, possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação, de forma nativa ou integrada;
- 9.31. A solução deverá integrar-se com a Solução de segurança de confiança zero deste termo, com a finalidade de estabelecer a identidade do dispositivo por meio de certificados de cliente e confiança do dispositivo
- 9.32. O padrão aprendido de forma automatizada deve poder ser identificável pela *interface web* da ferramenta, permitindo sua edição, inibição ou remoção;
- 9.33. A solução deverá integrar-se com a Solução de proteção, detecção e resposta para dispositivos de Tráfego de Rede deste termo, para detecção de arquivos suspeitos que foram carregados nas aplicações *WEB*;
- 9.34. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas, que permitam a troca de informações entre o WAF e as soluções de nuvens dos clientes da ATI-PE. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas no WAF.
- 9.35. Conectores SDN Públicos

9.35.1. AWS

9.35.2. Microsoft Azure

9.36. A solução deve ser capaz de verificar os eventos do cliente, como movimento do mouse, teclado, toque na tela e/ou rolagem em um período especificado e determinar se a solicitação vem de um humano ou de um bot. Deve ser possível configurar a regra de detecção baseada em biometria para definir o evento do cliente, o período de coleta e/ou URL da solicitação.

9.37. Deve possuir a capacidade de criação de políticas ou regras baseadas em assinaturas de ataque customizáveis; seja a partir de parâmetros aprendidos ou manualmente, de forma a criar regras OWASP baseadas em cabeçalhos, Cookies, características de parâmetros, dados presentes no corpo da requisição e expressões regulares.

9.38. Permitir que o ataque seja registrado mesmo sem ação de bloqueio (em regras de Bypass).

9.39. Deve ser possível implementar atualizações de novas assinaturas em modo de alerta ou monitoramento, evitando assim que novas assinaturas causem impacto no ambiente produtivo.

9.40. Deve possuir uma base de dados de reputação de endereços IP públicos com atualização automática.

9.41. Possuir a capacidade de implementar bloqueio automático de redes de má reputação, como redes de anonimato.

9.42. Permitir regras de bloqueio a métodos HTTP indesejados, com granularidade por aplicação configurada (possibilidade de criação de diferentes perfis para aplicar em diferentes aplicações/serviços/servidores);

9.43. Permitir regras de bloqueio conforme *Status Code* da resposta HTTP, com granularidade por aplicação configurada (possibilidade de criação de diferentes perfis para aplicar em diferentes aplicações/serviços/servidores);

9.44. Detectar e bloquear ataques que explorem violação ou não-conformidade no protocolo HTTP;

9.45. Possibilidade de proteger aplicações que disponibilizam o serviço HTTP ou HTTPS fora das portas padrão;

9.46. Possibilidade de configurar portas não-padrão para aplicação *web* HTTP e HTTPS;

9.47. Controle por número de requisições em determinado intervalo de tempo (Access Rate Control);

9.48. O WAF oferecido deverá implementar o bloqueio de ataques tipo DoS na camada 7, ou uso abusivo de funcionalidades (controle de requisições por intervalo de tempo) possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio.

9.49. Detecção de ataques automatizados e implementação de desafio de Captcha podendo ser por integração externa;

9.50. Criação de políticas e controle de acesso as aplicações por geolocalização de endereço IP, com lista de geolocalização atualizada automaticamente;

9.51. Permitir a criação de controles por lista de endereços IP de origens autorizadas (Allow List, Bypass) e lista de endereços IP de origens bloqueadas (Deny List), com granularidade por ativo protegido. Manual ou automaticamente (baseada em reputação de endereço IP);

9.52. Suportar políticas de segurança positiva e negativa, Allow Lists e Deny Lists;

9.53. Mecanismo automático de bloqueio de endereços de origem (Deny List) – permanente ou temporário, com alerta e possibilidade de reversão;

9.54. Ser compatível com IIS, Jboss, TomCat, Apache, Nginx entre outros;

9.55. Suporte a inspeção de sistemas com autenticação SSO (Single Sign On);

9.56. Proteção para API's:

9.57. Fornecer proteção para a comunicação API, sejam elas implementadas usando XML, JSON API ou RESTful API.

- 9.58. Permitir o processamento e a validação de arquivos de esquema JSON.
- 9.59. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403.
- 9.60. Permitir o processamento e a validação de arquivos de esquema XML.
- 9.61. Permitir definir o seguinte formato do esquema: SOAP ou XML
- 9.62. Suportar as seguintes funções de API *gateway*:
- 9.63. Autenticação de usuários API
- 9.64. Controle de acesso API
- 9.65. Controle de limite de taxa
- 9.66. Reescrita de chamada de API
- 9.67. Permitir a restrição baseada em endereçamento IP
- 9.68. Permitir a restrição baseada em referenciadores HTTP
- 9.69. Proteção de *Webservices* em arquitetura Soap;
- 9.70. Deve oferecer minimamente detecção e proteção a ataques do tipo:
  - 9.70.1. Clickjacking;
  - 9.70.2. Code Injection e suas variações, (contemplando no mínimo HTML, XML, Javascript, PHP e Java)
  - 9.70.3. Command Injection (contemplando no mínimo PHP, Java, Powershell e Linux Shell, e detectar técnicas de ofuscação de comandos);
  - 9.70.4. SQL Injection;
  - 9.70.5. Ldap Injection;
  - 9.70.6. Exploração de vulnerabilidades baseadas no formato XML;
  - 9.70.7. Exploração de vulnerabilidades baseadas no formato JSON;
  - 9.70.8. Alteração de Cookies;
  - 9.70.9. Alteração de campos escondidos;
  - 9.70.10. Cross Site Request Forgery (CSRF);
  - 9.70.11. Cross Site Scripting (XSS) e variantes;
  - 9.70.12. Comportamento de Botnet;
  - 9.70.13. Negação de serviço (DoS e DDoS) em camada de aplicação;
  - 9.70.14. Abuso de formulários de login e outros ataques de força bruta;
  - 9.70.15. HTTP Header Overflow;
  - 9.70.16. Violação de protocolo HTTP;
  - 9.70.17. Buffer Overflow;
  - 9.70.18. Local File Inclusion (FLI);
  - 9.70.19. Remote File Inclusion (RFI);
  - 9.70.20. Man In The Middle (MITM);
  - 9.70.21. Server Information Leakage e dados sigilosos de configuração;
  - 9.70.22. Path/Directory Traversal;

9.70.23. Server Side Request Forgery (SSRF).

9.71. A solução deve incluir funcionalidade de balanceamento de carga entre servidores *web*.

9.72. Deve ter a habilidade de configurar portas não-padrão para aplicação *web* HTTP e HTTPS.

9.73. Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores *web*.

9.74. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários.

9.75. Suportar algoritmo Round Robin para balanceamento de carga de servidores.

9.76. Suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores.

9.77. Suportar algoritmo Least Connections para balanceamento de carga de servidores.

9.78. A solução deve ser capaz de criar servidores virtuais que definem a *interface* de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido.

9.79. Os servidores virtuais devem entregar o tráfego à um único servidor *web* e também possuir a opção de distribuir as sessões/conexões entre os servidores *web* do Server Pool.

9.80. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool.

9.81. Permitir teste de disponibilidade de servidor *web* através do método TCP.

9.82. Permitir teste de disponibilidade de servidor *web* através do método ICMP ECHO\_REQUEST (ping).

9.83. Permitir teste de disponibilidade de servidor *web* através do método TCP Half Open.

9.84. Permitir teste de disponibilidade de servidor *web* através do método TCP SSL.

9.85. Permitir teste de disponibilidade de servidor *web* através do método HTTP.

9.86. Permitir teste de disponibilidade de servidor *web* através do método HTTPS.

9.87. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada.

9.88. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST.

9.89. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado.

9.90. Suportar roteamento das requisições dos clientes *web* baseado em conteúdo HTTP, através de "Host".

9.91. Suportar roteamento das requisições dos clientes *web* baseado em conteúdo HTTP, através de "URL".

9.92. Suportar roteamento das requisições dos clientes *web* baseado "Parâmetro HTTP".

9.93. Suportar roteamento das requisições dos clientes *web* baseado "Referer".

9.94. Suportar roteamento das requisições dos clientes *web* baseado "Endereço IP de Origem".

9.95. Suportar roteamento das requisições dos clientes *web* baseado "Cabeçalho".

9.96. Suportar roteamento das requisições dos clientes *web* baseado "Cookie".

9.97. Suportar roteamento das requisições dos clientes *web* baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509".

9.98. Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.

9.99. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem.

9.100. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP.

9.101. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.

9.102. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite.

9.103. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica).

9.104. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie.

9.105. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente.

9.106. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID.

9.107. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID.

9.108. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID.

9.109. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.

#### 10. Solução de filtro de mensagens indesejadas - ANTISPAM

10.1. Todos os tráfegos de rede, com destino ou origem relacionados aos servidores de *e-mails* dos CONTRATANTES aderentes, devem ser redirecionados para a solução de *AntiSpam* da Nova Rede Corporativa e reencaminhados para o destino, depois de realizado todos os tratamentos relacionados com a solução, conforme especificado neste Termo de Referência;

10.2. A solução deve suportar os seguintes requisitos mínimos de desempenho:

10.2.1. Capacidade de tratamento de mensagens por hora, com Antivírus e *AntiSpam*: 02 (dois) Milhões;

10.2.2. Suporte a, no mínimo, 200 (duzentos) domínios de e-mail, podendo ser contratado para qualquer domínio dos órgãos;

10.3. Solução de Armazenamento de no mínimo: 18 TeraBytes, em solução local, em nuvem ou outra solução armazenamento, sem perda de performance do serviço;

10.4. Quando equipamento físico, o mesmo deve ser fornecido com a quantidade de interfaces SFP ou Ethernet, de no mínimo 1Gbps, necessárias para implementação da solução na Nova Rede: 04 (Quatro)

10.5. Quando equipamento físico, o mesmo deve ser fornecido com a quantidade de quantidade de interfaces SFP ou Ethernet, de no mínimo 10Gbps, necessárias para implementação da solução na Nova Rede: 02 (Duas)

10.6. Solução de filtro de mensagens indesejadas - ANTISPAM, deve ser fornecida e mantida integralmente nas dependências da CONTRATADA, por meio de um *appliance*, que poderá ser implementado em formato virtual, físico ou baseado em Nuvem. A responsabilidade pela operação, atualização e manutenção ficará exclusivamente a cargo da CONTRATADA;

10.7. Qualquer solução implementada pela CONTRATADA dentre as diversas opções sugeridas, deve ser disponibilizada em alta disponibilidade, garantindo a continuidade dos serviços sem interrupções;

10.8. Fornecer uma solução completa, com as funções *Antispam*, Antivírus, *Anti-Spyware* e *Anti-Phishing*;

10.9. Realizar inspeção do tráfego entrante e saiente de *e-mail* da Internet;

- 10.10. Conectar-se em tempo real em uma base de dados centralizada do fabricante para baixar atualizações de *AntiSpam*;
- 10.11. Possuir proteção contra ataques de negação de serviço do tipo Mail Bomb;
- 10.12. Possuir controles de DNS Reverso para garantir proteção Anti-Spoofing;
- 10.13. Possuir controle de limite da taxa de *e-mails* enviados;
- 10.14. Suportar múltiplos domínios de *e-mail*;
- 10.15. Suportar aplicação de políticas de *e-mail* por destinatário, por domínio, por tráfego de entrada ou de saída;
- 10.16. Permitir a criação de perfis de configuração granulares, onde cada perfil agrega definições específicas de funcionalidades como *Anti-Spam*, *Anti-Vírus*, Autenticação, entre outras;
- 10.17. Operar como *gateway* de correio SMTP para servidores de correio existentes;
- 10.18. Encaminhar *e-mail* baseado em LDAP;
- 10.19. Realizar quarentena de *e-mail* e ser possível acessá-la via *Web Mail*, POP3 e/ou IMAP;
- 10.20. A solução deve ter uma API baseada em REST disponível para fins de monitoramento, automação e orquestração;
- 10.21. Enviar relatórios de quarentena aos usuários de *e-mail*, de forma agendada;
- 10.22. A solução deve suportar quarentena por usuário, com acesso via interface web ou protocolo equivalente, permitindo o gerenciamento individual de mensagens retidas;
- 10.23. Realizar arquivamento (archiving) baseado em políticas de mensagens recebidas e enviadas, com suporte à armazenamento remoto;
- 10.24. Suportar gerenciamento de fila de *e-mail* para mensagens com falhas, atrasadas e não entregues;
- 10.25. Realizar autenticação SMTP via LDAP, RADIUS, POP3 ou IMAP.
- 10.26. Manter uma lista de reputação de remetentes locais com base em: número de vírus enviados, a quantidade de *spam*, número errado de destinatários;
- 10.27. A solução deve suportar Sender Policy Framework (SPF);
- 10.28. A solução deve suportar Domain Keys Identified Mail (DKIM);
- 10.29. A solução deve suportar Domain Based Message Authentication (DMARC);
- 10.30. Filtrar anexos e conteúdo das mensagens de *e-mail*;
- 10.31. Realizar inspeção profunda de cabeçalhos de *e-mail*;
- 10.32. Realizar filtragem estatística bayesiana;
- 10.33. Utilizar listas de bloqueio em tempo real usando URLs e/ou URIs de *Spam*;
- 10.34. A solução deve ser capaz de filtrar *e-mails* baseados na URIs (Uniform Resource Identifier) contidos no corpo da mensagem;
- 10.35. A solução pode detectar se um *e-mail* é *spam*, verificando os URLs que contém, comparando-os com o banco de dados de reputação fornecido pelo fabricante;
- 10.36. A revisão de URLs deve permitir selecionar as categorias de URL que serão permitidas ou não, nos *e-mails* analisados. Este banco de dados de categorias será atualizado pelo fabricante;
- 10.37. Realizar filtragem por palavra proibida (Banned Word);
- 10.38. Realiza a administração de *SPAM* com capacidade de Aceitar, Reenviar (Relay), Rejeitar (Reject) ou descartar (Discard);

- 10.39. Realizar análise de imagem e “escaneamento” de PDF para detectar *Spam*;
- 10.40. A solução permite identificar imagens que fazem referência ao conteúdo *SPAM*. Ele deve suportar a análise das seguintes extensões GIF, JPEG, PNG;
- 10.41. A solução deve ter uma base de informações de *malware* fornecida pelo fabricante e terceiros aliados, que podem ser atualizados de forma recorrente;
- 10.42. Suportar lista negra (Black List) de terceiros;
- 10.43. Suportar endereçamento IPv4 e IPv6;
- 10.44. Suportar Greylisting para IPV4, IPV6 e contas de *e-mail*;
- 10.45. Suportar detecção de IPs falsificados (Forged IP);
- 10.46. Suportar usuários IPs permitidos ou negados (White/Black List) em nível global por equipamento, e personalizado por usuário;
- 10.47. Suportar o “escaneamento” de antivírus/anti*Spyware* de arquivos compactados: ZIP, PKZIP, LHA, ARJ, RAR;
- 10.48. Permitir a substituição e edição de mensagens de notificação de Antivírus/Anti*Spyware*;
- 10.49. Realizar bloqueio por tipo de arquivo;
- 10.50. Suportar modo de operação *Gateway*, atuando como MTA (Mail Transfer Agent) ou *Gateway* de *e-mail*, encaminhando *e-mail* de/para servidores de *e-mail* protegidos;
- 10.51. Suportar modo de operação Transparente, realizando proxy ou encaminhamento (relay) transparente de/para os servidores de *e-mail* protegidos;
- 10.52. Possuir armazenamento local ou remoto de *e-mails*;
- 10.53. Possuir *interface* de configuração via *Web* (HTTP, HTTPS);
- 10.54. Suportar a configuração de administradores do sistema por domínio, sendo possível restringir o acesso por endereço IP e máscara de rede de origem;
- 10.55. Suportar, no mínimo, dois níveis de administração: Leitura/Gravação (Read/Write) e somente leitura (ReadOnly);
- 10.56. Suportar a geração e armazenamento de mensagens de log locais ou servidores remotos *Syslog*;
- 10.57. Gerar relatórios de atividade analisando os arquivos de log, apresentando-os em formato tabular e gráfico;
- 10.58. Suportar a geração de relatórios sob demanda, ou agendados em intervalos específicos;
- 10.59. Os relatórios podem ser gerados e enviados em formato PDF ou HTML;
- 10.60. Suportar o monitoramento de estado de enlace em modo de Alta Disponibilidade;
- 10.61. Suportar sincronização de quarentena e fila de *e-mail* em modo de Alta Disponibilidade;
- 10.62. Não permitir a perda de dados de *e-mails* em caso de *Failover*, ou alterações de configuração, em modo de Alta Disponibilidade ativo/passivo;
- 10.63. Suportar a detecção e notificação de falhas do dispositivo em modo de Alta Disponibilidade;
- 10.64. Suportar a detecção de Newsletter;
- 10.65. Para o módulo AntiPhishing, esta funcionalidade deverá ser provida em tempo real, em conjunto com outras soluções deste termo, tais como NGFW ou *Sandboxing*;
- 10.66. Ainda sobre o tema da funcionalidade anti-*phishing* é requerido a capacidade de inspecionar links em QR-Codes nas mensagens de *e-mail*;

- 10.67. A solução deve inspecionar o *e-mail* em procura de links maliciosos e se o link é malicioso, deverá remover ou reescrever somente o link e entregar a mensagem para o destinatário;
- 10.68. A solução deve ter a capacidade de avaliar, reter e bloquear em tempo real *e-mails* e anexos que possuam ameaças avançadas, dia zero, através da análise com *sandboxing*;
- 10.69. Deve suportar criptografia de *e-mail* usando S / MIME;
- 10.70. Suportar criptografia SMTPS e SMTP over TLS;
- 10.71. A solução deve analisar o conteúdo e anexos de uma mensagem em busca de palavras que indicam que o *e-mail* deve ser em quarentena, criptografado, arquivado, bloqueado, marcado, substituído ou encaminhado para outro host;
- 10.72. Deve possuir dicionários predefinidos para identificação de dados sensíveis, bem como permitir a criação de dicionários personalizados.
- 10.73. Deve inspecionar arquivos protegidos por senha, usando senhas predefinidas, uma lista de senhas ou pesquisar a palavra password no corpo;
- 10.74. A solução deverá integrar-se com a solução de NDR deste termo, a fim de aumentar a taxa de detecção e diminuir o tempo de análise das mensagens e/ou anexos. Caso a solução não possua solução de NDR, deverá entregar a mensagem e/ou anexos a um NDR de terceiros através, de API ou roteamento da mensagem, e após análise da ferramenta de NDR, deverá retornar o veredito ao administrador para tomada de ação;
- 10.75. A solução deverá possuir suporte a modo API, sem a necessidade de alteração de registro MX, para que possa se conectar em servidores de *e-mail* em nuvem, como Office 365 e Google Workspace, para analisar mensagens suspeitas após a entrega da mensagem, mesmo que esta já tenha sido lida pelo usuário;
- 10.76. A solução deve ser integrar com a solução de SOAR deste termo, com conector ou plugin específico para a solução de Anti-Spam;
- 10.77. Suportar no mínimo as seguintes RFC's (Request for Comments):
- 10.77.1. RFC 1918 (Address Allocation for Private Internets);
  - 10.77.2. RFC 1985 (SMTP Service Extension for Remote Message Queue Starting);
  - 10.77.3. RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes);
  - 10.77.4. RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies);
  - 10.77.5. RFC 2505 (Anti-Spam Recommendations for SMTP MTAs);
  - 10.77.6. RFC 2634 (Enhanced Security Services for S/MIME);
  - 10.77.7. RFC 2920 (SMTP Service Extension for Command Pipelining);
  - 10.77.8. RFC 3207 (SMTP Service Extension for Secure SMTP over TLS);
  - 10.77.9. RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs);
  - 10.77.10. RFC 3463 (Enhanced Mail System Status Codes);
  - 10.77.11. RFC 3464 (Extensible Message Format for Delivery Status Notifications);
  - 10.77.12. RFC 4954 (SMTP Service Extension for Authentication);
  - 10.77.13. RFC 5321 (SMTP);
  - 10.77.14. RFC 5322 (Internet MessageFormat);
  - 10.77.15. RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures);
  - 10.77.16. RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages);

- 10.77.17. RFC 6409 (MessageSubmission);
- 10.77.18. RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-mail);
- 10.77.19. RFC 2088 (IMAP4 Non-synchronizing Literals);
- 10.77.20. RFC 2177 (IMAP4 IdleCommand);
- 10.77.21. RFC 2221 (LoginReferrals);
- 10.77.22. RFC 2342 (IMAP4 Namespace);
- 10.77.23. RFC 2683 (IMAP4 ImplementationRecommendations);
- 10.77.24. RFC 2971 (IMAP4 ID Extension);
- 10.77.25. RFC 3348 (IMAP4 Child Mailbox Extension);
- 10.77.26. RFC 3501 (IMAP4 rev1);
- 10.77.27. RFC 3502 (IMAP MultiappendExtension);
- 10.77.28. RFC 3516 (IMAP4 Binary Content Extension);
- 10.77.29. RFC 5032 (WITHIN SearchExtension);
- 10.77.30. RFC 5255 (IMAP Internationalization);
- 10.77.31. RFC 5256 (Sort and Thread Extensions);
- 10.77.32. RFC 5258 (ListCommandExtensions);
- 10.77.33. RFC 5267 (Contexts for IMAP4);
- 10.77.34. RFC 5819 (Extension for Returning STATUS Information in Extended LIST);
- 10.77.35. RFC 6154 (LIST Extension for Special-Use Mailboxes);
- 10.77.36. RFC 6851 (MOVE extension);
- 10.77.37. RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC));
- 10.77.38. RFC 1939 (POP3);
- 10.77.39. RFC 2449 (POP3 ExtensionMechanism);
- 10.77.40. RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface);
- 10.77.41. RFC 1157 (SNMP v1);
- 10.77.42. RFC 2595 (Using TLS with IMAP, POP3 and ACAP);
- 10.77.43. RFC 3410 (SNMP v3);
- 10.77.44. RFC 3416 (SNMP v2).

## ADENDO VII - SERVIÇOS DE CONECTIVIDADE PARA DATACENTER

### 1. Objetivo

1.1. Este adendo tem como objetivo definir os requisitos e condições para a contratação de serviços de conectividade através de links de dados específicos para datacenters dentro da Nova Rede Corporativa. Estes serviços objetivam aprimorar a infraestrutura de tecnologia da informação do Governo do Estado de Pernambuco, buscando estabelecer as diretrizes e especificações técnicas para a seleção de fornecedores qualificados. Dessa forma, espera-se garantir

que os serviços contratados atendam aos padrões de qualidade e eficácia esperados, em conformidade com as legislações vigentes.

1.2. Este adendo descreve os seguintes itens de serviço:

1.2.1. Link de Fibra Lan-2-Lan (L2L):

1.2.2. Link de Internet Trânsito para Datacenter com Anti-DDoS (LIT);

1.3. O prazo contratual para os serviços descritos neste ADENDO VII será de 48 (quarenta e oito) meses, observado o disposto no quadro constante do item “1. DO OBJETO DA LICITAÇÃO” deste Termo de Referência. Cada item de serviço possui estimativa de previsão de uso específica, 12 (doze) ou 6 (seis) meses, conforme indicado na coluna “Previsão de Uso em Meses” da tabela, de modo que a soma desses períodos de utilização compõe o prazo global de 48 (quarenta e oito) meses.

## 2. Definições

2.1. Link de Fibra Lan-2-Lan (L2L): este serviço objetiva estabelecer comunicação entre dois datacenters do estado através de fibra óptica;

2.2. Link de Internet Trânsito para Datacenter com Anti-DDoS (LIT): Este serviço tem como objetivo prover conectividade dos datacenters do Estado com a Internet, por meio da utilização de blocos de endereços IP pertencentes ao Sistema Autônomo nº 10938 (ATI). Os blocos de IP a serem utilizados nos Datacenters serão disponibilizados pelo CIISC, CONTRATADA através do Lote 01, e deverão ser configurados para o serviço de LIT com capacidade de mitigação de ataques de negação de serviço distribuídos (Anti-DDoS), assegurando resiliência contra ataques volumétricos que possam comprometer a disponibilidade dos serviços públicos hospedados.

2.2.1. Capacidades de Banda do Serviço LIT

2.2.1.1. Para fins de contratação e dimensionamento dos serviços de Link de Internet Trânsito para Datacenter com Anti-DDoS (LIT), ficam estabelecidas as seguintes faixas de capacidade de banda a serem disponibilizadas no âmbito deste Termo de Referência:

- |                                                         |      |      |            |    |   |      |     |           |        |
|---------------------------------------------------------|------|------|------------|----|---|------|-----|-----------|--------|
| a)                                                      | Link | para | Datacenter | de | 2 | Gbps | com | Anti-DDoS | (LIT); |
| b)                                                      | Link | para | Datacenter | de | 4 | Gbps | com | Anti-DDoS | (LIT); |
| c)                                                      | Link | para | Datacenter | de | 6 | Gbps | com | Anti-DDoS | (LIT); |
| d)                                                      | Link | para | Datacenter | de | 8 | Gbps | com | Anti-DDoS | (LIT); |
| e) Link para Datacenter de 10 Gbps com Anti-DDoS (LIT). |      |      |            |    |   |      |     |           |        |

2.2.1.2. As capacidades de banda descritas neste item representam as unidades de contratação do serviço LIT, devendo a CONTRATADA garantir o pleno atendimento aos requisitos técnicos, de desempenho, disponibilidade e segurança estabelecidos neste Adendo, independentemente da capacidade contratada.

2.2.1.3. A definição da capacidade de banda a ser efetivamente utilizada em cada Datacenter será realizada por meio da emissão de Ordem de Serviço (OS), observadas as necessidades operacionais da CONTRATANTE, bem como a disponibilidade orçamentária.

2.2.1.4. A solução ofertada pela CONTRATADA deverá ser dimensionada de forma a permitir a evolução de capacidade de banda de maneira escalável, preferencialmente sem necessidade de substituição integral da infraestrutura implantada e sem interrupção dos serviços.

2.2.1.5. Todas as capacidades de banda deverão ser entregues de forma simétrica (full-duplex), garantindo throughput efetivo compatível com a capacidade nominal contratada, sem aplicação de qualquer tipo de limitação, modelagem ou bloqueio de tráfego não previsto neste Termo de Referência.

## 3. Localizações dos datacenters do estado

3.1. O estado de Pernambuco possui datacenters nas seguintes localidades, que devem ser consideradas para objeto de precificação e prestação dos serviços previstos neste adendo:

3.1.1. ATI-PE – Av. Rio Capibaribe, 147, Santo Antônio. Recife-PE. CEP 50020-080;

3.1.2. SEE-PE – Av. Afonso Olindense, 1513, Várzea. Recife-PE. CEP 50810-000;

3.1.3. SEFAZ-PE – Av. Dantas Barreto, 1186, São José (Edif. San Rafael) Recife-PE. CEP 50020-904;

#### **4. Requisitos gerais para a infraestrutura de entrada para os Datacenters:**

4.1. A CONTRATADA será integralmente responsável pela execução de todos os serviços, obras e adequações de infraestrutura necessárias à entrega, ativação e pleno funcionamento dos links de Internet corporativa LIT e L2L, tanto nas áreas externas quanto internas dos prédios da CONTRATANTE, conforme ilustrado na Figura 01 e detalhado nos itens subsequentes.

Perímetro interno do órgão

DIO Outdoor da operadora com 72 conexões

Tubulação subterrânea com cabo ótico de 72 fibras ativo

Tubulação subterrânea com cabo ótico de 72 fibras backup

DATA CENTER

SALA SEGURA

SALA COFRE

RACK DE AGREGAÇÃO 1

RACK DE DISTRIBUIÇÃO 1

Cabo de 72 fibras A backup

Cabo de 72 fibras A ativo

Cabo de 72 fibras B ativo

Cabo de 72 fibras B backup

RACK DE AGREGAÇÃO 2

RACK DE DISTRIBUIÇÃO 2

DATA CENTER ATI

Tubulação subterrânea com cabo ótico de 72 fibras ativo

Tubulação subterrânea com cabo ótico de 72 fibras backup

DIO Outdoor da operadora com 72 conexões

Infraestrutura e cabos (responsabilidade da proponente LOTE 02)

Infraestrutura e cabos (responsabilidade da proponente LOTE 02)

Infraestrutura e cabos (responsabilidade da proponente LOTE 02)

Infraestrutura e cabos (responsabilidade da proponente LOTE 01)

Rack indoor e DIOs (responsabilidade da proponente LOTE 02)

Rack Outdoor e DIOs (responsabilidade da proponente LOTE 02)

Switch de Agregação (responsabilidade da proponente LOTE 01)

Firewall de Agregação (responsabilidade da proponente LOTE 01)

**Figura 01 - Topologia da infraestrutura interna dos Datacenters**

4.2. A CONTRATADA deverá realizar a instalação completa da infraestrutura de fibra óptica, desde o ponto de entrada do prédio da CONTRATANTE até a respectiva sala cofre dos Datacenters, assegurando caminhos físicos distintos e redundância para garantir alta disponibilidade. Todos os materiais, mão de obra e eventuais adaptações ou modificações no ambiente físico da CONTRATANTE, que sejam indispensáveis à prestação dos serviços contratados, serão de inteira responsabilidade da CONTRATADA. Ao final da implantação, todas as instalações da CONTRATANTE deverão permanecer em perfeito estado, sendo vedada qualquer alteração permanente sem prévia autorização formal da CONTRATANTE. A instalação inclui:

4.2.1. **Infraestrutura externa:** Instalação da infraestrutura de entrada, incluindo eletrodutos para a passagem dos cabos ópticos e, se necessário, o poste localizado em frente ao prédio da CONTRATANTE, além da instalação e configuração do DIO outdoor de entrada;

4.2.2. **Infraestrutura interna:** Instalação completa da infraestrutura interna, incluindo eletrodutos com contingência para a passagem dos cabos ópticos desde o DIO outdoor de entrada até os DIOS localizados no rack de distribuição na sala segura e o DIO da sala Cofre.

4.2.2.1. A infraestrutura de eletrodutos deverá ser composta por um duto com cabo de 72 fibras ópticas ativas e conectorizadas, e outro duto com cabo backup de 72 fibras ópticas igualmente conectorizadas.

4.2.3. **Espelhamento de DIOS:** Espelhamento dos DIOS da sala segura para os DIOS da sala cofre de cada Datacenters, garantindo a redundância e a disponibilidade da conexão.

4.2.4. A CONTRATADA será responsável pela manutenção integral de toda a infraestrutura de fibra óptica implantada, incluindo a totalidade das fibras ópticas ativas e de backup, estejam ou não em uso, bem como dos DIOS e eletrodutos correspondentes, garantindo o funcionamento pleno e a integridade física e lógica da solução ao longo de toda a vigência contratual.

4.2.4.1. A manutenção da infraestrutura deverá observar rigorosamente os Níveis Mínimos de Serviço (NMS) estabelecidos no Termo de Referência, incluindo prazos para correção de falhas, padrões de disponibilidade e exigências de desempenho, sendo de responsabilidade da CONTRATADA realizar, sem ônus adicional à CONTRATANTE, todas as correções, substituições e reparos necessários para preservar a operação contínua e segura da rede.

4.3. Cada abordagem deverá incluir 72 fibras ópticas devidamente conectorizadas, interligando os DIOS externos ao DIO localizado no rack de distribuição dentro da Sala Segura. Além disso, caso necessário, essas fibras deverão realizar o espelhamento entre os DIOS da Sala Segura e os DIOS da Sala Cofre em cada um dos Datacenters. Todos os DIOS envolvidos no serviço, incluindo o DIO outdoor, o DIO da Sala Segura e os DIOS da Sala Cofre, dos Datacenters serão de total responsabilidade da CONTRATADA;

4.4. Para cada datacenter será realizada uma avaliação conjunta com os Gestores responsáveis por cada Datacenter, conforme previsto no escopo do projeto. Essa abordagem garantirá que as necessidades específicas de cada ambiente sejam devidamente consideradas, alinhando a implementação às expectativas e aos requisitos técnicos de cada Datacenter;

4.5. A CONTRATADA também realizará as fusões das fibras ópticas nas extensões ópticas conectorizadas e suas devidas certificações através de um OTDR (reflectômetro óptico no domínio do tempo) sendo o resultado da certificação das fusões entregue ao CONTRATANTE.

4.6. As fibras ópticas que forem utilizadas nas dependências do CONTRATANTE deverão ser apropriadas para uso interno, ou seja, não suscetíveis a propagação de fogo (antichama).

4.7. Para interligação com os equipamentos da CONTRATANTE, a CONTRATADA deve disponibilizar os patch cords entre o DIO do Rack de distribuição e os equipamentos indicados pela CONTRATANTE para os serviços deste Adendo (LIT e L2L).

4.7.1 A responsabilidade da CONTRATADA do Lote 02 fica restrita ao meio físico do L2L. Além da rede Fibra óptica (externa e interna), os line cords/patch cords e conectores são de responsabilidade do Lote 02, de forma a garantir o padrão 100 Gigabit Ethernet.

4.7.2. A CONTRATADA do Lote 01 será a responsável pelos ativos/equipamentos e transceiver/Gbic que proverão o throughput de 100 Gbps no L2L.

4.8. Para qualquer link contratado/disponibilizado pela CONTRATANTE, a CONTRATADA deve utilizar a infraestrutura de entrada para os Datacenters, deve providenciar toda interligação com os equipamentos da CONTRATANTE e disponibilizar os patch cords entre o DIO do Rack de distribuição e os equipamentos indicados pela CONTRATANTE.

4.9. A CONTRATANTE deverá fornecer as condições ambientais de umidade, poeira e refrigeração adequados, pontos de energia redundante, espaço físico, bem como a segurança física de acesso ao ambiente.

4.10. A CONTRATADA deverá realizar a visita técnica em todas as localidades dos Datacenters especificados neste Adendo, para elaboração do Projeto de atendimentos dos itens de infraestrutura de entrada dos prédios.

4.11. O projeto deve ser avaliado e aprovado pelos responsáveis técnicos da ATI e do Órgão de cada *Datacenters*, devendo a CONTRATADA realizar todo e qualquer ajuste necessário do Projeto apresentado.

4.12. A CONTRATADA deverá seguir todas as normas técnicas e de segurança aplicáveis na execução dos serviços, garantindo a qualidade e a segurança da instalação;

4.13. Ao término do contrato, toda a infraestrutura física implantada a partir dos pontos de distribuição óptica (DIO OUTDOOR) das entradas 01 e 02 até as dependências internas do Ponto Conectado Seguro (PCS) da CONTRATANTE, incluindo cabeamento, conectores, suportes, dutos, dispositivos de terminação e demais elementos associados, passará a ser de propriedade da CONTRATANTE, sem ônus adicional.

4.14. Ao término do contrato, para fins de incorporação ao patrimônio do Estado, considera-se exclusivamente a infraestrutura do item 4.2 e subitens conforme figura 01.

4.15. Ao término do contrato, a infraestrutura óptica da rede externa em via pública, postes, caixas de emenda subterrâneas ou aéreas, permanecerá de propriedade exclusiva da CONTRATADA do LOTE 2, sob sua integral responsabilidade regulatória, técnica e operacional.

## 5. Topologia para provimento dos Serviços LIT e L2L:

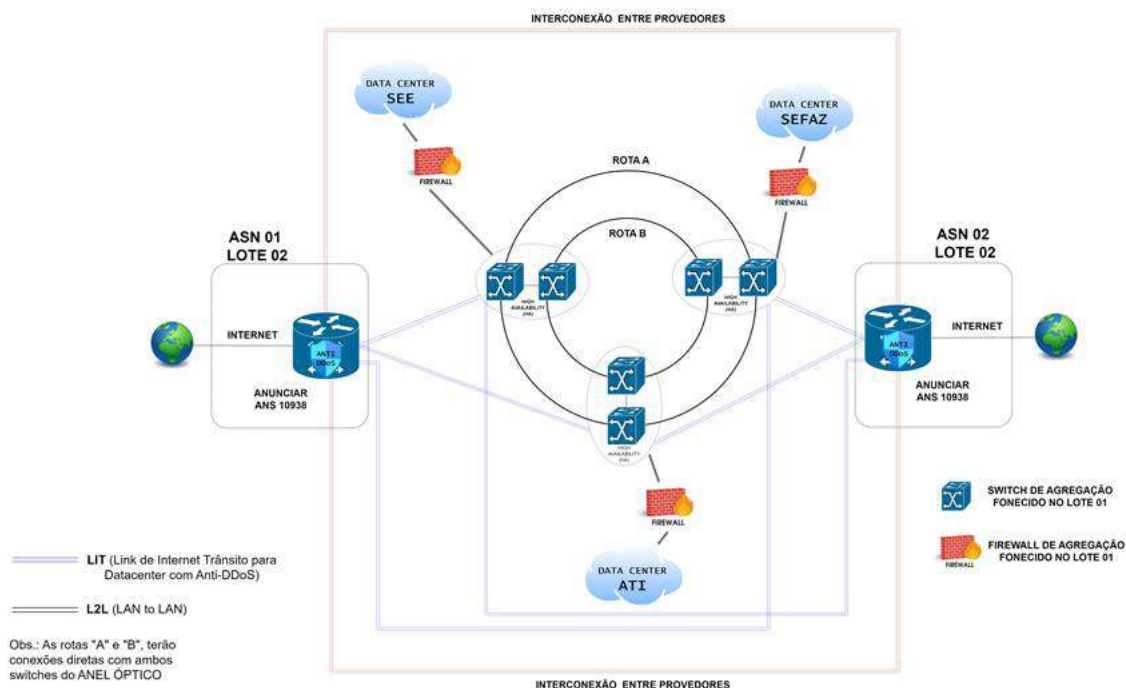


Figura 02 - Topologia LIT e L2L

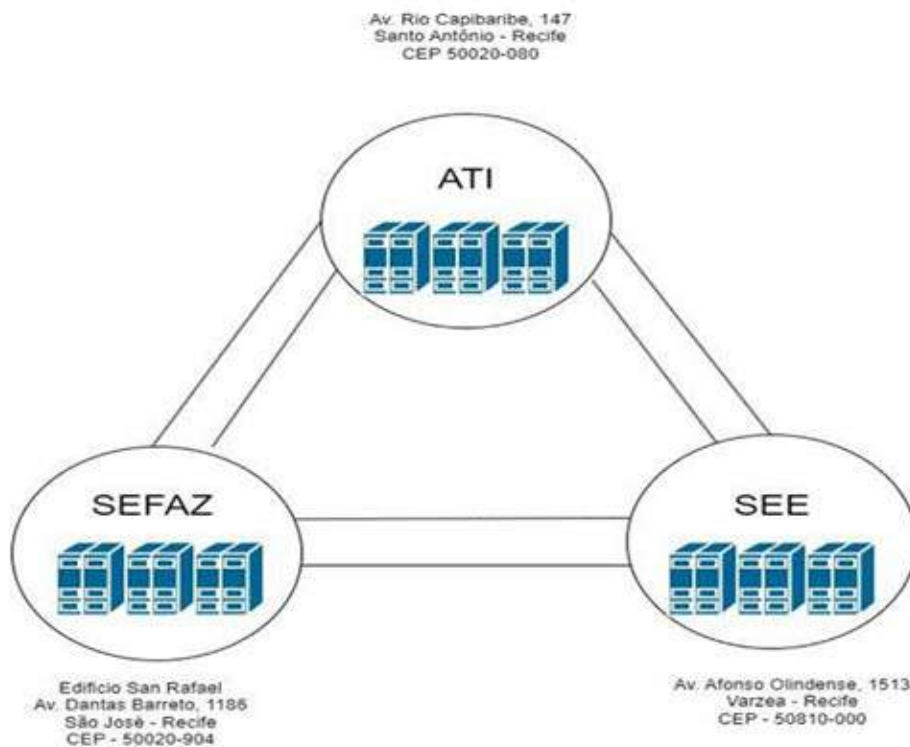


Figura 03 - Topologia do Link de Fibra Lan-2-Lan (L2L)

### 5.1 Requisitos para o Link de Fibra Lan-2-Lan (L2L):

5.1.1. Este serviço é composto por dois Links bidirecionais de fibra óptica apagada, sendo 1 (um) par de fibras por link para conexão em topologia de anel óptico entre os *Datacenters* especificados neste Adendo, conforme Figura 02 Rota A e Rota B.

5.1.2. Este serviço não deve possuir ativos (equipamentos de conectividade) entre os *Datacenters*.

5.1.3. Os equipamentos de conectividade do link de fibra L2L serão fornecidos pela contratada do Lote 1 deste Termo de Referência;

5.1.4. A CONTRATADA será responsável por toda a manutenção física da fibra óptica.

5.1.4.1. A CONTRATADA poderá realizar o monitoramento do enlace através de senhas de leitura/comunidade disponibilizado pelo CIISC do Lote 1. Dado que a iluminação da fibra (L2L) e os ativos de borda são de responsabilidade do LOTE 1, fica assegurado à CONTRATADA do LOTE 2 o acesso sistêmico contínuo (em tempo real) à telemetria das interfaces ópticas (ex: leitura de potência TX/RX via SNMP ou painel de monitoramento do LOTE 1) dos equipamentos conectados às suas fibras, única e exclusivamente para fins de monitoramento da atenuação, integridade do meio físico e aferição de NMS.

5.1.4.2. Toda a Interação com relação a abertura de chamados, manutenção programada e registro de ocorrências, deve ser realizada através do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), para ter um único ponto de Gestão de Demandas e Registro de Ocorrências;

5.1.5. Os acessos aos prédios dos *Datacenters* deverão ser entregues em rotas e abordagens distintas entre si. Desta forma, a CONTRATADA deverá garantir rotas distintas (internas e externas) a serem percorridas por cada um de seus acessos. Isso evitará que uma eventual falha na rede de um acesso impacte simultaneamente o outro serviço, garantindo a inexistência de pontos comuns de falha. Assim, a continuidade operacional dos serviços em todos os *Datacenters* será preservada.

5.1.6. A solução de L2L deve garantir redundância por meio de Anel (Rota A e Rota B), podendo ser entregue por um único fornecedor ou por meio de arranjos de parceria, consórcio ou subcontratação tecnicamente integrada, desde que a CONTRATADA assuma a responsabilidade integral pela entrega do serviço.

5.1.7. A CONTRATADA deve prover uma rede de fibra óptica que permita comunicação de dados do link L2L no padrão de 100 Gigabit Ethernet permitindo o transporte dos protocolos superiores ao nível 2 de forma transparente.

5.1.8. A CONTRATADA deve garantir transparência ao protocolo de agregação de enlaces por meio do protocolo LACP (Link Aggregation Control Protocol), conforme o padrão IEEE 802.3ad, e o uso de VLANs configuradas pela CONTRATANTE, seguindo o padrão IEEE 802.1q, sem qualquer interferência no transporte.

5.1.9. A CONTRATADA deve garantir transparência ao roteamento **ECMP (Equal Cost Multipath)**, no provisionamento do serviço.

5.1.10. Os circuitos L2L deverão garantir transporte transparente em camada 1 (físico), garantindo a passagem de qualquer protocolo de rede sem interferência ou degradação de performance, incluindo, mas não limitado a, IP, MPLS e Multicast.

5.1.11. A CONTRATADA deve garantir transparência aos protocolos de prevenção de loop em redes Spanning Tree Protocol (IEEE 802.1d), Rapid Spanning Tree Protocol (IEEE 802.1w) e Multiple Spanning Tree Protocol (IEEE 802.1s), no provisionamento do serviço;

5.1.12. A CONTRATADA deve garantir transparência quanto ao uso de VLANs (padrão IEEE 802.1q), definidas pela CONTRATANTE, no provisionamento do serviço;

5.1.13. A CONTRATADA deve garantir suporte a jumbo frames de 9.000 bytes, no provisionamento do serviço, assegurando que o transporte de frames maiores ocorra de forma transparente e sem fragmentação, caso necessário para o pleno funcionamento da infraestrutura do CONTRATANTE.

5.1.14. A Taxa de Erro de Bit (BER) para circuitos dedicados deverá ser melhor ou igual a  $10^{-9}$ , medida na taxa de transmissão máxima de cada circuito, durante um período de 24 horas.

5.1.15. A taxa de perda de pacotes (Frame Loss) medida através do teste RFC 2544 deverá ser menor ou igual do que 0,1%, medida na taxa de transmissão máxima do circuito.

5.1.16. O retardo dos circuitos deverá ser de, no máximo, 1 (um) milissegundos em um único sentido (RTT 2ms) e será medido através do protocolo ICMP (Internet Control Message Protocol) da pilha de protocolos TCP (Transmission Control Protocol) e IP (Internet Protocol).

5.1.17. A CONTRATADA deve implementar controles de segurança no transporte óptico, assegurando proteção contra interceptações não autorizadas ou espionagem óptica.

## 5.2. Requisitos para o Link de Internet Trânsito para Datacenter com Anti-DDoS (LIT):

5.2.1. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar e manter os equipamentos e recursos que forem necessários (roteadores, switches meios de transmissão, cabeamento, licenças de softwares, licenças de órgãos reguladores, acessórios, rack, entre outros) para o provimento e perfeito funcionamento dos serviços;

5.2.2. Todos os equipamentos para a solução do LIT devem ser disponibilizados no ambiente da CONTRATADA.

5.2.3. Os equipamentos fornecidos na solução podem ser de propriedade da contratada ou serem adquiridos novos, desde que garantam o provimento e o perfeito funcionamento dos serviços conforme este Termo de Referência;

5.2.4. A CONTRATADA deve garantir o bom funcionamento de toda a infraestrutura para prestação do serviço, garantir que a solução proposta (Hardware, Software e outros) tenha o suporte técnico e manutenção adequados, trocando-os sempre que ocorrer obsolescência tecnológica, ou sempre que seja necessário para garantir o perfeito funcionamento dos serviços;

5.2.5. A CONTRATADA deve garantir que a instalação física e a configuração dos equipamentos e serviços implantados e disponibilizados poderão ser acompanhadas por técnicos da CONTRATANTE;

5.2.6. Toda a infraestrutura no ambiente da CONTRATADA deve funcionar em alta disponibilidade para garantir a continuidade do serviço da Solução LIT (roteadores, switches, energia e tudo que for necessário para a continuidade do serviço da Solução);

5.2.7. Serão contratados 2 (dois) serviços de LIT que devem ser entregues com as seguintes características:

5.2.7.1. Para o Link de Trânsito LIT 1, é obrigatório que o ASN esteja em nome da CONTRATADA ou de uma empresa pertencente ao seu grupo econômico;

5.2.7.2. Para o Link LIT 2, o ASN deve ser obrigatoriamente distinto do utilizado no Link LIT 1. Este serviço pode ser subcontratado ou consorciado, desde que a empresa ou grupo econômico envolvido seja diferente daqueles responsáveis pelo Link LIT 1. Em qualquer caso, a CONTRATADA deve comprovar sua qualificação técnica para atender tanto ao Link LIT 1 quanto ao Link LIT 2;

5.2.7.3. A CONTRATADA deve fornecer, garantir e implementar a infraestrutura necessária para assegurar que: o Link LIT 1 tenha 02 (duas) abordagens por caminhos fisicamente distintos; e o Link LIT 2 tenha 02 (duas) abordagens por caminhos fisicamente distintos, totalizando em cada Datacenter 04 (quatro) abordagens externas sempre por caminhos separados. A entrega dessas 4 abordagens externas deverá ser distribuída pelas infraestruturas de entrada fisicamente separadas do prédio (conforme Figura 01), garantindo que não exista nenhum ponto único de falha (físico ou lógico) no trajeto externo que possa indisponibilizar simultaneamente os serviços do LIT 1 e do LIT2. Essa configuração é essencial para garantir alta disponibilidade, redundância e resiliência na troca de tráfego entre os links;

5.2.7.3.1. A CONTRATADA deverá fornecer todos os serviços de LIT 1 nos endereços de cada Datacenter de forma independente do serviço L2L. Ou seja, o serviço de LIT 1 (ASN1) deve ser entregue diretamente em cada um dos Datacenters em dupla abordagem conforme descrito no item 5.2.7.3;

5.2.7.3.2. A CONTRATADA deverá fornecer todos os serviços de LIT 2 nos endereços de cada Datacenter de forma independente do serviço L2L. Ou seja, o serviço de LIT 2 (ASN2) deve ser entregue diretamente em cada um dos Datacenters em dupla abordagem conforme descrito no item 5.2.7.3.

5.2.7.4. A CONTRATADA deve prover e implementar toda a infraestrutura essencial nos Provedores do Link LIT 1 e do Link LIT 2 assegurando que ambos disponham, em seus Datacenters, dos recursos necessários (roteadores e switches) para a divulgação das tabelas BGP do ASN 10938 na Internet;

5.2.7.5. A solução deve garantir que o Link LIT 1 e o Link LIT 2 sejam responsáveis pelo roteamento e encaminhamento do tráfego destinado à rede da CONTRATANTE, vinculada ao ASN 10938;

5.2.7.6. A CONTRATADA deve assegurar que o tráfego seja encaminhado para a rede da CONTRATANTE sem a necessidade de implementação do protocolo BGP na infraestrutura local da CONTRATANTE;

5.2.7.7. A CONTRATADA deve garantir que todos os serviços disponíveis nos Datacenters mencionados no Termo de Referência neste ADENDO VII estejam plenamente acessíveis via Internet, atendendo aos requisitos de conectividade, desempenho e disponibilidade estabelecidos;

5.2.8. A CONTRATADA deverá fornecer ao CONTRATANTE as informações para acesso (usuário e senha), via porta de console ou SSH ou HTTPS, para acesso, com privilégios para ver configurações e estatísticas;

5.2.9. A CONTRATADA deve garantir, disponibilizar e implementar solução que permita o envio dos logs, via protocolo Syslog, para as plataformas indicadas pela CONTRATANTE, conforme o disposto no ADENDO VIII – Soluções de Segurança do Centro de Gerenciamento.

### 5.3. Requisitos para abordagens dos serviços do tipo LIT e L2L:

5.3.1. Para o provimento dos acessos dos serviços LIT e L2L, não pode haver pontos de rota em comum durante todo o percurso entre a origem e o destino.

5.3.2. As rotas também não poderão compartilhar estações/centrais/pontos de presença/edificações/postes ao longo do encaminhamento das fibras;

5.3.3. Os projetos de implantação dos acessos devem ser fornecidos para análise e aprovação da CONTRATANTE, com informações detalhadas em mapa (arruamento), do percurso a ser percorrido por cada acesso.

5.3.4. Os projetos de implantação mencionados acima deverão seguir a padronização técnica vigente.

5.3.5. A fim de garantir a continuidade dos serviços e minimizar o tempo de indisponibilidade, a CONTRATADA deverá implementar uma infraestrutura totalmente redundante nos endereços dos *Datacenters*, em alta disponibilidade e resiliente contra falhas, abrangendo todas as camadas da rede, desde o acesso (última milha totalmente independente), infraestrutura interna, equipamentos até a sala/cofre dos *Datacenters*, conforme a figura 01;

5.3.6. A CONTRATADA deverá apresentar o projeto à ATI, para que a área técnica responsável possa elaborar parecer técnico antes da implantação, com a topologia, indicação de rotas, material utilizado, encaminhamentos etc.

5.3.7. O projeto/ As Built deverá conter informações detalhadas sobre a infraestrutura de fibra óptica, incluindo no mínimo:

5.3.7.1. Traçado das rotas de fibra óptica (principal e redundante);

5.3.7.2. Localização dos cabos, dutos, caixas de emenda, caixas de distribuição e dispositivos ópticos.

5.3.7.3. Detalhes sobre os pontos de acesso, como distribuidores ópticos (DOs) e distribuidores gerais ópticos (DGOs);

5.3.7.4. Identificação dos elementos de redundância, como rotas alternativas e equipamentos de *backup*;

5.3.8. A área técnica da ATI responsável pela gerência da rede corporativa emitirá parecer técnico aprovando o projeto com base nos documentos apresentados e normativos que achar necessário;

5.3.9. O órgão responsável pelo *Datacenters* que terá o serviço contratado, precisará formalizar a anuência ao parecer técnico da ATI para que a CONTRATADA possa seguir com os procedimentos necessários de entrega do serviço;

5.3.10. O As Built deverá ser entregue imediatamente após a conclusão da implantação da rede para a CONTRATANTE;

5.3.11. O projeto deverá seguir a NBR 14565:2005 (ou norma mais atual), que estabelece requisitos técnicos para o compartilhamento de infraestruturas de redes de distribuição de energia elétrica com as redes de telecomunicações. Essa norma garante a qualidade, desempenho e segurança das redes de comunicação.

5.3.12. A CONTRATADA deverá apresentar contrato de utilização compartilhada de pontos de fixação de cabos de fibra óptica e recursos de telecomunicações em poste da concessionária do serviço público de distribuição de energia elétrica de Pernambuco. Caso contrário, a licitante deverá comprovar a existência de postes próprios, redes enterradas, ou ainda compartilhamento de infraestruturas com outras operadoras, como também as devidas autorizações das entidades para tal propriedade, nos municípios envolvidos no trajeto da rede.

5.3.13. As manutenções corretivas deverão ser realizadas a qualquer tempo e em quantas vezes se fizer necessário de acordo com a necessidade do CONTRATANTE.

5.3.14. Ocorrendo acidentes ou furtos que ocasionem o rompimento da fibra, a CONTRATADA deverá realizar a correção nos prazos estabelecidos no adendo referente aos Níveis Mínimos de Serviço (NMS).

5.3.15. O incidente só será concluído com restabelecimento dos serviços do link conforme especificado neste termo.

## 6. Requisitos gerais para a parte lógica dos serviços

6.1. A CONTRATADA deverá configurar todos os seus equipamentos fornecidos para suportar a interconexão com os *Datacenters* mencionados neste adendo;

6.2. A solução deverá permitir que sejam disponibilizadas para a CONTRATANTE acesso aos equipamentos fornecidos, inclusive no ambiente da CONTRATADA, para monitoramento e visualização de 100% das informações de configuração e operação.

6.3. Os aumentos de largura de banda, quando requeridos, deverão ser implementados de forma transparente, isto é, prever uma solução tecnológica para que permita realizar as atualizações requisitadas, de forma modular, suportadas pelos recursos e equipamentos envolvidos na solução, visando não comprometer a qualidade e não causar descontinuidade dos serviços contratados.

6.4. Para o serviço L2L, a CONTRATANTE se tiver necessidade de aumentar a banda do serviço de L2L, acionará a CONTRATADA para estudo de viabilidade e ajustes contratuais;

6.5. O LIT deve garantir, realizar, disponibilizar e implantar a conexão para todos os *Datacenters* designados pela CONTRATANTE à Internet por meio de tráfego de trânsito IP e de pontos de troca de tráfego (PTT), utilizando o protocolo BGP, com suporte a IPv4 e IPv6 para o ASN 10938;

6.6. A CONTRATADA deverá configurar os equipamentos com filtros apropriados para evitar o recebimento de rotas indesejadas de quaisquer serviços, garantindo a integridade e segurança do roteamento.

6.7. A CONTRATADA deve garantir, prover, implementar conexão em alta disponibilidade entre os ASN1 e ASN2 para a infraestrutura disponibilizada para a prestação da solução do LIT.

## 7. Requisitos Técnicos da CONTRATADA

7.1. A CONTRATADA deverá estar conectada em pelo menos 3 (três) PTTs (Pontos de Troca de Tráfego) Nacional assim detalhado:

7.1.1. 01 (um) Estadual na Cidade de Recife onde estão os *Datacenters* da CONTRATANTE;

7.1.2. 02 (dois) Nacionais localizados em São Paulo e Fortaleza;

7.2. A CONTRATADA deverá fornecer conectividade de trânsito IP para o Sistema Autônomo da ATI, garantindo que o ASN da ATI tenha acesso aos Pontos de Troca de Tráfego (PTTs) IX.br Recife, Fortaleza e São Paulo através do AS da CONTRATADA.

7.2.1. Caso a CONTRATADA não possua infraestrutura própria de conexões diretas e ativas nos PTTs IX.br Recife, Fortaleza e São Paulo, a CONTRATADA deverá utilizar-se de Acordos de Tráfego Multilateral ou acordos bilaterais suficientes para garantir conectividade ampla ao PTTs, atuando como provedor de trânsito para o ASN da ATI.

7.2.2 Para fins de homologação, a CONTRATADA deverá comprovar que:

- a) O ASN da ATI possui conectividade plena aos PTTs IX.br Recife, Fortaleza e São Paulo através do fornecimento de internet trânsito pelo ASN da CONTRATADA;
- b) O ASN da CONTRATADA anuncia as rotas do ASN da ATI nos PTTs especificados tanto em IPv4 quanto IPv6, garantindo que o tráfego destinado ao ASN da ATI transite obrigatoriamente pelo ASN da CONTRATADA;
- c) O tráfego bidirecional (inbound e outbound) entre o ASN da ATI e os demais sistemas autônomos presentes nos PTTs flui exclusivamente através do ASN da CONTRATADA;
- d) Existe tráfego mensurável confirmado através de monitoramento em tempo real ou relatórios técnicos;
- e) Show bgp summary demonstrando o peering entre ASN da ATI e ASN da CONTRATADA;
- f) Tabelas de roteamento dos PTTs mostrando o ASN da CONTRATADA como único next-hop para alcançar o ASN da ATI;
- g) Estatísticas dos PTTs IX.br mostrando o ASN da ATI como downstream do ASN da CONTRATADA;
- h) Tracerouters bidirecionais demonstrando que o tráfego de/para o ASN da ATI passa pelo ASN da CONTRATADA;
- i) Testes de conectividade de diferentes ASNs nos PTTs confirmando que o ASN da ATI é alcançado via ASN da CONTRATADA;
- j) Relatórios de tráfego fim-a-fim confirmando a conectividade bidirecional.

7.3. A CONTRATADA deverá comprovar, na etapa de instalação/ homologação do serviço, que está conectado a pelo menos 01 (um) ASN Internacional, ou que possui contratos de trânsito IP com pelo menos duas empresas que estejam conectadas a algum ASN Internacional. Entenda-se por ASN Internacional aquele que se acha fora dos limites do território brasileiro. A comprovação de que a empresa está conectada a uma fornecedora Internacional será feita através das ferramentas públicas, como bgp.he.net ou outra similar.

7.4. A CONTRATADA deverá apresentar um documento impresso com as informações que constam no site <http://bgp.he.net/> - dentre elas: os números dos ASNs utilizados para o LIT 1 e LIT 2, os peers IPv4 e IPv6 e os pontos de interconexão IX (Internet eXchange) em que estão conectados.

7.5. O somatório das larguras de banda do backbone da LICITANTE considerando conexões com Pontos de Troca de Tráfego e trânsito IP, deve resultar em um total de no mínimo o dobro da banda contratada dos serviços LIT ativos.

7.6. A ausência de comprovação do fornecimento efetivo de trânsito IP para conectividade do AS da ATI aos PTTs listados, tanto em IPv4 como em IPv6 nativamente, acarretará insucesso na homologação técnica, impedindo o início do faturamento até que a exigência seja plenamente atendida.

7.7. A comprovação do fornecimento de trânsito deverá ser apresentada até a entrega do serviço para fins de homologação e início do faturamento.

7.8. A CONTRATADA deverá manter políticas de roteamento que impeçam conexões diretas alternativas do AS da ATI aos PTTs, garantindo que todo o tráfego passe exclusivamente pelo AS da CONTRATADA.

## 8. Especificações exclusivas do Link de Internet Trânsito para *Datacenter* com Anti-DDoS (LIT).

8.1. Os Links de trânsito (LIT 1 e LIT 2) da solução do serviço Link de Internet Trânsito para *Datacenter* com Anti-DDoS (LIT) deverão operar simultaneamente, com a configuração de responsabilidade da CONTRATADA, e orientados pela CONTRATANTE, conforme as melhores práticas de configuração de rotas de IPv4 e IPv6, em alta disponibilidade.

8.2. Os links LIT 1 E LIT 2 deverão ser atendidos, cada um, por rotas distintas entre si, acessos distintos e em pontos de presença distintos, porém em cada um dos Links LIT 1 e LIT 2 poderão operar na forma ATIVA+ATIVA ou ATIVA+PASSIVA, conforme a necessidade da CONTRATANTE, conectados obrigatoriamente em equipamentos (Roteadores e Switches) distintos nos ambientes dos provedores dos LIT 1 e LIT 2 da CONTRATADA.

8.3. Os acessos dos links LIT 1 e LIT 2 não poderão utilizar o mesmo ponto de presença físico em cada um dos ASNs, assim como não será permitido o compartilhamento de PoPs entre os ASNs.

8.4. A CONTRATADA deverá fornecer conectividade IP (Internet Protocol) com velocidades simétricas (DOWNLOAD e UPLOAD), não sendo permitido nenhum tipo modelagem de tráfego (Traffic Shaping) que limite ou bloqueie qualquer tipo de aplicações em qualquer percentual abaixo da velocidade nominal CONTRATADA bem como também nenhum tipo de bloqueio de acesso a qualquer site da Internet ou bloqueios de quaisquer tipos de arquivos em uploads/downloads realizados pelos usuários do CONTRATANTE.

8.5. A CONTRATADA deverá publicar o bloco ASN (Autonomous System Number) 10938 do CONTRATANTE para todas as operadoras de telecomunicações nacionais e internacionais através do protocolo de roteamento externo BGP (IPv4 e IPv6).

#### 8.6. Requisitos Lógicos:

8.6.1. A CONTRATADA não deverá impor restrições à CONTRATANTE que impliquem na necessidade de reduzir o MTU (Maximum Transmission Unit) para menos de 1522Bytes (mil, quinhentos e vinte e dois bytes) considerando payload e cabeçalhos.

8.6.2. A CONTRATADA deverá tomar todas as medidas para garantir o correto funcionamento do tráfego, inclusive gerenciando o tráfego Internet de maneira proativa em suas próprias redes, independente de quem tenha gerado o tráfego Internet.

##### 8.6.3. Requisitos de Desempenho:

8.6.3.1. A latência na conexão entre o ambiente do CONTRATANTE e quaisquer dos PoPs deverá ser inferior a 5ms (cinco milissegundos).

8.6.3.2. O jitter na conexão entre o ambiente do CONTRATANTE e quaisquer dos PoPs deverá ser inferior a 2ms (dois milissegundos).

8.6.3.3. A perda de pacotes na conexão entre o ambiente do CONTRATANTE e quaisquer dos PoPs deverá ser no máximo de 1% (um por cento).

8.6.3.4. O serviço será considerado como indisponível caso o limite estabelecido pelas métricas de latência, jitter e perda de pacotes seja ultrapassado.

8.6.4. Serão tolerados valores das métricas de latência, jitter e perda de pacotes acima do limite, se for comprovado que o consumo do serviço esteja acima de 80% da velocidade CONTRATADA.

#### 8.7. ANTI-DDOS

8.7.1. A solução do serviço de Link de Internet Trânsito para *Datacenter* com Anti-DDoS (LIT), deve ser composto de uma solução de proteção a ataques do tipo DDoS (Distributed Denial of Service), e todo o tráfego originado para Internet deverá ser encaminhado à infraestrutura da CONTRATADA para análise de ataques DDoS, e só reencaminhar à infraestrutura da CONTRATANTE o tráfego livre destes conteúdos indesejados, sendo este recurso disponibilizado e atuante nas instalações da CONTRATADA, protegendo este serviço de possíveis problemas de desempenho devido a este tipo de tráfego;

8.7.2. A solução do serviço de LIT o acesso à Internet para cada infraestrutura deve incluir uma solução de proteção contra-ataques DDoS (Distributed Denial of Service). Todo o tráfego originado da Internet e dos PTT para AS10938 deve ser redirecionado para a solução de Anti-DDoS da CONTRATADA, de forma Inline;

8.7.3. A solução deverá analisar todo o tráfego em tempo real, identificando e mitigando ataques DDoS antes de reencaminhar o tráfego para o AS da ATI. Todo o tráfego deve estar limpo para a infraestrutura da CONTRATANTE. Esse recurso, disponível e atuante nas instalações da CONTRATADA, garantirá a proteção contra problemas de desempenho relacionados a esse tipo de tráfego, assegurando a continuidade e a integridade dos serviços da CONTRATANTE;

8.7.4. Segurança de *Backbone*: Solução de segurança para proteção contra-ataques do tipo DDoS (Distributed Denial of Service) a ser implementada no *backbone* da CONTRATADA garantindo que, através da análise de comportamento do tráfego, seja identificado o ataque e de forma preventiva encaminhado para infraestrutura da Solução de Anti-DDoS da CONTRATADA, que, após aplicação a limpeza, o tráfego legítimo seja redirecionado às localidades da CONTRATANTE;

8.7.5. A limpeza do tráfego deverá ser seletiva e atuar apenas sobre os pacotes destinados aos IPs das unidades atacadas, das redes disponibilizadas IPv6 e IPv4 para tratamento, sendo que todo tráfego restante não poderá sofrer nenhuma forma de limpeza ou desvio;

8.7.6. A técnica para identificação de ataques DoS e/ou DDoS utilizada deverá ser por métrica de volumetria;

8.7.7. A Segurança de Backbone deverá atuar em todas as localidades previstas neste Termo de Referência;

8.7.8. A CONTRATADA deverá manter a política de mitigação sempre em automática, realizando alterações somente mediante solicitação por abertura de chamado pela Equipe do CIISC.

8.7.9. A CONTRATADA deverá notificar a Equipe do CIISC em caso de suspeita de ataque, permitindo que esta solicite a mitigação do ataque.

8.7.10. A CONTRATADA terá até 5 (cinco) minutos para iniciar a mitigação após solicitação da Equipe do CIISC.

8.7.11. A CONTRATADA deverá iniciar em, no máximo, 30 segundos a mitigação de ataques de DoS e/ou DDoS após a identificação da anormalidade do tráfego;

8.7.12. A CONTRATANTE poderá optar pela troca de mitigação automática (padrão) para manual previamente configurada para ataques detectados, sendo que a detecção e a mitigação deverão ocorrer em tempo real (Inline) quando configurado em modo manual ou automático.

8.7.13. A Segurança de Backbone atuará em todos os ataques identificados, não podendo ser limitada ou interrompida por franquias ou volume de mitigação;

8.7.14. A solução deverá possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

8.7.15. A CONTRATADA deverá tomar todas as providências necessárias para recompor a disponibilidade do Serviço de Internet em caso de incidentes de ataques de DoS e/ou DDoS, recuperando o pleno funcionamento dele;

8.7.16. A mitigação de ataques deverá ocorrer de forma regionalizada, garantindo que o tráfego seja tratado antes da entrega à CONTRATANTE (ATI): ataques de origem nacional devem ser obrigatoriamente mitigados em centros de limpeza (scrubbing centers) localizados em território brasileiro, enquanto ataques de origem internacional devem ser tratados em centros internacionais. O encaminhamento de tráfego nacional para centros de limpeza fora do país será admitido apenas em caráter excepcional, caso a volumetria do ataque ultrapasse a capacidade operacional dos centros nacionais, visando sempre a menor latência e a máxima proteção da rede do Estado.

8.7.17. Nos períodos de ataque a latência do circuito deverá ser de no máximo 100ms (cem milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250ms (duzentos e cinquenta milissegundos) quando se originar do(s) centro(s) internacionais;

8.7.18. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da CONTRATANTE para coleta dos dados a serem analisados;

8.7.19. A mitigação de ataques deverá ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

8.7.20. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS da CONTRATADA, deverão ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo;

8.7.21. A CONTRATADA deverá realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

8.7.22. As funcionalidades de monitoramento, detecção e mitigação de ataques deverão ser mantidas pela CONTRATADA em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

8.7.23. A CONTRATADA deverá disponibilizar um portal e credenciais de acesso de leitura, onde a CONTRATANTE tenha acesso online às informações da Segurança de Backbone, quando solicitadas;

8.7.24. Adotar o Protocolo TCP/IP - IPV6 e garantir a coexistência, bem como a interoperabilidade, entre IPv6 e IPv4 nos equipamentos conectados via Rede e aos produtos que suportam ambos os protocolos, respeitando a RFC 3531, mantendo as conexões entre eles;

8.7.25. A CONTRATADA deverá implementar e garantir o acesso de consulta (via SNMPv3 ou superior) à Solução de Proteção Anti-DDoS, para monitoramento do tráfego pela CONTRATANTE, inclusive por meio do Centro Integrado de Inteligência e Segurança Cibernética (CIISC);

8.7.26. Prover e manter o registro de log do serviço, onde todos os logs devem ser disponibilizados na Solução de Guarda de Logs, especificado no ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO;

8.7.27. A CONTRATADA deve garantir as seguintes características para o Anti-DDoS:

8.7.28. Ser capaz de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;

8.7.29. Permitir a criação de listas negras (Black Lists) assim como listas brancas (White Lists) visando dinamizar a decisão de mitigação automática de tráfego potencialmente malicioso na rede - ou de respeitar determinada política de segurança;

8.7.30. A solução deverá permitir a criação de tais listas de forma direta (configuradas no próprio equipamento) ou indireta (criadas externamente à solução e importadas para a plataforma de mitigação DDoS), suportando mitigação de ataques, utilizando técnicas como: limitação de taxa, desafio-resposta, descarte de pacotes malformados, mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras;

8.7.31. Prover a inclusão de tráfego em listas negras ou brancas de forma estática ou dinâmica. A inclusão de tráfego de forma dinâmica nas listas negras/ brancas deverá realizar-se, no mínimo, como consequência de autenticação de tráfego de rede pela plataforma de mitigação DDoS, ou de limites previamente ultrapassados na plataforma;

8.7.32. Suportar a aplicação de regras de mitigação com base nos seguintes parâmetros:

8.7.32.1. Origem IP;

8.7.32.2. Destino IP; e

8.7.32.3. Combinação Origem + Destino IP.

8.7.33. Suportar mitigação de ataques que visam vulnerabilidades nas Camadas 2 OSI, 3 OSI, 4 OSI e 7 OSI;

8.7.34. Prover informações de origem de ataque dos países, intervalos (ranges) de endereços IP e características do tipo de ataque;

8.7.35. Prover serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação;

8.7.36. Ser capaz de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv6 como para IPv4, incluindo, mas não se restringindo aos seguintes:

8.7.36.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

8.7.36.2. Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

8.7.36.3. Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn;

- 8.7.36.4. Limitar o número de conexões TCP simultâneas de um mesmo host;
- 8.7.36.5. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
- 8.7.36.6. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
- 8.7.36.7. Ataques denominados de “Comand-and-Control”, Point of Sale *Malware*, Remote Access Trojans RAT’s via feed atualizado diariamente;
- 8.7.36.8. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumétricos;
- 8.7.36.9. Bloqueio de query de DNS, resposta de query de DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de recursão DNS;
- 8.7.36.10. DNS BlackList;
- 8.7.36.11. RegEx para registros específicos ou “flags de recursão”;
- 8.7.37. Possuir mecanismos que permita bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente;
- 8.7.38. Possuir autenticação em query DNS por requisição em TCP;
- 8.7.39. Possuir autenticação em JavaScript e Redirect para HTTP;
- 8.7.40. Adicionar expressão regular de “payload” em blacklists;
- 8.7.41. Prevenir que hosts válidos sejam adicionados a blacklists por engano;
- 8.7.42. Ser capaz de detectar um ataque DDoS automaticamente, ou manualmente, e realizar mitigação na nuvem para apenas o tráfego atacado, contudo na infraestrutura da CONTRATADA, e só redirecionar o tráfego para a rede da CONTRATANTE quando este estiver limpo deste tipo de ataque;
- 8.7.43. Realizar a sinalização entre a rede da CONTRATANTE e a rede da PROPONENTE em qualquer protocolo protegido, podendo ser ativada por qualquer uma das contramedidas especificadas para este serviço;
- 8.7.44. Manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período considerado seguro;
- 8.7.45. Possuir serviço de atualização de assinaturas de ataques para as soluções de detecção e mitigação;
- 8.7.46. Prover a mitigação de ataques baseada em arquitetura na qual haja o desvio de tráfego suspeito, comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
- 8.7.47. A CONTRATADA deve fornecer acesso à ferramenta através de um navegador padrão para disponibilizar relatórios e informações do tráfego monitorado, bem como visualizar os eventos e alertas de segurança, contendo, no mínimo, as seguintes informações sobre os ataques:
  - 8.7.47.1. Tipo;
  - 8.7.47.2. Horário de início e fim;
  - 8.7.47.3. Volume de tráfego bloqueado e não bloqueado;
  - 8.7.47.4. IP(s) de destino(s);
  - 8.7.47.5. Os maiores alvos;
  - 8.7.47.6. Os maiores ofensores (IP de origem);
  - 8.7.47.7. Os maiores ofensores por geolocalização (país);
  - 8.7.47.8. Percentual das origens, por geolocalização (país);
- 8.7.48. A CONTRATADA deve atender aos seguintes requisitos mínimos da Infraestrutura de Suporte Anti-DDoS:

- 8.7.48.1. Garantir que o Centro Integrado de Inteligência e Segurança Cibernética (CIISC) seja informada de qualquer evento deste tipo de ataque;
- 8.7.48.2. Não permitir a saturação da banda de Internet em caso de ataques de negação de serviço (Distributed Denial of Service – DDoS );
- 8.7.48.3. Disponibilizar um portal onde a CONTRATANTE e a Centro Integrado de Inteligência e Segurança Cibernética (CIISC) tenha acesso online aos tipos de ataques sofridos e ao tamanho destes ataques categorizados por severidade (Ex: baixo, médio, alto);
- 8.7.48.4. Garantir que não haja interrupção, na totalidade CONTRATADA, do acesso ao Serviço de Internet por ataque anti-DDoS;
- 8.7.48.5. A CONTRATADA deverá permitir no mínimo 20 (vinte) usuários para consulta, com no mínimo 5 (cinco) acessos simultâneos à Solução Anti-DDoS disponibilizada;
- 8.7.49. Toda a Interação com relação a abertura de chamados, manutenção programada e registro de ocorrências, deve ser realizada através do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), para ter um único ponto de Gestão de Demandas e Registro de Ocorrências;
- 8.7.50. A abertura de chamados, o agendamento de manutenções programadas e o registro de ocorrências operacionais pelo Estado deverão ser realizados exclusivamente por meio do CIISC;
- 8.7.51. Sem prejuízo do disposto no item 8.7.50, a CONTRATADA do LOTE 2 poderá realizar o monitoramento proativo de falhas no meio físico por meio de coleta de informações via SNMPv3 ou superior, a ser disponibilizado pelo CIISC, devendo, nos casos identificados, iniciar de imediato as ações de correção e manter o CIISC informado, em paralelo, sobre o evento e as providências adotadas.

## ADENDO VIII - SOLUÇÕES DE SEGURANÇA DO CENTRO DE GERENCIAMENTO

### 1. Requisitos gerais

- 1.1. O serviço de segurança da Nova Rede Corporativa deve garantir a proteção do tráfego, de forma gerenciada, em toda a Nova Rede. As especificações destes serviços estão detalhadas neste Termo de Referência;
- 1.2. De acordo com o Marco Civil da Internet, Lei nº 12.965/2014, os administradores de sistemas autônomos (ASN) são obrigados a guardar os logs de conexão;
- 1.3. De acordo com a resolução da Anatel nº 614/2013, que estabelece regras para SCM, determina a guarda de logs pelas “prestadoras”, ou seja, todos que possuem SCM devem guardar os logs de conexão;
- 1.4. A CONTRATADA deve realizar a implantação dos equipamentos que compõem o Serviço de Segurança da Nova Rede Corporativa seguindo o cronograma proposto para atendimento dos níveis de maturidade citados no Serviço de Evolução da Maturidade em Segurança da Informação;
- 1.5. O Serviço de Segurança da Nova Rede, deve disponibilizar toda infraestrutura da solução adotada, para garantir as seguintes funcionalidades detalhadas neste Termo de Referência:
- 1.5.1. Solução de gerenciamento e monitoramento de ativos – ITAM;
- 1.5.2. Solução para guarda de LOGs;
- 1.5.3. Solução de gerenciamento de identidade de acesso – IAM;
- 1.5.4. Solução de monitoramento e análise de eventos de segurança – SIEM;

1.5.5. Solução de automação de resposta a incidentes de segurança – SOAR;

1.5.6. Serviço de disponibilização de ambiente de testes;

1.5.7. Solução de gerenciamento de serviços de TI - ITSM.

1.6. Todas as funcionalidades deste serviço devem ser disponibilizadas pela CONTRATADA e operacionalizada (Acompanhamento, Configuração, Implementação de Regras de segurança, disponibilização de acessos e outros) pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede;

1.7. Todos os equipamentos que compõem a solução devem:

1.7.1. Suportar o protocolo de gerenciamento SNMP compatível com pelo menos a versão 3. Durante a execução contratual, caso surja uma versão mais atual, estável, do protocolo, os equipamentos devem ser atualizados para suportar esta nova versão;

1.7.2. Manter atualizados, durante a vigência do contrato, os softwares/firmwares que compõem a solução em suas versões estáveis e livres de vulnerabilidades conhecidas, com janelas de manutenção combinadas, e sob a anuência da ATI;

1.7.3. Fornecer à ATI credenciais de acesso de leitura a todas as soluções e recursos que compõem este serviço na Nova Rede, quando solicitadas;

1.7.4. Assegurar a operação contínua de todos os recursos de segurança, incluindo atualizações de bases de dados para todas as funcionalidades, ao longo da vigência do contrato da Nova Rede, com toda a documentação acessível através do site do fabricante;

1.7.5. Possuir interface de administração via web no próprio dispositivo, permitindo configurá-lo diretamente através de um navegador web;

1.7.6. Possuir interface de administração via linha de comando CLI (Command Line Interface);

1.7.7. Possuir bases de dados, assinaturas e funcionalidades (engines) de segurança desenvolvidas pelo mesmo fabricante ou parceiros, desde que atenda todas as especificações solicitadas e não haja perda de funcionalidades;

1.7.8. Permitir operar em alta disponibilidade ativo/ativo e ativo/passivo, caso necessário, de modo transparente;

1.7.9. Garantir e suportar acesso para gerenciamento da solução via SSH e cliente WEB (HTTPS);

1.7.10. Permitir a aplicação de políticas de senhas de acesso na solução adotada;

1.7.11. Todos os dispositivos disponibilizados para uso da nova Rede, devem ser acessados por protocolos seguros e os usuários devem estar cadastrados em uma base de dados LDAP, LDAP/AD, disponibilizada pela CONTRATADA;

1.7.12. A Solução deve prover exportação de dados via CSV;

1.7.13. A CONTRATADA deve prover, a partir dos dados exportados da solução, arquivos e relatórios para a CONTRATANTE aderente Técnica (ATI) e os CONTRATANTES aderentes nos seguintes formatos: PDF, CSV, HTML, XML, ODS, XLSX, DOCX e ODT;

1.7.14. Todos os equipamentos disponibilizados para O Serviço de Segurança da Nova Rede, devem funcionar em alta disponibilidade (HA – High Availability);

## 2. Solução de gerenciamento e monitoramento de ativos - ITAM

2.1. Operar e funcionar em alta disponibilidade (HA – High Availability) sincronizando as configurações, objetos e políticas entre as estações de gerência;

2.2. Garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

2.3. Definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.4. Gerar alertas automáticos via e-mail e SNMP para destinatários definidos pela ATI;

2.5. Possibilitar a criação e administração de políticas de Firewall, controle de aplicação, Sistema de prevenção a intrusão (IPS – Intrusion Prevention System), Antivírus, pontos de acesso sem fio e de Filtro de URL;

2.6. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

2.7. Permitir localizar quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;

2.8. Atribuir sequencialmente um número a cada regra de Firewall, de NAT ou de QoS;

2.9. Permitir criação de regras que fiquem ativas em horário definido;

2.10. Permitir criação de regras com data de expiração;

2.11. Realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;

2.12. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;

2.13. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

2.14. Garantir que todos os Firewalls sejam controlados de forma centralizada;

2.15. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

2.16. Permitir ao administrador transferir os backups para um servidor sFTP;

2.17. Garantir que as alterações realizadas em um servidor de gerência sejam automaticamente replicadas para o servidor redundante;

2.18. Realizar as funções de gerência e monitoramento através de um ou mais dispositivos;

- 2.19. Continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;
- 2.20. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;
- 2.21. Permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS, de acordo com o modelo de autenticação adotado sendo definido pela CONTRATANTE com o custo da infraestrutura arcado pela CONTRATADA;
- 2.22. Garantir que os operadores da CONTRATADA, e os usuários designados pela CONTRATANTE, se autenticuem nos servidores de gerência das soluções adotadas, através de solução de autenticação LDAP ou LDAP/AD, disponibilizada pela CONTRATADA. O acesso a essa infraestrutura deve ser de acordo com o modelo de autenticação definido pela CONTRATANTE;
- 2.23. Suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP;
- 2.24. O protocolo NTP deve ser prioritariamente sincronizado com o NTP da ATI, e como contingência com os servidores do NTP.br;
- 2.25. Registrar e manter nos registros e logs, pelo período do contrato, os logins validados pelo sistema, de qualquer usuário, como também as tentativas de login, por um período de 06 (seis) meses;
- 2.26. Prover e manter, pelo período do contrato, logs de auditoria das configurações de regras e objetos. Tais regras devem ser visualizadas em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- 2.27. Gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- 2.28. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;
- 2.29. Permitir criar os objetos que serão utilizados nas políticas, de forma centralizada;
- 2.30. Permitir bloqueio por países para qualquer IP, domínio ou aplicações hospedadas na Nova Rede;
- 2.31. Deverá ser liberado o acesso às instâncias virtuais, definidas e especificadas neste Termo de Referência, para a CONTRATANTE aderente Técnica e CONTRATANTES aderentes criarem regras específicas seguindo o Termo de Responsabilidade. As regras globais devem ser implementadas pelo Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede, após a aprovação da Gestão Técnica da Rede/ATI.

### 3. Solução para guarda de LOGs

- 3.1. Garantir uma infraestrutura para receber e consolidar os logs (tipo syslog) de todos os dispositivos e serviços da Nova Rede, com estimativa de 320 GB/dia e manter por 120 (cento e vinte) dias com acesso online;
- 3.2. Todos os logs dos dispositivos e serviços da Nova Rede devem ser mantidos off-line, até o fim do contrato, utilizando, por exemplo, uma das seguintes soluções: em nuvem ou backup no através de bibliotecas LTO (Linear Tape Open), ou outra solução de armazenamento adequada;
- 3.3. Todos os logs devem ser disponibilizados para exportação com acesso apenas de leitura para a CONTRATANTE aderente Técnica (ATI);

- 3.4. Todos os logs referentes aos dispositivos e serviços dos CONTRATANTES aderentes, devem ser disponibilizados para exportação com acesso apenas de leitura;
- 3.5. Deve ser disponibilizada uma aplicação web padrão para gestão de Syslog, com o objetivo de disponibilizar os arquivos de logs;
- 3.6. Possibilitar a contingência do backup, desde o início da prestação do serviço, através da conexão de rede local com o Datacenter da ATI. As políticas de backup, atualizações e seus períodos de execução serão definidos pela ATI;
- 3.7. Possibilitar, de forma centralizada, a visualização dos logs recebidos por um ou vários dispositivos externos, incluindo a capacidade de uso de filtros nas pesquisas deste log;
- 3.8. Garantir que a solução atue como um servidor de syslog, aceite e concentre logs de todos os dispositivos de diferentes fabricantes da nova Rede.
- 3.9. Requisitos da solução de Relatórios da Segurança:
- 3.9.1. Garantir uma infraestrutura para receber e consolidar os logs dos dispositivos de segurança da Nova Rede, e manter por 120 (cento e vinte) dias com acesso online;
- 3.9.2. Todos os logs dos dispositivos de segurança da Nova Rede devem ser mantidos off-line, até o fim do contrato, utilizando, por exemplo, uma das seguintes soluções: em nuvem ou backup, através de bibliotecas LTO (Linear Tape Open), ou outra solução de armazenamento adequada;
- 3.9.3. Todos os logs devem ser disponibilizados para exportação com acesso apenas de leitura para a CONTRATANTE aderente Técnica ATI;
- 3.9.4. Possuir taxa de coleta de Logs/sec de 160.000 (cento e sessenta mil);
- 3.9.5. Possuir capacidade de armazenamento de 10.5 TB Log/dia;
- 3.9.6. Possibilitar acesso simultâneo de administradores, permitindo a criação de perfis para administração e monitoração;
- 3.9.7. Permitir a criação de administradores que acessem a todas as instâncias de virtualização da solução de relatórios;
- 3.9.8. Permitir a criação de contas de administradores para uso da ATI que possam gerar, e editar relatórios gerenciais de todos os de diferentes instâncias de virtualização da solução, assim como também visualizar o status deles (dispositivos);
- 3.9.9. Garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego gerado no PCM;
- 3.9.10. Definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 3.9.11. Possuir mecanismo para que logs antigos sejam removidos automaticamente, após estarem consolidados na Solução para guarda de LOGs;
- 3.9.12. Permitir a extração de relatórios;
- 3.9.13. Garantir a exportação dos logs no formato de arquivo do tipo CSV;
- 3.9.14. Gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 3.9.15. Possuir relatórios pré-definidos;
- 3.9.16. Possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida;
- 3.9.17. Possuir a capacidade de personalização de capas para os relatórios, que devem ser gerados com os logotipos definidos pela CONTRATANTE aderente;
- 3.9.18. Possibilitar, de forma centralizada, a visualização dos logs recebidos por um ou vários dispositivos externos, incluindo a capacidade de uso de filtros nas pesquisas deste log;
- 3.9.19. Permitir a geração de relatórios de logs de tráfego de dados;
- 3.9.20. Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos;
- 3.9.21. Possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza, para inserção aos relatórios;
- 3.9.22. Deve possuir mecanismo para exibir de forma detalhada (Drill-Down) nos relatórios em tempo real (realtime);
- 3.9.23. Dever ser possível fazer download dos arquivos de logs recebidos;
- 3.9.24. Possibilitar o envio de maneira automática de relatórios por e-mail;
- 3.9.25. Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido;

- 3.9.26. Permitir programar a geração de relatórios, conforme calendário definido pela CONTRATANTE;
- 3.9.27. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da CONTRATANTE, adaptando-o às suas necessidades;
- 3.9.28. Ter a capacidade de definir filtros nos relatórios;
- 3.9.29. Ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
- 3.9.30. Gerar alertas automáticos via e-mail, SNMP e Syslog baseados em eventos de ocorrência como log, severidade de log, entre outros;
- 3.9.31. Permitir a criação de painéis (Dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
- 3.9.32. Garantir a capacidade de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;
- 3.9.33. Garantir a visualização na interface gráfica de usuário (GUI) da solução de relatórios de informações do sistema: total de logs diários recebidos, alertas gerados, entre outros;
- 3.9.34. Deve possuir uma ferramenta para análise de desempenho, com o objetivo de detectar problemas de performance, caso a solução não possua ferramentas para análise de desempenho na solução de gerência;
- 3.9.35. Permitir a emissão de relatórios/exportação para análise de logs arquivados de outros dispositivos da mesma solução;
- 3.9.36. Garantir o espaço necessário para que cada instância de virtualização realize o armazenamento de logs, permitindo filtro por instância virtual.

#### 4. Solução de gerenciamento de identidade de acesso - IAM

- 4.1. Garantir Infraestrutura para prover e implementar cópias em alta disponibilidade do serviço de LDAP principal do Governo de Pernambuco, hospedado no Datacenter da ATI. A solução, para receber a cópia do LDAP principal da infraestrutura (hardwares/softwarewares) da Nova Rede, deve ter capacidade mínima de 629.058 (seiscentos e vinte e nove mil e cinquenta e oito) usuários;
- 4.2. Prover e implementar uma solução em alta disponibilidade para autenticar todos os alunos da rede estadual de ensino do Governo de Pernambuco, e os cidadãos considerados visitantes dos Órgãos Públicos, quando do acesso à Internet. A infraestrutura disponibilizada (hardwares/softwarewares) da Nova Rede, deve suportar a autenticação de no mínimo 629.058 (seiscentos e vinte e nove mil e cinquenta e oito) usuários. Essa autenticação pode ser utilizada aproveitando cadastro em redes sociais, bases LDAP e RADIUS, realizando apenas os registros desses usuários na hora do uso dos recursos de Internet, com as informações de tempo ativo, sites acessados etc.;
- 4.3. Ser ofertada em appliance que pode ser virtual ou físico de responsabilidade da CONTRATADA;
- 4.4. Possuir um servidor LDAP interno que permite ser configurado de forma hierárquica, para a correta administração por grupos ou unidades organizacionais dos usuários locais;
- 4.5. Permitir a geração em massa de usuários na base de dados local pelo administrador, possibilitando que uma lista de usuários seja importada a partir de um arquivo externo;
- 4.6. Deve permitir a importação dinâmica de usuários a partir de um LDAP externo, baseado em filtros customizados. Deve, ainda, associar um grupo a esses usuários importados e vincular tokens a eles, automaticamente;
- 4.7. Realizar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;
- 4.8. Permitir o backup completo da solução, incluindo toda a configuração: interfaces, endereços IP, base de usuários, grupos e tokens. O arquivo de restauração deverá permitir recuperar o equipamento diretamente da interface gráfica;
- 4.9. Suportar a opção de backup criptografado;
- 4.10. Funcionar em Alta Disponibilidade (HA) em implementação "Ativo/Ativo" evitando a descontinuidade do serviço;
- 4.11. Permitir sincronismo automático de configurações entre todos os equipamentos que fazem parte da solução em Alta Disponibilidade (HA);
- 4.12. Suportar SSO por estrutura RSSO (RADIUS Single SignOn);
- 4.13. Permitir ordenação de Logs de acordo com a necessidade do administrador: por usuário que realizou a mudança, por data, por forma ascendente e por forma descendente;

- 4.14. Suportar filtragem dos usuários que irão utilizar recurso de SSO (Single SignOn), separando-os de grupos que não necessitam;
- 4.15. Suportar a validação de certificados de fontes externas;
- 4.16. Funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
- 4.17. Suportar captura de pacotes através da interface gráfica para resolução de problemas (troubleshoot) avançado em Wireshark ou outra ferramenta de análise de pacotes;
- 4.18. Suportar a criação de usuários em base local independente, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade da CONTRATANTE, contudo em canal de comunicação seguro;
- 4.19. Permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO;
- 4.20. Suportar SCEP (Simple Certificate Enrollment Protocol), assinando petições de certificados digitais assinados (CSR), automaticamente ou manualmente;
- 4.21. Permitir a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
- 4.22. Permitir que a geração dos usuários na base de dados local seja feita de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;
- 4.23. Permitir enviar e-mails aos administradores relacionados a reinicialização de senha, aprovação de novos usuários e autenticação de segundo fator (token);
- 4.24. Atuar como Autoridade Certificadora (CA);
- 4.25. Permitir associar os tokens aos usuários criados localmente na base de dados;
- 4.26. Possibilitar, a critério da CONTRATANTE, a autenticação de dispositivos conhecidos com o mínimo de interação dos usuários através de autenticação por endereço MAC, ou seja, MACs previamente conhecidos, cadastrados e autorizados são automaticamente autenticados pela solução sem necessidade de interação do usuário final (como redigitar usuário e senha);
- 4.27. Permitir, a critério da CONTRATANTE, que usuários visitantes, que não possuam uma conta local ou em mídias sociais, também se autenticuem em uma rede sem fio apropriada, com cadastro rápido, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail e/ou números de telefone, a infraestrutura para prover essa autenticação deve ser fornecida pela CONTRATADA, hospedada no ambiente físico da CONTRATADA e/ou nuvem (seguindo os requisitos mínimos do ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM), sendo os dados desses usuários mantidos pelo período do contrato, tais dados devem ser encaminhados para solução de concentração de logs;
- 4.28. A solução deve suportar a integração com servidor RADIUS remoto;
- 4.29. Deve permitir a criação de regras de autenticação RADIUS para que, de forma bem granular, seja possível impor modelos de autenticação distintos (OTP, MAB etc) a depender do RADIUS client bem como os atributos envolvidos na requisição;
- 4.30. Prover repositório para autenticação de VPN Site-to-Site através de Certificados;
- 4.31. Suportar a gerência centralizada de usuários, em todos os aspectos e recursos disponibilizados pela solução;
- 4.32. Funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
- 4.33. Suportar designação automática de VLANs para usuários, com base em critérios pré-definidos pelo administrador;
- 4.34. Prover um portal web, de acordo com os requisitos definidos pela CONTRATADA, para o auto registro dos usuários, de forma que ele possa ingressar em um portal e registrar seus dados. Após o usuário efetuar o registro, o administrador deverá receber um e-mail para aprovar ou negar o cadastro dele antes que ele seja ativado;
- 4.35. Poderá ser entregue em solução única ou conjunto de soluções, desde que atenda a todos os requisitos sem perda de desempenho, funcionalidade ou limitação;
- 4.36. Permitir que o usuário possa recuperar sua senha através de um correio eletrônico ou pergunta de segurança, que poderão ser configuráveis pelo usuário;
- 4.37. Prover capacidade de serviço Single SignOn (SSO), com autenticação transparente (passiva) de usuários em sistemas compatíveis;

- 4.38. Permitir que a solução garanta a geração dos usuários na base de dados local seja feita pelo administrador, que poderá definir uma senha no momento de geração do usuário;
- 4.39. Permitir criar políticas de bloqueio automático de usuários após uma quantidade de falhas de autenticação, evitando assim ataques de força bruta contra o usuário;
- 4.40. A solução deve ser compatível com o item Múltiplo fator de autenticação;
- 4.41. Deve impor tempo máximo para ativação de token, bem como tamanho mínimo do OTP e configuração de PIN para visualização do OTP;
- 4.42. Deve permitir push notification, de forma que o usuário não precise digitar o código para obter acesso ao recurso demandado. Deve, ainda, permitir o filtro baseado em geolocalização.
- 4.43. A solução deve permitir o roteamento da autenticação, associando nomes a diretórios de LDAP, RADIUS e SAML e, dessa forma, seja possível identificar a que servidor pertence um determinado login;
- 4.44. Deve suportar o protocolo de verificação online de status de certificado OCSP (Online Certificate Status Protocol) para que se possa fornecer uma lista de certificados revogados (CRL);
- 4.45. Permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;
- 4.46. Suportar customização de mensagens padrão em páginas Web, como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas páginas sem a necessidade recursos ou conectividade externa;
- 4.47. Permitir e implementar a integração com servidor LDAP remoto (como Microsoft Active directory);
- 4.48. Deve suportar OAUTH, permitindo integração ao G Suite e outras plataformas;
- 4.49. Deverá garantir o suporte à integração de diretórios de usuários existentes na conta do Google GSuite (Google Workspace) e Office365 (Microsoft 365) atualmente em utilização em alguns clientes da ATI-PE. Esta solução deverá disponibilizar funcionalidade de SSO (Entrada Única), permitindo o uso das mesmas credenciais da base de dados do GSuite (Google Workspace) e Office365 (Microsoft 365) para autenticação na rede corporativa;
- 4.50. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO (Single SignOn), onde se utilizariam as mesmas credenciais que o usuário utiliza ao autenticar-se no domínio em seu computador pessoal;
- 4.51. Possuir indicador visual, centralizado, de informações críticas (versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);
- 4.52. Permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;
- 4.53. Ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
- 4.54. Permitir criar e assinar certificados X.509 para utilização em servidores HTTPS e SSH, assim como para os clientes de serviços HTTPS, SSH, VPNs e IPSec;
- 4.55. Possuir nativamente Trap SNMP indicando mudança de status de Alta Disponibilidade (HA);
- 4.56. Permitir remoção de usuários inativos por bulk (remoção massiva), baseado em critérios definidos;
- 4.57. Suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);
- 4.58. Suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO (Single SignOn);
- 4.59. Suportar ultrapassar (by-pass) de autenticação 802.1X para dispositivos não compatíveis, e autenticá-los através de MAC Address (MAC Address Authentication Bypass);
- 4.60. Suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;
- 4.61. Deve permitir a configuração do CN (Common Name) dos usuários, para a integração com serviços e/ou dispositivos que o requeiram;
- 4.62. Suportar o envio de e-mails atuando como servidor próprio (localhost) ou integrar-se com servidor(es) externo(s) para envio das mensagens aos usuários ou administradores;
- 4.63. Permitir a utilização de mecanismo de autenticação de dois fatores, utilizando aplicativo que gerem códigos a intervalos não superiores a 60 segundos, e com ao menos 6 dígitos (Token Mobile). O aplicativo deve ser compatível para iOS ou Android que forneça segurança de autenticação forte sem hardware adicional;
- 4.64. Deve permitir o auto provisionamento de MFA por parte dos usuários, por tipo de token, bem como permitir que eles usem temporariamente SMS e que consigam revogar tokens sem interação do administrador da solução;

- 4.65. Permitir que se configure um perfil de complexidade mínimo para as senhas de todos os usuários que sejam cadastrados na base de dados locais, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos e caracteres especiais;
- 4.66. Permitir autenticação de usuários visitantes por método de validação com base em credenciais de mídias sociais: Facebook, Twitter, LinkedIn, Google, pelo menos;
- 4.67. Suportar NTP (Network Time Protocol), visando sincronismo com ativos existentes com base em fonte central para fornecimento de hora/data corretos;
- 4.68. Prover os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS, EAP-GTC;
- 4.69. Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas.
- 4.70. Requisitos mínimos para Solução de gerenciamento de identidade de acesso (identificação do usuário), de responsabilidade da CONTRATADA:
- 4.70.1. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 4.70.2. Possuir integração com LDAP, LDAP/Microsoft Active directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on; essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso, não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 4.70.3. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 4.70.4. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 4.70.5. Permitir o recurso de bloqueio e continuação, possibilitando que o usuário acesse um site potencialmente bloqueado, informando ao mesmo, na tela de bloqueio, e possibilitando, a utilização de um botão “Continuar”, que permita ao usuário acessar o site;
- 4.70.6. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 4.70.7. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP, LDAP/AD;
- 4.70.8. Permitir integração com tokens ou agentes para autenticação dos usuários;
- 4.70.9. Prover, no mínimo, um token ou agente nativamente, possibilitando autenticação de duplo fator ou baseada em Kerberos.
- 4.70.10. Gerenciamento do Serviço de Segurança implantados nos Acessos Dedicados, de responsabilidade da CONTRATADA:
- 4.70.11. Todo o tráfego dos Links de Banda Larga deve ser gerenciado sob o aspecto de segurança de redes, possibilitando a aplicação e manutenção unificada de políticas através do serviço do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede;
- 4.70.12. O Serviço de segurança dos PCs da nova Rede deverá ser realizado através dos dispositivos de conectividade especificados neste Termo de Referência;
- 4.70.13. Todos os dispositivos dos PCs devem ser implementados com a família de IPV6, entregue pela ATI ao Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede.
- 4.70.14. Todos os dispositivos implementados nos PCs, devem ser visualizados no Centro Integrado de Inteligência e Segurança Cibernética e quando necessário através do Geolocalização.
- 4.71. Do captive portal
- 4.71.1. A CONTRATADA deverá ser responsável pelo fornecimento, instalação e customização inicial de um sistema de cadastro e autenticação de usuário que permita aos clientes acessarem a internet de forma segura, eficiente e uniforme em todos os órgãos do estado de PE;
- 4.71.2. A solução de captive portal deverá possuir um SSID único em todos os órgãos. Esse SSID deverá exigir o cadastro de usuário apenas na primeira conexão. Para conexões subsequentes o captive portal deverá reconhecer o dispositivo e apenas confirmar a credencial dos usuários, independente do tempo de desconexão. Caso o usuário

deseje conectar através de um novo dispositivo, um novo login deverá ser efetuado com os mesmos dados de acesso previamente utilizado em outros dispositivos. Este processo deverá acontecer de forma transparente para acessos em qualquer rede dos órgãos estaduais de Pernambuco.

4.71.3. O cadastro para autorização de acesso à internet deverá ser possível das seguintes maneiras:

- 4.71.3.1. Cadastro manual através de preenchimento de formulário pelo cliente;
- 4.71.3.2. Cadastro por login social através do Gov.br, LinkedIn, Facebook e Twitter;
- 4.71.3.3. Login social Google, através de integração com o Google Workspace via SAML;
- 4.71.3.4. Confirmação de cadastros das plataformas acima citada;
- 4.71.3.5. Possibilidade de autenticação com validação de cadastro do usuário via SMS (exclusivo);
- 4.71.3.6. Pesquisas pós-autenticação;
- 4.71.3.7. Integração com o fabricante do ponto de acesso e controladora;
- 4.71.3.8. Autenticação automática após o primeiro cadastro;
- 4.71.3.9. Acesso a um Dashboard customizado com base de dados analytics;
- 4.71.3.10. Controle de acesso ao Dashboard com níveis de permissões;
- 4.71.3.11. Timeout de acesso ao Dashboard;
- 4.71.3.12. Possibilidade de autenticação via API de integração;
- 4.71.3.13. A Ferramenta também deverá incluir um mapa de calor que identifique a quantidade de conexões feitas em cada ponto de acesso;
- 4.71.3.14. A Ferramenta deve permitir a rastreabilidade dos usuários via mapa, através do histórico de conexão dos endereços dos pontos de acesso utilizados;
- 4.71.3.15. A Ferramenta deve ser aderente as normas de (LGPD e Marco Civil da Internet);
- 4.71.3.16. Verificação de cadastro robusta, incluindo validação de CPF e de e-mail;
- 4.71.3.17. Recursos de controle de acesso incluindo bloqueio por horário, dispositivo (MAC ADDRESS) e tempo de visita;
- 4.71.4. A ferramenta deverá contemplar uma forma de validação do cadastro efetuado pelo cliente e proteção contra cadastros automatizados "efetuados por robôs". O sistema de cadastro deverá possuir uma interface web amigável e customizável pela CONTRATANTE, com auto redimensionamento para diferentes dispositivos, como celulares, tablets e computadores;
- 4.71.5. Os dados de cadastro preenchidos pelos usuários deverão ser armazenados e disponíveis para análise da CONTRATANTE em tempo real, para que possa monitorar o desempenho da plataforma e tomar decisões estratégicas com base nas informações coletadas.

## 5. Solução de monitoramento e análise de eventos de segurança - SIEM

### 5.1. Implantação e medição:

5.1.1. Solução para comportar no mínimo os itens deste termo de referência (Firewalls, PAM, WAF, EDR, NAC, IAM, NDR) durante o período do contrato, podendo sofrer alterações mediante acordo prévio entre a CONTRATADA e a CONTRATANTE técnica ATI;

5.1.2. Considerando que a utilização efetiva da solução de SIEM está diretamente vinculada à integração gradual dos ativos e serviços que enviarão LOGs ao sistema, o faturamento da solução deverá ser realizado sob demanda, com base no consumo real de EPS (Eventos por Segundo) utilizados no período faturado;

5.1.3. Embora haja uma estimativa máxima prevista para a contratação por EPS, o consumo efetivo será variável ao longo da vigência contratual, especialmente nos meses iniciais, em função do cronograma de implantação, homologação e integração dos serviços, ativos e sistemas;

5.1.4. Dessa forma, o pagamento será realizado mensalmente, com base na média mensal de EPS efetivamente utilizados, conforme apurado por ferramenta de medição automatizada fornecida e validada pela CONTRATADA, auditável pela CONTRATANTE. Não haverá pagamento por capacidade ociosa ou reserva de EPS não utilizados no período faturado, sendo o valor mensal proporcional ao consumo registrado no período de faturamento;

5.1.5. A CONTRATADA deverá garantir a capacidade técnica e de infraestrutura necessária para suportar, a qualquer tempo, a expansão do consumo até o limite contratado de EPS, conforme demanda evolutiva da CONTRATANTE, sem necessidade de recontração ou interrupção do serviço;

5.1.6. A solução de SIEM deverá armazenar os logs por no mínimo 12 (doze) meses em ambiente online, com acesso imediato para monitoramento, investigação e auditoria. O armazenamento deve contar com proteção autônoma e contínua contra ransomware, capaz de detectar e reagir automaticamente a ameaças, protegendo os dados com bloqueio, isolamento de volumes e cópias imutáveis. Caso essa funcionalidade não esteja integrada, a CONTRATADA deverá fornecer recursos adicionais (software e hardware) que garantam o mesmo nível de segurança e disponibilidade.

5.1.6.1. Após 12 (doze) meses em armazenamento online, os logs deverão ser migrados automaticamente para cold storage (armazenamento de acesso não imediato), permanecendo acessíveis para consulta, exportação ou auditoria durante toda a vigência contratual. Ambos os ambientes (online e cold storage) devem contar com proteção ativa contra ransomware, com detecção automática de ameaças e ações autônomas de defesa em tempo real, como bloqueio e preservação de dados imutáveis. Garantindo a integridade, disponibilidade e segurança dos logs armazenados em todas as fases do ciclo de vida da informação;

5.1.6.2. O cold storage poderá ser implementado de forma nativa pela solução de SIEM ou por meio de integração com a solução de guarda de logs eventualmente contratada pela CONTRATANTE, desde que atendidos os seguintes requisitos:

5.1.6.2.1. Preservação da integridade e autenticidade dos dados arquivados;

5.1.6.2.2. Suporte à recuperação de dados em até 24 horas;

5.1.6.2.3. Armazenamento seguro, com proteção contra alterações, perdas ou acessos não autorizados, incluindo proteção autônoma em tempo real contra ransomware. Deve haver conectividade total entre o armazenamento ativo e o cold storage (armazenamento de acesso não imediato), garantindo consistência, integridade e segurança dos dados em todas as fases do ciclo de vida da informação;

5.1.6.2.4. Indexação mínima que permita buscas ou filtros por data, origem e tipo de evento.

5.1.6.3. A CONTRATADA deverá apresentar, quando solicitado, evidências da retenção dos dados, plano de arquivamento e procedimentos de recuperação dos logs, conforme as melhores práticas de segurança da informação e requisitos legais aplicáveis.

5.2. Arquitetura de Implementação:

5.2.1. A solução deverá permitir implementação distribuída ou em servidores, desde que utilize acesso contínuo e resiliente aos armazenamentos, sem ponto único de falha, garantindo alta disponibilidade e integridade dos dados;

5.2.2. A arquitetura da solução permite com que seus componentes possam ser instalados em redes IPv4 e IPv6;

5.2.3. A implementação em servidores deverá permitir a utilização de armazenamento de eventos local ou através de servidor NFS para manter a integridade dos dados e cópias protegidas por defesa autônoma contra ransomware;

5.2.4. A implementação em servidores deverá permitir a capacidade de processamento da quantidade total de EPS solicitada nesse edital;

5.2.5. Deverá permitir o aumento da capacidade de processamento de EPS através da adição de novos servidores;

- 5.2.6. A solução deverá possuir coletores para coleta de logs e informações de performance em sites remotos.;
- 5.2.7. A solução deve possuir a capacidade de encaminhar qualquer evento recebido em tempo real, nos formatos syslog e netflow;
- 5.2.8. A solução deverá suportar a filtragem dos dados coletados no nível de aplicação, identificando endereço IP, tipo do dispositivo e tipo do evento;
- 5.2.9. A solução deverá permitir que todos os seus componentes sejam virtualizados;
- 5.2.10. A solução deverá suportar a virtualização nos seguintes Hypervisors: VMware ESX, Hyper-V e KVM;
- 5.2.11. A solução deverá permitir Failover e Disaster Recovery em ambiente físico e virtual.
- 5.2.12. A solução pode ser implementada em ambiente virtual ou físico de responsabilidade da CONTRATADA:
- 5.2.12.1. Deve suportar implementação em ambiente distribuídos;
- 5.2.12.2. As descobertas efetuadas devem, por padrão, atrelar novos dispositivos automaticamente à empresa/departamento/localidade a qual pertencem;
- 5.2.12.3. A solução deve permitir o monitoramento de elementos mesmo quando houver sobreposição de IP's (overlapping);
- 5.2.12.4. Deve permitir a alocação mínima (garantida) de EPS por organização, bem como alocar EPS dinamicamente entre organizações caso um número excessivo e inesperado de EPS seja recebido.;
- 5.2.12.5. Deve suportar a definição de uma quantidade máxima de devices por organização;
- 5.2.12.6. Deve ser permitido criar logins de gerenciamento limitados a uma ou mais organizações, definindo níveis de privilégio para cada.
- 5.3. A solução deverá possuir coletores Multi-tenant, permitindo assim pelo menos as seguintes formas de configuração/implementação:
- 5.3.1. Multi-tenant Agents;
- 5.3.2. Multi-tenant Event Pulling;
- 5.3.3. Multi-tenant Collector Pool.
- 5.4. Gerenciamento
- 5.4.1. A solução deverá permitir ser gerenciada através de interface gráfica Web;
- 5.4.2. Deve permitir alteração de idioma de sua interface para português;
- 5.4.3. Deve permitir o controle de acesso granular limitando o acesso a interface gráfica e a diversos níveis de dados;
- 5.4.4. Deve permitir a autenticação de usuários administrativos através dos seguintes diretórios: Local, Microsoft Active directory, LDAP, Single Sign On and SAML via OKTA;
- 5.4.5. Toda a comunicação entre os módulos deverá ser feita através de HTTPS;
- 5.4.6. Deve permitir a auditoria completa da atividade de usuários do SIEM;
- 5.4.7. Para fins de resolução de problemas, a solução deve possuir ferramentas que permitam: iniciar e parar processos individuais, executar shutdowns e reboots, validar métricas de performance do SIEM e exportar informações de evento em CSV;
- 5.4.8. A solução deve permitir a visualização de usuários que estiverem logados no sistema, atividades de consulta de usuários e usuários bloqueados;
- 5.4.9. A solução deve permitir o backup e recuperação de arquivos de configuração e conteúdo;
- 5.4.10. Deverá permitir a atualização dos componentes da solução através de interface gráfica ou através do próprio sistema operacional via linha de comando;
- 5.4.11. A respeito da capacidade em Eventos por Segundo (EPS), se o número de EPS recebido atingir o limite da licença, o SIEM deverá automaticamente gerar um incidente. Deverá ser capaz de receber um número de EPS 10% superior a quantidade de EPS licenciados por um período de até 3 minutos sem descartar nenhum evento;
- 5.4.12. A solução deverá permitir especificar um limite de EPS por coletor;
- 5.4.13. Deverá permitir acesso de suporte seguro e auditável;
- 5.5. Deve ser possível monitorar a saúde dos coletores exibindo as seguintes informações:
- 5.5.1. Nome da Organização onde coletor está instalado
- 5.5.2. Nome do Coletor
- 5.5.3. Endereço IP
- 5.5.4. Status
- 5.5.5. Saúde

- 5.5.6. Tempo em Operação (uptime)
- 5.5.7. Utilização de CPU e Memória
- 5.5.8. Versão
- 5.5.9. EPS Alocados
- 5.5.10. EPS Processados
- 5.5.11. A solução deve suportar a administração centralizada em uma implementação geograficamente distribuída onde todos os componentes são monitorados e gerenciados a partir de um portal centralizado;
- 5.5.12. Deve permitir a visualização da utilização de licenças através da interface gráfica com, pelo menos, as seguintes informações: dispositivos, EPS e agentes;
- 5.5.13. Deve permitir o arquivamento de dados baseado em políticas;
- 5.5.14. Deve permitir o “hashing” de logs em tempo real para o não repúdio e verificação de integridade;
- 5.5.15. A solução deve possuir compatibilidade e integração através de APIs documentadas e homologadas pelo fabricante, com pelo menos 30 soluções de segurança do mercado, com intuito de complementar a capacidade de análise de atividade maliciosa e resposta a incidentes;
- 5.5.16. A solução deve prover uma console e visão intuitiva para realizar investigações sobre os dados;
- 5.5.17. A solução deve possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;
- 5.5.18. A solução deve permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
- 5.5.19. A solução deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;
- 5.5.20. O fabricante da solução deve possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;
- 5.5.21. A solução deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;
- 5.5.22. A solução deve possuir integração aberta com soluções de análise de malware;
- 5.5.23. A solução deverá prover capacidades de SOC e integração com funções de NOC na mesma solução ou por integração, mantendo visão unificada de incidentes e performance;
- 5.5.24. A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;
- 5.6. Possuir suporte ao framework MITRE ATT&CK, com pelo menos as seguintes características:
  - 5.6.1. Capacidade de associar uma técnica MITRE a uma regra do SIEM (integrada ou personalizada);
  - 5.6.2. Possuir pelo menos 900 regras integradas para detectar uma ampla variedade de técnicas MITRE;
  - 5.6.3. Capacidade de atribuir técnicas e táticas às regras e pesquisar incidentes por técnicas e táticas;
  - 5.6.4. Possuir Dashboard que exibe regras associadas a uma tática ou técnica;
  - 5.6.5. Possuir Dashboard que exibe incidentes associados a uma tática ou técnica;
  - 5.6.6. Coletores
    - 5.6.6.1. A solução deverá possuir coletores para a obtenção de eventos em sites remotos;
    - 5.6.6.2. A solução não deverá restringir o número de coletores utilizados através de licença;
    - 5.6.6.3. O coletor deve suportar a instalação em Hypervisor VMware ESX ou diretamente em Bare Metal;
    - 5.6.6.4. O coletor deve possuir a capacidade de coletar os dados, realizar “parsing”, compressão e envio através de HTTPS.
    - 5.6.6.5. O coletor deve ser capaz de realizar o armazenamento local das informações caso não haja conectividade com o SIEM. Não deverá haver restrição de tempo para o armazenamento, desde que haja disponibilidade de espaço em disco;
    - 5.6.6.6. Deve permitir a atualização dos coletores através da interface gráfica do SIEM;
- 5.7. Agentes
  - 5.7.1. A solução de SIEM deverá permitir a utilização de agentes nativos ou integrados para coleta e correlação de eventos em sistemas operacionais Windows e Linux, garantindo visibilidade detalhada e contextualizada dos ativos monitorados.
    - 5.7.1.1. Os agentes poderão ser:

5.7.1.1.1. Agentes nativos do próprio SIEM, desenvolvidos e mantidos pelo fabricante;

5.7.1.1.2. Agentes de endpoint de soluções de EDR homologadas conforme o ADENDO VI - SEGURANÇA DE DATACENTER, devidamente integradas ao SIEM, desde que mantenham equivalência funcional na coleta e correlação dos eventos e logs previstos neste Termo de Referência.

5.7.1.1.2.1. Quando utilizada a integração com agente de EDR, a contratada deverá garantir a integridade e a correlação adequada dos eventos gerados.

5.7.2. A solução com o agente para Windows deverá ser capaz de coletar as seguintes informações:

5.7.2.1. Agente Básico

5.7.2.1.1. Windows Security Logs

5.7.2.1.2. Windows Application Logs

5.7.2.1.3. Windows System Logs

5.7.2.1.4. Windows DNS Logs

5.7.2.1.5. Window DHCP Logs

5.7.2.1.6. IIS logs

5.7.2.1.7. DFS logs

5.7.2.2. Agente Avançado para Windows

5.7.2.2.1. Windows Security Logs

5.7.2.2.2. Windows Application Logs

5.7.2.2.3. Windows System Logs

5.7.2.2.4. Windows DNS Logs

5.7.2.2.5. Window DHCP Logs

5.7.2.2.6. IIS logs

5.7.2.2.7. DFS logs

5.7.2.2.8. Monitoramento de Integridade de Arquivos

5.7.2.2.9. Monitoramento de Mudança de Software Instalado

5.7.2.2.10. Monitoramento de Mudança no Registro

5.7.2.2.11. Monitoramento de Arquivos

5.7.2.2.12. Monitoramento de Saída WMI

5.7.2.2.13. Monitoramento de Saída de Power Shell

5.7.2.2.14. Análise adicional de logs DNS do Windows para incluir IP de Origem, Nome do Destino, IP de Destino, Nome canônico do destino e bytes recebidos.

5.7.2.2.15. Durante a atualização do agente é evitada a perda da Configuração do Agente no Gerenciador de Agentes do Windows.

5.7.2.2.16. Limpeza automática de arquivos .SVC quando atinge um determinado tamanho.

5.7.2.2.17. O arquivo de log não é apagado após a reinicialização do agente.

5.7.2.2.18. Coletar eventos do sistema operacional relativos a uso de mídia removível.

5.7.2.2.19. A solução é capaz de executar verificações de certificado SSL.

5.7.2.2.20. Possuir capacidade de liberar arquivos de log durante a rotação de arquivos de um arquivo monitorado.

5.7.2.3. Agente Avançado para Linux

5.7.2.3.1. Sistema de Coleta (Alto Desempenho), Logs de aplicativos e logs de segurança.

5.7.2.3.2. Monitoramento de Integridade de Arquivos.

5.7.2.3.3. Monitoramento de arquivo de log do cliente

5.7.2.4. O agente deverá suportar os seguintes sistemas operacionais:

5.7.2.4.1. Windows

5.7.2.4.2. Windows Server

5.7.2.4.3. CentOS

5.7.2.4.4. Red Hat Enterprise Linux

5.7.2.4.5. Ubuntu

5.7.2.4.6. SUSE Linux Enterprise Server

5.7.2.4.7. É imprescindível que o agente seja atualizado periodicamente para garantir a compatibilidade contínua com novas versões dos sistemas operacionais. Caso qualquer versão do sistema operacional atinja o fim do suporte, o fornecedor deverá manter o suporte do agente por um período adicional de 6 meses, assegurando que o cliente tenha tempo suficiente para transitar para uma versão compatível, minimizando impactos operacionais;

5.7.2.4.8. Caso não exista um agente compatível com o sistema operacional presente no ambiente da CONTRATANTE, será permitido o uso da técnica de envio dos logs via protocolo SYSLOG para integração com a solução de SIEM, assegurando a continuidade do monitoramento e a coleta adequada de informações;

5.7.3. Os agentes deverão ser gerenciados por uma aplicação central;

5.7.4. O agente para Windows poderá ser gerenciado diretamente pela console GUI da solução, dispensando assim a necessidade de um gerenciador central.

5.7.5. A aplicação de gestão dos agentes deverá suportar os seguintes sistemas operacionais:

5.7.5.1. Windows Server

5.7.6. Os agentes deverão encaminhar logs para a aplicação de gestão dos agentes através da porta TCP 443;

5.7.7. O agente deverá permitir sua instalação através de GPO;

5.8. Dashboards e Relatórios

5.8.1. A solução deve prover, de forma nativa, Dashboards para monitoramento e correlação de eventos de segurança, incluindo visão de disponibilidade e desempenho dos ativos monitorados;

5.8.2. Deve permitir customização de dashboards com inclusão, remoção e ajuste de widgets, filtros e intervalos de atualização;

5.8.3. Deve permitir ao administrador importar e exportar Dashboards;

5.8.4. A solução deve possuir modelos de reports pré-definidos, envolvendo padrões como PCI, HIPAA, SOX, ISO e GLBA, dentre outros;

5.8.5. Deve permitir a criação de novos reports;

5.8.6. Por padrão, a solução deve possuir baselines, definindo padrões de comportamento distintos para dias de semana, finais de semana e para cada hora do dia, permitindo ao operador criar alertas para eventos que fujam ao padrão;

5.8.7. A solução deve permitir criar relatórios e correlações de eventos que associem endereços IP, usuários e ativos de rede a suas respectivas origens ou localizações lógicas, com base nas informações disponíveis na base de dados do SIEM ou integradas a outras soluções da Nova Rede Corporativa;

5.8.8. Deve possibilitar o agendamento de reports, que podem ser gerados uma única vez ou de forma recorrente, além permitir notificações quando o report for gerado e até quando ele deverá estar disponível;

5.8.9. A solução deve permitir ao administrador auditar o uso da plataforma SIEM e dos sistemas monitorados, identificando desvios de comportamento, falhas de autenticação, tentativas de acesso indevido e inconsistências nos eventos coletados, com possibilidade de geração de relatórios de conformidade;

5.8.10. A solução deve permitir exportar o report de auditoria, tanto em PDF, CSV e RTF, bem como possibilitar o agendamento;

5.8.11. Deve ser possível integrar a plataforma à sistemas de Business Intelligence;

5.9. Ingestão de Dados

5.9.1. Deve ser capaz de receber logs de diversos dispositivos diferentes, incluindo dados estruturados como também dados não estruturados;

5.9.2. Deve ser capaz de receber logs de, pelo menos, 200 dispositivos diferentes sem necessidade de criação de parsers customizados;

5.9.3. Deve ser capaz de receber logs de dispositivos de segurança de rede, tais como: roteadores, switches, dispositivos de prevenção contra intrusão, web proxies, gateway de proteção de e-mail, DNS e servidores DHCP de diversos fabricantes;

5.9.4. Deve ser capaz de receber logs de sistemas operacionais de diversos fabricantes;

5.9.5. Deve ser capaz de receber logs de aplicações de segurança, tais como: servidores web, servidores de aplicações, banco de dados e sistemas de proteção de endpoints;

5.9.6. Deve ser capaz de receber logs via syslog, traps SNMP, Netflow, SFlow, JFlow, FTP e SCP;

- 5.9.7. Deve ser capaz de obter dados através de JDBC, JMX, Cisco SDEE e CheckPoint LEA;
- 5.9.8. Deve ser capaz de coletar qualquer arquivo de logs de sistemas operacionais Windows através de agente próprio;
- 5.9.9. Deve permitir que arquivos de log formatados em CSV personalizados possam ser carregados através da console GUI para análise mais detalhada
- 5.9.10. Deve ser capaz de obter logs de aplicações Cloud através de API's específicas, tais como: Google Apps e Office 365;
- 5.9.11. Deve ser capaz de inserir contexto aos dados obtidos;
- 5.9.12. Deve ser capaz de realizar o parsing, armazenar, analisar e exibir conteúdo de pacotes TCP/UDP em eventos que são gerados por sistemas de prevenção de intrusão;
- 5.9.13. Capacidade de analisar arquivos de log de um diretório em nós da solução.
- 5.9.14. Permitir ao usuário analisar arquivos PCAP. Incluindo os atributos IP, TCP / UDP e HTTP.
- 5.10. Enriquecimento de Dados
- 5.10.1. Deve ser capaz de obter informações de uma variedade de fontes públicas e privada de dados para enriquecer os dados obtidos;
- 5.10.2. Deve fornecer uma base de dados de localização de endereços IP (GeoIP) e ser capaz de obter informações de cada endereço de IP público recebido nos eventos, sendo cada evento enriquecido com informações de localização geográfica, tais como: cidade, país, ASN, longitude e latitude;
- 5.10.3. Deve permitir que os administradores da solução possam pesquisar informações sobre endereços IP e reputação de domínio de qualquer website público;
- 5.10.4. Deve permitir o agrupamento de ativos de rede de forma automática e realizar a sua classificação através de segmento de rede, sistema operacional, aplicação etc.;
- 5.10.5. Deve permitir a criação de grupos customizados e regar de mapeamento;
- 5.10.6. Deve ser capaz de utilizar informações de serviços de DHCP e de diretório para gerar alertas e relatórios;
- 5.10.7. Deve ser capaz de monitorar a atividade de servidores DNS com o objetivo de detecção de malwares;
- 5.10.8. Possui capacidade de verificações de reputação (Indicadores de compromisso) como IP, Domínio, URL e Hash
- 5.11. Classificação de Dados
- 5.11.1. Deve ser capaz de classificar diferente tipos de dados coletados para auxiliar na sua utilização em consultas analíticas ou "ad hoc" por analistas do SOC. Também deve ser capaz de classificar esses dados com base em sua sensibilidade ou proteção de segurança / privacidade necessários;
- 5.11.2. Deve ser capaz de agrupar dados semelhantes;
- 5.11.3. A solução deve ser capaz de analisar o tipo do evento e atribuí-lo a um grupo de tipo de evento;
- 5.11.4. A solução deve possuir, pelo menos, 200 grupos de tipo de eventos incorporados;
- 5.11.5. Deve permitir a utilização de expressões regulares para fazer correspondência nos dados recebidos;
- 5.11.6. Permite a definição de tags, que podem ser usadas em regras e incidentes.
- 5.12. Armazenamento de Dados, Gerenciamento e Arquivamento
- 5.12.1. Deve prover integridade dos logs através de criptografia dos dados;
- 5.12.2. Deve permitir a execução de relatórios para validar a integridade dos dados e identificar possíveis blocos de dados que tenham sido modificados;
- 5.12.3. A solução deve prover ferramentas integradas para gestão dos dados;
- 5.12.4. A solução deve permitir armazenamento de dados on-line e off-line;
- 5.12.5. A solução deve permitir o gerenciamento da retenção de logs através de políticas. Deve permitir a criação de regras baseadas na identificação do cliente, tipo do evento, dispositivos e especificar o número de dias no armazenamento on-line e off-line;
- 5.12.6. A solução de SIEM deve suportar integração técnica e interoperabilidade com plataformas de análise e Big Data da Administração Pública, permitindo o envio, recepção e arquivamento em tempo real de eventos, por meio de barramentos de mensagens, APIs RESTful ou conectores compatíveis;
- 5.12.6.1. A CONTRATADA deverá prover e manter os conectores, scripts ou APIs necessários à integração, sempre que fornecidas pela CONTRATANTE as especificações técnicas do ambiente de destino.

5.12.6.2. Caso a integração dependa de protocolos específicos, a CONTRATADA deverá assegurar compatibilidade com pelo menos um barramento de mensagens de padrão aberto ou API RESTful, garantindo interoperabilidade e integridade dos dados.

5.12.7. Deve ser capaz de tornar anônimos ou mascarar campos sensíveis (PII) nos logs analisados, incluindo endereços IP, nomes de usuário, hosts, MACs e e-mails, conforme as boas práticas de proteção de dados e privacidade.

5.12.8. Deve permitir o armazenamento e consulta indexada dos eventos em mecanismos de busca e análise estruturados, devendo suportar soluções baseadas em banco relacional, NoSQL ou sistemas de indexação distribuída;

5.12.9. O sistema de armazenamento deverá ser escalável e distribuído, podendo ser implementado em ambiente local ou em nuvem, com suporte a topologias de nó único ou cluster, conforme a arquitetura da Administração Pública.

5.12.10. O arquivamento de eventos deve suportar sistemas de arquivos distribuídos ou object storage, assegurando escalabilidade, resiliência e integridade dos dados armazenados.

### 5.13. Analytics

5.13.1. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

5.13.2. A solução deve possibilitar a busca de eventos históricos e em tempo real;

5.13.3. Efetuar a análise dos eventos em tempo real;

5.13.4. Realizar a correlação dos eventos antes dos dados serem armazenados na base de dados;

5.13.5. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

5.13.6. A solução deve fornecer atualizações predefinidas de regras de correlação e atualizações de software;

5.13.7. A solução deve suportar a realização de um filtro dos dados coletados antes de realizar a correlação;

5.13.8. A solução deve possuir mais de 500 regras pré-definidas incluindo regras de segurança, disponibilidade/performance e mudanças de configuração;

5.13.9. Permitir a criação de novas regras e a edição das existentes;

5.13.10. A solução deve permitir a criação de regras de correlação unificando todos os eventos, como logs de segurança, disponibilidade, performance, storage e mudanças de configurações;

5.13.11. A solução deve ser capaz de gerar alertas automáticos e notificações quando alcançar os limites de dados coletados, sem descartar os dados;

5.13.12. Deve permitir buscas simples em raw data (não estruturadas), através de palavra-chave, bem como definir quais campos serão apresentados no resultado, o período da busca e a organização (ambientes multi-tenant);

5.13.13. Deve permitir salvar a consulta, definindo o tempo que ela estará disponível para uso futuro.

5.13.14. Deve permitir salvar e enviar por e-mail o resultado da busca, como PDF e CSV;

5.13.15. Deve possibilitar buscas estruturadas, baseadas em atributos, inserindo múltiplas condições. Deve haver opção para agrupamento de eventos;

5.13.16. Ao operador será possível definir: de qual elemento ele deseja verificar os logs, eventos cuja ação tomada pelo dispositivo foi "negar" e filtrar por dispositivos presentes em uma determinada categoria da base de conhecimento, de forma condicional (AND) ou excludente (OR);

5.13.17. Deve possibilitar uma busca que mostre mudanças em logins/grupos do domínio não executadas por usuários de um determinado grupo de admins do domínio;

5.13.18. O uso de expressões regulares deve ser permitido nas buscas;

5.13.19. A depender do tipo de informação buscada, a solução deve exibir gráficos nos formatos de: tendência, tabela, barra, dispersão (correlação entre duas variáveis) e árvore (análise de componentes dominantes) e heat map (intensidade);

5.13.20. Deve permitir, de forma simples, converter uma busca histórica em tempo real, sem que haja necessidade de reinserir os mesmos filtros para essa nova busca;

5.13.21. A partir de uma busca, deve ser possível criar uma regra reaproveitando os filtros já definidos, e gerar um alerta, a fim de notificar o administrador sobre um determinado evento;

5.13.22. As buscas simples devem aceitar os seguintes operadores: AND, OR e AND NOT;

- 5.13.23. As buscas estruturadas devem aceitar os seguintes operadores: =, !=, >, >=, IN, IN, BETWEEN, IS, CONTAINS e REGEXP;
- 5.13.24. Deve listar, por padrão, atributos que podem ser utilizados nas queries. Adicionalmente, deve permitir buscar atributos presentes na base de conhecimento, filtrando por funcionalidade e equipamento;
- 5.13.25. Deve mostrar, quando possível, a localização geográfica de um IP (origem ou destino), tais como: país, cidade, estado, longitude e latitude;
- 5.13.26. Deve exibir, em formato de mapa, os resultados da query no que tange países envolvidos no tráfego resultante do filtro;
- 5.13.27. O administrador deve ser capaz de salvar filtros de pesquisas, que podem ser reutilizados no futuro;
- 5.13.28. A solução deve suportar análise de dados históricos de segurança, eventos, dispositivos e sistemas ou dados de aplicativos de longo prazo;
- 5.13.29. A solução deve possibilitar o uso de "queries" em formato "SQL like" para minimizar a curva de aprendizado para administradores familiarizados em banco de dados relacionais;
- 5.13.30. A solução deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;
- 5.13.31. A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
- 5.13.32. A solução deve prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;
- 5.13.33. A solução deve possuir a capacidade de navegação contínua sobre os dados em formato "drill down", sem a obrigatoriedade de realizar pesquisas avançadas;
- 5.13.34. A solução deve possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;
- 5.13.35. A solução deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;
- 5.13.36. A solução deve ser capaz de suportar análises preditivas;
- 5.13.37. A solução deve ser capaz de suportar análises avançadas como anomalias estatísticas;
- 5.14. Monitoramento
- 5.14.1. A solução deve suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;
- 5.14.2. Para casos em que será utilizado o WMI como coletor de logs, a solução deverá ser capaz de criar filtros para obtenção dos mesmos. Estes filtros podem contemplar Todos os Logs ou logs como: Eventos de Sistema, Segurança ou Aplicação
- 5.14.3. A solução deve automaticamente classificar os dispositivos por tipo ou grupos, sendo depois referenciados em relatórios, regras, queries e outros;
- 5.14.4. A solução deve suportar a monitoração de dispositivos como disponibilidade, mudanças de configuração, performance e outros;
- 5.14.5. A solução deve suportar no mínimo os protocolos: TCP, UDP baseado em syslog, Netflow, Sflow, Jflow, SNMP trap, JDBC, Cisco SDEE, Microsoft WMI, banco de dados JDBC para Oracle, banco de dados do servidor SQL, banco de dados IBM DB2, JDBC para Snort, JDBC para McAfee Foundstone, SSH / telnet para arquivos de configuração, VMware SDK para descoberta VMware e coleção de logs. Para as métricas de desempenho e disponibilidade, o SIEM deve usar SNMP, JMX, Windows WMI, JDBC para vários bancos de dados, VMware SDK;
- 5.14.6. A solução deve suportar a monitoração de seus próprios processos internos com possibilidade de geração de alertas;
- 5.15. Alertas e Incidentes
- 5.15.1. Como resultado de regras, deverá ser capaz de executar ações automáticas, tais como:
- 5.15.1.1. Executar script, como reiniciar um processo, remover arquivos de um diretório, mudança de configuração ou execução de comandos dentro outros.
- 5.15.1.2. Criação de um TRAP SNMP.
- 5.15.1.3. Enviar e-mail para uma lista de usuários.
- 5.15.1.4. Enviar mensagens para o usuário conectado no console.
- 5.15.1.5. Criar um ticket no sistema de ticketing interno ou externo;

- 5.15.1.6. A solução organiza os incidentes em categorias e subcategorias, permitindo assim que esses campos possam ser usados em pesquisas.
- 5.15.1.7. A solução deve permitir a criação e acompanhamento de Incidentes de Segurança, com no mínimo as seguintes características:
- 5.15.1.8. Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
- 5.15.1.9. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- 5.15.1.10. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;
- 5.15.1.11. Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
- 5.15.1.12. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
- 5.15.1.13. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- 5.15.1.14. Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2); - Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux;
- 5.15.1.15. Possuir integração nativa com ferramenta de gerenciamento de incidentes externa;
- 5.15.2. A solução deverá possuir atributos para resolução de incidentes, com as seguintes opções:
- 5.15.2.1. Positivo
- 5.15.2.2. Falso Positivo
- 5.15.2.3. Aberto
- 5.15.2.4. Os atributos de resolução de incidentes podem ser usados em pesquisas.
- 5.15.2.5. Deve ser capaz de encaminhar logs para um sistema externo usando o formato Common Event Format (CEF) sobre UDP ou TCP
- 5.15.2.6. Deve permitir que os Incidentes detectados sejam visualizados através de todas as categorias definidas pela Matrix Enterprise do MITRE ATT&CK.
- 5.15.2.7. Permite a integração com soluções externas de incidentes/Secops via JSON REST API
- 5.16. CMDB
- 5.16.1. A solução deve possuir ou integrar-se à sistemas de CMDB (Configuration Management Database), atendendo de forma nativa ou através de composição os requisitos listados nesse documento;
- 5.16.2. A solução deve prover informações detalhadas sobre devices, aplicações, usuários e qualquer outro componente de rede compatível com protocolos de gerência (SNMP, SYSLOG, NETFLOW etc.), de forma nativa. Para elementos desconhecidos, deve ser possível a criação de scripts que permitam a correta identificação deles;
- 5.16.3. Deve permitir realizar um discovery da rede, de forma dinâmica, evitando a adição manual dos elementos ao CMDB;
- 5.16.4. O discovery deve promover categorização dinâmica, alocando os elementos nos devidos grupos;
- 5.16.5. Deve informar: nome do dispositivo gerenciado, IP, tipo, versão, protocolo utilizado para coleta dos dados e organização a qual pertence;
- 5.16.6. Deve ser capaz de mostrar os elementos gerenciados de forma tabelada e em topologia, posicionando cada elemento conforme configurações/logs analisados;
- 5.16.7. Deve mostrar estatísticas relativas à performance do dispositivo, tais como: tráfego, memória, disco e CPU;
- 5.16.8. Ao selecionar um dispositivo específico, deve permitir visualizar seus logs em tempo real (analytics), sem necessidade de criar um filtro manual para tal;

5.16.9. Deve permitir agregar dispositivos e aplicações que suportam um determinado serviço dando ao operador uma visão macro sobre o serviço em si;

5.16.10. Quando aplicável, deve informar ao operador o software, hardware e configuração utilizada pelo dispositivo;

5.16.11. De forma simples, deve informar os incidentes e eventos de disponibilidade, performance e segurança relacionados a um elemento monitorado.;

5.16.12. Deve prover, por padrão, listas de domínios (threat feeds) conhecidos por gerar spam, suportar botnets, participar de ataques DDoS e conter malwares. O operador deve ser capaz de adicionar novas listas;

5.16.13. A solução deve prover uma lista de credenciais padrão utilizadas por equipamentos. Caso a plataforma identifique um dispositivo que as use, um alerta deve ser gerado;

5.16.14. Ao operador deve ser possível agrupar em listas elementos que devem ser acompanhados com maior atenção. Exemplo: logins que são constantemente bloqueados e máquinas cujos discos apresentam falta de espaço;

5.16.15. Deve prover reports que informem dispositivos aprovados no CMDB, usuários descobertos, sistemas operacionais utilizados, hardwares, serviços em execução em máquinas Windows, softwares e patches instalados, dentre outros;

#### 5.17. Controle de Acesso

5.17.1. Dado o grande escopo abordado pela solução, se torna difícil a um único administrador gerenciar performance, disponibilidade, mudanças e segurança em equipamentos de rede, servidores e aplicações. A solução ofertada deve permitir a divisão de tarefas por função (RBAC), localidade/área, dispositivos/sistemas e nível de criticidade da informação;

5.17.2. A solução deve possuir controle de acesso baseado em perfis de usuários e ser multi-tenant;

5.17.3. Por padrão, a plataforma deve disponibilizar os seguintes tipos de gerência: escrita e leitura, equipamentos de rede, sistemas, servidores, Windows, segurança, helpdesk e apenas leitura.

5.17.4. Deve permitir a criação de funções customizadas;

5.17.5. Deve suportar o uso de logins locais e externos para autenticação na gerência da solução. Nesse último caso: LDAP, RADIUS e SAML via Okta;

5.17.6. Suporte à duplo fator de autenticação em logins de gerência;

#### 5.18. Threat Intelligence

5.18.1. A solução deve suportar a obtenção de informações de inteligência de ameaças.

5.18.2. Deve ser capaz de obter, pelo menos, as seguintes informações: domínio de malware, IP de malware, URL de malware, Hash de malware, redes anônimas incluindo proxies abertos e VPN, User Agent de malware;

5.18.3. A solução deverá prover importação via STIX/TAXII;

5.18.4. Deve ser capaz de obter informações de inteligência de ameaças nativamente das seguintes fontes: Emerging Threat, Malware Domain List, Zeus e Threat Stream (Anomali);

5.18.5. Deve ser capaz de obter informações de inteligência de ameaças nativamente da fonte AlienVault OTX pelos menos os seguintes itens:

5.18.6. IPs Maliciosos

5.18.7. Urls Maliciosas

5.18.8. Hashs de Ameaças

#### 5.19. UEBA

5.19.1. A solução deve possuir capacidade UEBA (User Entity Behavioral Analytics) para usuários Windows.

5.19.2. Deve ser capaz de monitorar eventos de usuário, máquina, arquivos, processos e unidade de montagem de forma a apontar potenciais riscos de segurança.

### 6. Solução de automação de resposta a incidentes de segurança - SOAR

#### 6.1. Case Management

6.2. Alertas e incidentes devem ser tratados separadamente, cada um em seu próprio módulo na interface do usuário

- 6.3. Atributos de cada módulo (campos), como nome, gravidade, do módulo alerta, deve ser personalizável para que os usuários possam adicioná-los ou removê-los, além disso os usuários devem poder criar, modificar e excluir seus próprios atributos personalizados em qualquer módulo do sistema;
- 6.4. A solução deve permitir que cada registro seja correlacionado e vinculado a qualquer outro registro no sistema, incluindo tipos personalizados de registros que os próprios usuários definem;
- 6.5. A solução deve fornecer a capacidade de agrupar registros semelhantes com base em valores de campo semelhantes;
- 6.6. A solução deve ter um mecanismo de previsão baseado em aprendizado de máquina que prevê valores de campos com base em dados históricos. O escopo da previsão de aprendizado de máquina deve abranger todos os módulos do produto, incluindo os built-in (como alertas, incidentes, indicadores) e personalizados;
- 6.7. A solução deve incluir um recurso de detecção de e-mail de phishing baseado em IA;
- 6.8. A visualização de cada módulo deve ser personalizável por meio de um modelo de visualização que define a posição de cada campo e widget;
- 6.9. O sistema deve fornecer uma funcionalidade de pesquisa global que permita ao analista pesquisar palavras-chave em todo o sistema em todos os módulos;
- 6.10. A interface Web para o usuário deve oferecer a possibilidade de vincular vários registros a um ticket ou criar registros todos juntos e vinculá-los ao ticket atual. Os registros podem ser, mas não limitados a: Artefatos, Tarefas, Sala de Guerra, Usuários, Campanhas, Buscas, Ativos, Alertas, Anexos, E-mails e Incidentes;
- 6.11. Os tickets devem ter um atributo de prioridade que possa ser usado para classificá-los enquanto os exibe na interface do usuário da Web;
- 6.12. O escalonamento de tickets deve ser possível manualmente por meio da interface Web ou automaticamente por meio de um fluxo de trabalho de automação que pode aplicar qualquer lógica como condição antes de escalonar o ticket;
- 6.13. Deve incluir um gerenciamento de crises da sala de guerra para permitir a colaboração entre equipes durante as crises, a sala de guerra deve poder ser criada manualmente ou escalando um ticket;
- 6.14. Tickets, artefatos, anexos e módulos customizados devem dar aos analistas um meio de comunicar por texto (comentários) cada mensagem deixada por um analista, ou um workflow de automação deve permanecer como atributo do registro onde foi criado. Além disso, os comentários devem suportar as funcionalidades abaixo:
- 6.14.1. Os comentários podem ser texto simples ou rich text;
- 6.14.2. Os analistas podem ser marcados em um comentário para atrair sua atenção;
- 6.14.3. Um comentário pode ser usado para executar ações;
- 6.14.4. Comentários são compatíveis com tags genéricas;
- 6.14.5. Os comentários suportam anexos de arquivos;
- 6.14.6. Comentários são compatíveis com RBAC;
- 6.15. O sistema deve permitir que o analista execute a Análise de Causa Raiz com uma média de correlação gráfica;
- 6.16. A correlação gráfica deve estar disponível para diferentes tipos de registro, como ativos, vulnerabilidades, alertas e incidentes;
- 6.17. A solução deve se integrar ao framework MITRE ATTACK fornecendo enriquecimento tático, análise de ameaças, investigação de incidentes e sugestões de remediação;
- 6.18. O sistema deve permitir que o analista realize a Análise Pós-Incidente (PIA – relacionada ao tratamento de incidentes);
- 6.19. O sistema deve suportar tíquetes de mapeamento para fases da cadeia de morte cibernética;
- 6.20. A solução deve ter um recurso de gerenciamento de filas personalizável que ofereça suporte a atribuições automatizadas de alertas/incidentes/tarefas para vários grupos de usuários;
- 6.21. A solução deve oferecer suporte a um sistema de rastreamento de Acordo de Nível de Serviço configurável dentro da estrutura de gerenciamento de caso para que o tempo de conclusão de vários marcos possa ser identificado e relatado;
- 6.22. O gerenciamento de casos deve oferecer suporte a anexos de arquivo;
- 6.23. A solução deve ser capaz de extrair artefatos (IP, URL, Domínio) de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs. Os artefatos extraídos devem estar vinculados ao registro do arquivo de onde foram extraídos;

- 6.24. A solução deve ser capaz de extrair metadados de arquivos (autor, timestamp) juntamente com uma visualização de conteúdo como texto ou HTML de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs;
- 6.25. A solução deve permitir que o analista edite campos diretamente na WebUI se o RBAC estiver configurado para;
- 6.26. As notificações devem ser flexíveis e usar vários canais, como interface do usuário, e-mail e várias integrações com serviços de conferência, como MS Teams e Slacks;
- 6.27. Filas de emissão de bilhetes, gerenciamento de turnos e entrega devem ser um recurso integrado. A solução deve fornecer um sistema de filas onde os analistas são designados com base em sua disponibilidade (turno);
- 6.28. Deve permitir que os usuários definam condições para controlar a visibilidade dos objetos na interface do usuário. Isso não está relacionado à filtragem de registros, mas às condições de exibição para objetos de página específicas, como guias;
- 6.29. Solução deve criar uma linha do tempo automática para alertas e incidentes e salas de guerra (no mínimo), de forma a permitir visualizar os eventos que relacionados em uma linha de tempo;
- 6.30. Para um alerta, incidente, indicador, sistema devem mostrar correlações. Para um alerta, deve-se apresentar indicadores, informações do Mitre, características do alerta, conteúdo do alerta, anexos (se possui), SLA do alerta, possibilidade de escalar para Incidente, dentre outros;
- 6.31. Solução deve permitir a construção de WarRooms (salas de guerra) para gestão de casos críticos de ataques cibernéticos. A ala de guerra deve permitir atribuir tarefas aos seus integrantes, monitorar alertefartos ligados ao ataque, monitorar SLA e linha do tempo de ações da sala de guerra, permitir colaboração por intermédio de Zoom, slack, Teams ou outros métodos populares;
- 6.32. Solução deve permitir reduzir a quantidade de falsos positivos, permitindo maior eficiência operacional ao SOC;
- 6.33. Automation Workflows (Playbooks);
- 6.34. O número de manuais fornecidos pelo fornecedor, incluindo casos de uso, amostras e outros relacionados a conectores, deve ser superior a 4.500;
- 6.35. Os playbooks devem ser agrupados em pastas com a capacidade de exportar ou importar a pasta inteira de playbooks diretamente da WebUI;
- 6.36. Os playbooks devem ter propriedades que permitam que determinados playbooks sejam executados antes de outros na fila com base em sua importância;
- 6.37. Os manuais devem ter acionadores condicionais, portanto, os manuais não serão acionados a menos que condições específicas sejam atendidas. Os operadores abaixo devem ser suportados:
- 6.37.1. Igual;
- 6.37.2. Não igual;
- 6.37.3. Menor que/Menos que ou igual;
- 6.37.4. Maior que/maior que ou igual;
- 6.37.5. Está na lista;
- 6.37.6. Não está na lista;
- 6.37.7. É nulo.
- 6.38. Os playbooks devem ser compatíveis com os seguintes acionadores:
- 6.38.1. Manual: O analista pode executar um manual manualmente a partir da WebUI;
- 6.38.2. No registro Criar/Atualizar/Excluir: quando um registro (Alerta, indicador, incidente) é criado ou modificado;
- 6.38.3. Via API: quando o SOAR recebe uma solicitação HTTP com parâmetros específicos, ele executa um playbook específico;
- 6.38.4. Referenciado: um playbook deve poder ser executado por outro playbook fornecendo seus parâmetros necessários.
- 6.39. O sistema deve fornecer uma interface gráfica do usuário para o construtor de playbook, onde os usuários podem usar o mouse para arrastar e soltar componentes no designer. Além disso, o designer do playbook deve conter um painel assistente para buscar todas as variáveis disponíveis e um painel utilitário para ajudar o analista a manipular os dados dentro do playbook;
- 6.40. O designer do playbook deve permitir que o analista reverta e refaça ações, portanto, se uma etapa for criada, por exemplo, uma reversão excluiria a ação e um "refazer" a traria de volta;

- 6.41. A solução deve permitir que o usuário execute o playbook de dentro do playbook designer e teste sua execução com registros do ambiente ou o último registro com o qual o playbook foi executado;
- 6.42. Os analistas devem ter a capacidade de exportar e importar Playbooks individualmente, incluindo várias versões do playbook;
- 6.43. A solução deve suportar a criação, modificação e exclusão de variáveis globais acessíveis por todos os manuais. As variáveis globais devem ser editáveis por meio de playbooks ou por meio da WebUI;
- 6.44. O sistema deve fornecer um histórico visual de execução do playbook que identifica a saída, entrada e configuração de cada etapa;
- 6.45. O nível de log dos playbooks deve ser configurável globalmente (todo o sistema) e localmente para cada playbook.
- 6.46. As ferramentas de depuração devem estar disponíveis, prontas para uso no designer do playbook. O depurador deve ser capaz de usar dados da execução anterior do playbook ou dados fornecidos pelo analista;
- 6.47. O RBAC deve abranger manuais e fluxos de trabalho de automação;
- 6.48. A solução deve fornecer mensagens de erro detalhadas quando a execução de um playbook falhar e permitir a reinicialização do playbook a partir da etapa em que o mesmo falhou;
- 6.49. As etapas de decisão dentro dos manuais devem ser flexíveis o suficiente para acomodar condições complexas, incluindo aquelas com aritmética, comparação e operador lógico abaixo:
- 6.49.1. Igual (Compara dois objetos para igualdade)
- 6.49.2. Não igual (Compara dois objetos para desigualdade)
- 6.49.3. Maior que (verdadeiro se o lado esquerdo for maior que o lado direito)
- 6.49.4. GT/igual (verdadeiro) se o lado esquerdo for maior ou igual ao lado direito)
- 6.49.5. Menos do que (verdadeiro se o lado esquerdo for mais baixo que o lado direito)
- 6.49.6. Menor ou igual (verdadeiro se o lado esquerdo for menor ou igual ao lado direito)
- 6.49.7. "e" (Retorna verdadeiro se os operandos esquerdos e direito forem verdadeiros)
- 6.49.8. "ou" (Retorna verdadeiro se o operando esquerdo ou direito for verdadeiro)
- 6.49.9. não (negar uma declaração)
- 6.49.10. Adição (Adiciona dois objetos juntos)
- 6.49.11. Subtração (Subtraia o segundo número do primeiro)
- 6.49.12. Divisão (Divida dois números)
- 6.49.13. Módulo (Calcular o resto de uma divisão inteira)
- 6.49.14. Multiplicação (Multiplique o operando esquerdo pelo direito)
- 6.49.15. potência (Elevar o operando esquerdo à potência do operando direito)
- 6.49.16. Condições como:
- 6.49.17.  $(\text{Variável1} + \text{variável2}) / 2 > \text{variável3}$
- 6.49.18.  $((\text{Variável1} + \text{variável2}) / 2 > \text{variável3})$  ou  $(\text{Variável4} / \text{variável5}) < 2$
- 6.49.19. Deve ser possível utilizar as condições do item 7.83 e 7.84 sem usar qualquer linguagem de programação explícita.
- 6.49.20. Em relação as condições dos itens 7.83 e 7.84, a etapa de tomada de decisão deve ter uma opção para definir uma próxima etapa padrão caso todas as condições falhem
- 6.50. Os playbooks devem ser chamados de outros playbooks;
- 6.51. Os analistas devem ser capazes de usar a linguagem de programação Python com pelo menos formatação automática e destaque de sintaxe diretamente em um playbook, caso desejem. O administrador da solução SOAR deve ser capaz de limitar os módulos que podem ser usados nos scripts python;
- 6.52. A solução deve oferecer suporte ao gerenciamento de conflitos de registros e permitir que os usuários selecionem quais campos podem ser substituídos;
- 6.53. A solução deve fornecer um editor de Rich text em sua WebUI para permitir que os analistas editem texto formatado com tabelas, imagens e vídeos;
- 6.54. As etapas do playbook devem ser configuráveis para interromper a execução do playbook se ocorrer um erro no nível da etapa ou passar a mensagem de erro para a próxima etapa e continuar;
- 6.55. O gerenciamento de playbooks deve permitir que os analistas editem playbooks em massa com a capacidade de executar as funções abaixo:

- 6.55.1. Alterar status (Playbook Ativo ou Desativado);
- 6.55.2. Clone o(s) playbook(s) selecionado(s);
- 6.55.3. Mover o(s) manual(ais) selecionado(s) para um grupo diferente;
- 6.55.4. Alterar o nível de registro para o(s) playbook(s) selecionado(s);
- 6.55.5. Exportar o(s) playbook(s) selecionado(s);
- 6.55.6. Qualquer playbook dentro da solução proposta deve ser escalonável para ser executado em um intervalo específico com a capacidade de impedir sua execução se uma instância anterior ainda estiver em execução.
- 6.56. Dentro do designer de playbook, os analistas devem ser capazes de:
  - 6.56.1. Clonar uma etapa;
  - 6.56.2. Copiar Cola uma etapa ou um grupo de etapas no mesmo manual ou em um diferente;
  - 6.56.3. Alinhar as etapas em um diagrama vertical ou horizontal;
  - 6.56.4. Selecione uma etapa ou um grupo de etapas e exclua-os;
- 6.57. Os manuais devem ser capazes de obter dados e aprovações por e-mails com a capacidade de realizar uma ação específica se ocorrer um tempo limite;
- 6.58. Solução deve permitir o versionamento de Playbooks;
- 6.59. Solução deve permitir trocar as prioridades de playbooks;
- 6.60. Solução deve permitir pesquisar histórico de playbooks executados, assim como obter KPIs de quantidade de playbooks executados, número de ações executadas.
- 6.61. Solução deve ter suporte a construção automática de playbooks por inteligência artificial. Por exemplo, analista cibernético pede para IA criar playbook que faz enriquecimento de um IP levando em consideração fontes X, Y e Z e então, IA gera o playbook, que pode depois ser modificado pelo analista.
- 6.62. Solução deve ser capaz de sugerir playbooks para serem executados para remediar ameaças detectadas em alertas e incidentes, usando inteligência artificial.
- 6.63. Solução deve permitir a execução de simulações de ataques, a fim de monitorar a forma como o time do SOC responde a incidentes. Solução deve permitir instalar cenários de simulação diversos, além de poder executar mesmo cenário de simulação inúmeras vezes.
- 6.64. Solução deve fazer a triagem automática de alertas, seguindo com o enriquecimento de indicadores extraídos, além de potencialmente mudar a severidade dos alertas em decorrência da gravidade detectada a partir de seu conteúdo (tudo de forma automática).
- 6.65. Solução deve permitir diminuir o MTTR (Mean Time to Response) através de playbooks pré-configurados para resposta;
- 6.66. Os playbooks podem ser ativados por sistemas externos a solução através de API;
- 6.67. Solução deve ter suporte a playbooks que pedem aprovação em certo passo/etapa para continuar com os próximos passos;
- 6.68. Solução deve permitir Playbooks que referenciam outros playbooks (playbooks aninhados).
- 6.69. Licensing
  - 6.69.1. A solução deve suportar licenciamento quando implantada em redes air-gapped;
  - 6.69.2. O Playbook Editor deve permitir que os usuários criem vários grupos recolhíveis de etapas e notas para melhorar a legibilidade;
  - 6.69.3. Os playbooks devem oferecer suporte a uma etapa de espera configurável com uma quantidade de tempo definida ou uma condição que, se atendida ou um tempo limite configurável atingido, o playbook encerrará a espera e prosseguirá para a próxima etapa;
  - 6.69.4. A solução deve fornecer um portal de conteúdo público e de dentro de sua interface de usuário da Web para baixar e consumir componentes do produto, como:
    - 6.69.4.1. Painéis
    - 6.69.4.2. Relatórios
    - 6.69.4.3. Manuais
    - 6.69.4.4. Widgets personalizados
    - 6.69.4.5. Integrações (conectores)
    - 6.69.4.6. Módulos e extensões do produto

- 6.69.5. A solução deve ter pelo menos 390 Integrações com sistemas de terceiros, como por exemplo, soluções de SIEM, serviços de inteligência de ameaças e Firewalls;
- 6.69.6. O sistema deve ter um mecanismo de atualização de conteúdo in-life independente das atualizações de firmware da solução. As integrações com sistemas de terceiros devem ter suas próprias atualizações utilizáveis em qualquer versão suportada do firmware da solução;
- 6.69.7. A interface do usuário da Web deve incluir assistentes para auxiliar os usuários na criação de conteúdo, seja esse conteúdo uma integração, uma extensão de produto ou um widget personalizado
- 6.69.8. Cada integração deve ser documentada online;
- 6.69.9. O fornecedor deve fornecer um SDK de integração para permitir que os clientes desenvolvam suas próprias integrações;
- 6.69.10. O sistema deve fornecer um assistente de ingestão de dados amigável para configurar a ingestão de dados de sistemas de terceiros;
- 6.70. Integrations/Content
- 6.70.1. O sistema deve fornecer um painel de integridade que indica se todas as integrações com os sistemas de terceiros estão íntegras;
- 6.70.2. As ações dos conectores devem estar sujeitas ao RBAC, portanto, apenas perfis definidos podem usar ações definidas;
- 6.70.3. O sistema deve permitir que o analista execute qualquer ação do conector por meio do SOAR WebUI sem usar fluxos de trabalho de automação (playbooks);
- 6.70.4. A solução deve permitir que os usuários criem, editem e personalizem integrações e automações de forma visual e simplificada, por meio de interface gráfica ou ambiente low-code, sem necessidade de desenvolvimento avançado. As integrações existentes devem ser editáveis e versionáveis, devendo a plataforma suportar também o uso de SDK ou API abertos para casos de desenvolvimento avançado;
- 6.70.5. A solução deve permitir a instalação local de novas integrações;
- 6.70.6. A solução deve permitir múltiplas configurações para um mesmo conector ou integração, possibilitando o uso de credenciais, parâmetros ou endpoints distintos, conforme o ambiente ou sistema monitorado;
- 6.70.7. Cada conector deve vir acompanhado de uma documentação, que explica casos de uso e detalhes da instalação dos conectores;
- 6.70.8. Solução deve permitir ao analista construir seus conectores (caso a solução ainda não disponibilize conectores que o analista deseja);
- 6.70.9. Solução já deve trazer conectores prontos para uso para, no mínimo os seguintes tipos de appliances/soluções: Network, Firewall, Ticket Management, SIEM, Gestão de vulnerabilidade, Endpoint Security, Threat Intelligence Feeds, Cloud providers, Sandboxing, Email Security, soluções de Incident Investigation, soluções de Big Data Analytics, Web Security, Threat Detection, Identity Management, Soluções de bancos de dados;
- 6.70.10. Solução deve se integrar com os SIEM líderes de mercado: IBM Qradar, Splunk FortiSIEM, ArcSight (ou nome mais novo), LogRhythm, RSA Netwitness, Rapid7;
- 6.70.11. Solução deve poder importar Processos de Fluxos de Trabalho (workflows) de Flowable, Camunda e Signavio (no mínimo);
- 6.70.12. Solução deve poder enviar mensagens de Syslog para elementos externos com informações sobre saúde, playbooks, execução de sistemas internos;
- 6.71. Threat Intelligence
- 6.71.1. O fabricante da solução deve fornecer seu próprio serviço de inteligência de ameaças gratuitamente trabalhando nativamente com o SOAR proposto;
- 6.71.2. A solução deve ter um módulo de gerenciamento de inteligência de ameaças que inclua um painel de informações de ameaças com estatísticas sobre: Feeds ativos, observáveis de alta confiança, fontes de feed;
- 6.71.3. Integração com várias dezenas de fontes CTI;
- 6.71.4. Os feeds de ameaças devem mostrar seus dados correlacionados com outros indicadores, a estrutura MITRE e as solicitações de inteligência de prioridade. Além disso, cada indicador deve ter um widget gráfico de correlação que indica graficamente todos os relacionamentos;
- 6.71.5. O gerenciamento de caso deve permitir que os analistas levantem a solicitação de requisito de Inteligência de prioridade para indicadores desconhecidos. As tarefas devem ser criadas para rastrear a solicitação. A solução deve

fornecer uma estrutura que permita que os analistas respondam com um relatório abrangente de ameaças para o PIR levantado;

6.71.6. A solução deve atuar como serviço de Inteligência de Ameaças para sistemas de terceiros, onde coleções ou indicadores específicos podem ser buscados do SOAR por SIEMs, EDRs e NGFWs via TAXII e CSV sobre HTTP;

6.71.7. Deve ser possível importar e exportar indicadores em massa diretamente da WebUI;

6.71.8. A solução deve ser flexível o suficiente para permitir a reputação de indicadores de computação com base em dados de várias fontes de Threat Intelligence;

6.71.9. Solução deve permitir a partir de um alerta ou indicador, abrir um PIR (Priority Intelligence Requirement) para o time de Threat Intelligence;

6.71.10. Solução deve permitir a criação de datasets a partir do conjunto de IOCs monitorados. Por exemplo. Filtrar e exportar dataset relacionado com Comando e Controle e Botnets.

6.72. Deployment & Architecture

6.72.1. A solução deve suportar implantação on premise como um software appliance ou como um software;

6.72.2. A solução deve permitir backup e restauração da configuração e dos dados do sistema

6.72.3. Solução Deve ter a capacidade de criar módulos de produtos personalizados a partir da GUI da web, um módulo é um subsistema para gerenciar um novo tipo de registro, como: Alertas, Incidentes e indicadores;

6.72.4. O sistema deve ser escalável e resiliente. Deve ser possível agrupar vários nós (mais de 2) em uma configuração Ativa/Ativa;

6.72.5. A solução deve suportar comunicação segura e de alta disponibilidade entre seus componentes distribuídos e o ambiente central, sem necessidade de exposição direta dos módulos à Internet, podendo utilizar proxy reverso, túnel criptografado ou equivalente;

6.72.6. A solução deve oferecer uma arquitetura multilocatário escalável geograficamente distribuída com; nós remotos no local, execução remota de playbook, gerenciamento centralizado de MSSP;

6.72.7. A solução deve permitir a execução de ações de remediação e coleta de dados na rede segmentada por meio de um agente SOAR implantado no segmento de rede remoto, os agentes devem suportar atualizações automáticas;

6.72.8. O sistema deve permitir o uso de banco de dados interno e externo;

6.72.9. A solução deve incluir um aplicativo móvel para gerenciamento e monitoramento remoto;

6.72.10. A solução deve suportar integração de saída com um sistema NMS que, por padrão, monitore a lista abaixo pronta para uso (sem configuração):

6.72.10.1. CPU (Uso em %)

6.72.10.2. Disco (Uso em % para cada volume lógico e para partição /boot)

6.72.10.3. E/S (solicitações de leitura e gravação/s para discos)

6.72.10.4. Largura de banda da placa de rede incluindo interface loopback(lo) (kb/s)

6.72.10.5. Uso de RAM (%)

6.72.10.6. NTP (Diferença entre NTP e máquina em segundos)

6.72.10.7. Servidor Web (conexões perdidas, solicitações por segundo, conexões manipuladas, etc)

6.72.10.8. Banco de dados (ativo conexões, blocos lidos do disco (blocos/min), taxa de acerto do cache do buffer (%), total de transações (tx/min)

6.72.10.9. MTA (número de solicitações, tamanho da fila do MTA)

6.72.10.10. Expiração da licença SOAR

6.72.10.11. Expiração dos certificados SOAR

6.72.10.12. Saúde dos conectores configurados SOAR (para cima/para baixo)

6.72.10.13. SOAR Playbook fila

6.72.11. Solução deve permitir que múltiplos tenants sejam coordenados por um ponto central, permitindo ao cliente atuar como MSSP;

6.72.12. Solução deve permitir a comunicação segura entre seus elementos;

6.72.13. Solução deve permitir a criação de filas de trabalho e organização de turnos e camadas de analistas (N1, N2, N3). A atribuição de alertas e incidentes aos analistas pode ser feita por um gestor ou de forma automática pela solução;

6.73. Audit

- 6.73.1. O sistema deve fornecer uma trilha de auditoria de todo o sistema, abrangendo tanto o sistema (como login, logoff, instalações) e eventos de dados (como criação de registro, atualização e exclusão);
- 6.73.2. O sistema deve permitir o encaminhamento de eventos para um servidor de log ou solução SIEM. Os protocolos a seguir devem ser compatíveis com um nível de log configurável:
- 6.73.2.1. UDP
- 6.73.2.2. TCP, TCP/TLS
- 6.73.2.3. RELP, RELP/TLS
- 6.73.3. O sistema deve manter um widget de cronograma de registro de auditoria rastreando cada evento de registro com detalhes de cada alteração.
- 6.74. User Management & RBAC
- 6.74.1. O sistema deve fornecer controle de acesso baseado em função (RBAC) granular e flexível. Os administradores devem poder definir os direitos de acesso para cada tipo de registro em um nível de campo. Por exemplo, o endereço IP de origem é um campo;
- 6.74.2. A solução deve suportar o gerenciamento de relacionamento de grupos de usuários, onde um grupo deve ser capaz de herdar o escopo de acesso de um grupo ou grupos diferentes em uma hierarquia pai, irmão, filho e que deve ser possível para que cada nível superior ter acesso ao inferior
- 6.74.3. Solução deve permitir a colaboração entre analistas através de buscas compartilhadas, comentários em alertas e incidentes, entre outros métodos;
- 6.74.4. Solução deve permitir autenticação através de autenticação de dois fatores (MFA);
- 6.74.5. Solução deve permitir autenticação externa de usuários usando LDAP, SAML (SSO);
- 6.75. Dashboards
- 6.75.1. O sistema deve fornecer vários painéis configuráveis que se integram ao RBAC com controle de acesso por função;
- 6.75.2. O sistema deve fornecer um mecanismo para destacar alertas que estão se aproximando de violações de SLA;
- 6.75.3. O painel deve exibir informações específicas do analista, como alertas e tarefas atribuídas ao analista;
- 6.75.4. O sistema deve calcular um ROI estimado e permitir que isso seja exibido em um painel;
- 6.75.5. Deve ser possível importar e exportar modelos de painel;
- 6.75.6. O sistema deve fornecer painéis focados em funções, como; analista de nível 1, analista de nível 2, gerente de SOC;
- 6.75.7. O sistema deve medir métricas de SOC, relevantes, como tempo médio para identificação, confirmação, contenção, erradicação, recuperação. Deve ser possível ainda exibir essas métricas em um painel;
- 6.75.8. A solução deve suportar configurações de Dashboards em Tenants específicos em um ambiente Multi Tenancy;
- 6.75.9. A solução deve ter um painel dedicado para monitorar o status de integridade/disponibilidade de cada integração e a integridade do sistema do próprio SOAR;
- 6.75.10. A solução deve dar suporte à identidade visual da GUI para diferentes Tenants;
- 6.75.11. A solução deve fornecer uma estrutura de desenvolvimento de painel baseada em HTML/JSON/JS para permitir que os usuários criem seus Widgets de painel personalizados e os importem para a solução SOAR;
- 6.75.12. Solução deve ter suporte a Inteligência Artificial Generativa, permeando os módulos da solução. Analista deve ser capaz de fazer perguntas, requerer sugestões, interagir com a Inteligência artificial;
- 6.75.13. Solução deve permitir ao analista criar módulos e customizar Dashboards;
- 6.75.14. Solução deve possuir sistema de Ajuda, que permite ao analista ou usuário tirar dúvidas. Além disso, solução deve ter disponível documentação completa, incluindo como construir playbooks, conectores, como customizar o dashboard, como gerenciar a força de trabalho do SOC, como configurar a solução;
- 6.75.15. Solução deve permitir monitorar a saúde do sistema através de Dashboard específico para essa função;
- 6.75.16. Solução deve trazer Dashboard com métricas (KPIs) de segurança e eficiência do SOC (tempo salvos com playbooks, retorno do investimento);
- 6.75.17. Os Dashboards devem permitir auto-refresh;
- 6.75.18. Todas as ações da solução devem ser feitas na mesma interface (não desejamos duas interfaces / sistemas distintos);
- 6.76. Reporting + Notifications

- 6.76.1. O sistema deve fornecer relatórios gráficos personalizados;
- 6.76.2. Deve ser possível agendar relatórios para serem executados em um horário definido pelo usuário;
- 6.76.3. Os relatórios devem estar disponíveis em formato PDF ou CSV;
- 6.76.4. Deve ser possível enviar relatórios programados para um destinatário de e-mail;
- 6.76.5. A solução deve permitir um controle programático dos relatórios, para que um analista possa criar um playbook para automatizar o processo de geração dos mesmos;
- 6.76.6. O acesso à funcionalidade de relatório deve ser controlado pela função RBAC;
- 6.76.7. O sistema deve ter uma trilha de auditoria que identifique a atividade do relatório, incluindo download do mesmo;
- 6.76.8. Deve ser possível incluir uma variedade de gráficos e métricas em relatórios personalizados;
- 6.76.9. Além da exportação automatizada de registros por meio de playbooks, a interface do usuário deve ter um meio que permita aos usuários baixarem alguns/todos os registros para sua estação de trabalho;
- 6.76.10. Solução permite customizar E-mail Templates que são enviados pelo time de SOC;
- 6.76.11. Solução deve ter flexibilidade para envio de notificações externas.
7. Serviço de disponibilização de ambiente de testes
  - 7.1. A CONTRATADA deverá realizar a implementação de um laboratório virtual para testes de resposta a incidentes e brechas de vulnerabilidade, incluindo fornecimento, instalação, configuração e manutenção, equipamentos e soluções de segurança, composto por Firewall, pontos de acesso (AP) e switches de segurança;
  - 7.2. O laboratório pode ser no ambiente da CONTRATADA ou em nuvem (segundo os requisitos mínimos do ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM);
  - 7.3. A utilização de Firewalls, pontos de acesso e switches de segurança garantirá um ambiente de testes seguro e controlado, visando simular um ambiente real de um órgão do poder executivo do estado;
  - 7.4. A CONTRATADA deverá fornecer, instalar, configurar e manter os seguintes equipamentos e soluções durante todo o período do contrato:
    - 7.4.1. Firewall:
      - 7.4.1.1. Fornecimento de Firewalls de última geração com funcionalidades avançadas de segurança, incluindo prevenção de intrusões (IPS), filtragem de URL, VPN, inspeção profunda de pacotes (DPI) e suporte a múltiplos WANs, similar aos instalados nos sites do governo atendidos pelo projeto da Nova Rede;
      - 7.4.1.2. Manutenção e suporte técnico contínuos, incluindo atualizações de firmware e assinaturas de segurança;
      - 7.4.1.3. Possibilidade de configuração de HA para atendimento dos requisitos do serviço de Alta Disponibilidade (HA);
    - 7.4.2. Access point:
      - 7.4.2.1. Fornecimento de pontos de acesso com capacidade para redes sem fio similar aos instalados nos sites do governo atendidos pelo projeto da Nova Rede;
      - 7.4.2.2. Manutenção e suporte técnico contínuos, incluindo atualizações de firmware e assistência técnica;
    - 7.4.3. Switch:
      - 7.4.3.1. Fornecimento de switches de segurança gerenciáveis com suporte a VLANs, e funcionalidades avançadas de segurança, como controle de acesso baseado em portas e monitoramento de tráfego, similar ao instalado nos sites do governo atendidos pelo projeto da nova Rede;
      - 7.4.3.2. Manutenção e suporte técnico contínuos, incluindo atualizações de firmware e assistência técnica.
  - 7.5. A CONTRATADA deverá fornecer um plano detalhado de implementação, incluindo cronograma, etapas de instalação e configuração, e testes de validação;
  - 7.6. Deverão ser emitidos relatórios de todos os testes de atualização de firmware, configuração de alta disponibilidade, resposta a incidentes e brechas de vulnerabilidades realizados no laboratório, e enviados a CONTRATANTE técnica ATI;
  - 7.7. Antes de toda e qualquer atualização de ambientes que possuam o serviço de Alta Disponibilidade (HA) ativos, deverão ser realizados testes no laboratório e relatórios deverão ser emitidos e enviados a CONTRATANTE aderente, bem como a CONTRATANTE técnica ATI para validação;
  - 7.8. Todas as atividades realizadas devem estar em conformidade com as normas e melhores práticas de segurança da informação;

7.9. A CONTRATADA deve assegurar a confidencialidade e integridade das informações e dados tratados durante a implementação do projeto e de todos os testes realizados no ambiente.

8. Solução de gerenciamento de serviços de TI - ITSM

8.1. Monitoramento de Incidentes

8.1.1. A solução gerencia incidentes através de um processo próprio para estes objetos.

8.1.2. Permite categorizar Incidentes

8.1.3. Interface WEB para o analista

8.1.4. Permite configurar alertas no caso de alterações no conteúdo de incidentes

8.1.5. Permitir que o usuário anexe links para documentos ao incidente.

8.1.6. Permitir que o usuário anexe documentos completos ao incidente.

8.1.7. Permitir a priorização dos incidentes

8.1.8. Permitir que os incidentes sejam direcionados para grupos específicos dependendo de sua categoria

8.1.9. Possibilitar o relacionamento dos incidentes com outros incidentes, problemas, mudanças ou requisições.

8.1.10. Disponibilizar a funcionalidade de pesquisa de incidentes similares na abertura de um novo incidente

8.1.11. Permitir a geração de problemas e de solicitações de mudanças a partir de um incidente

8.1.12. Permitir que os incidentes possam ser associados aos itens de configuração cadastrados no CMDB.

8.1.13. Permitir a criação de incidentes a partir de modelos pré-definidos.

8.1.14. Permitir o fechamento de todos os incidentes relacionados a um incidente pai.

8.1.15. Possibilitar o registro das soluções dos incidentes e disponibilizar a geração de documentos de conhecimento a partir destes registros.

8.1.16. Monitorar e emitir relatórios sobre os incidentes.

8.2. Monitoramento de Problemas

8.2.1. A solução deverá gerenciar problemas através de um processo próprio para estes objetos.

8.2.2. Permitir categorizar Problemas

8.2.3. Possuir Interface WEB para o analista

8.2.4. Permitir configurar alertas no caso de alterações no conteúdo de problemas

8.2.5. Permitir que o analista anexe links para documentos ao problema.

8.2.6. Permitir que o analista anexe documentos completos ao problema.

8.2.7. Permitir a priorização dos problemas

8.2.8. Permitir que os problemas sejam direcionados para grupos específicos dependendo de sua categoria

8.2.9. Possibilitar o relacionamento dos problemas com outros incidentes, problemas, mudanças ou requisições.

8.2.10. Disponibilizar a funcionalidade de pesquisa de problemas similares na abertura de um novo problema

8.2.11. Permitir a geração de solicitações de mudanças a partir de um problema

8.2.12. Permitir que os problemas possam ser associados aos itens de configuração cadastrados no CMDB.

8.2.13. Possibilitar o registro das soluções dos problemas e disponibilizar a geração de documentos de conhecimento a partir destes registros.

8.2.14. Permitir a criação de problemas a partir de modelos pré-definidos.

8.2.15. Permitir o fechamento de todos os problemas relacionados a um problema pai.

8.2.16. Monitorar e emitir relatórios sobre os problemas

8.3. Monitoramento de Mudanças

8.3.1. A solução deverá gerenciar mudanças através de um processo próprio para estes objetos.

8.3.2. Permitir avaliar o impacto, custos, benefícios e riscos da mudança.

8.3.3. Permitir categorizar Solicitações de Mudanças

8.3.4. Possuir Interface WEB para o analista

8.3.5. Permitir configurar alertas no caso de alterações no conteúdo da solicitação de mudanças

8.3.6. Permitir criar um fluxo de aprovações para as mudanças

8.3.7. Permitir gerenciar as atividades de implantação das mudanças

8.3.8. Monitorar e emitir relatórios sobre a implantação das mudanças

8.3.9. Permitir revisar e encerrar os processos de mudanças

8.3.10. Permitir que as solicitações de mudanças possam ser associadas aos itens de configuração cadastrados no CMDB.

- 8.3.11. Possuir calendário de visualização para facilitar o planejamento das mudanças
- 8.3.12. Permitir que o analista anexe links para documentos à solicitação de mudança.
- 8.3.13. Permitir que o analista anexe documentos completos à solicitação de mudança.
- 8.3.14. Permitir a priorização das solicitações de mudanças
- 8.3.15. Permitir que as mudanças sejam direcionadas para grupos específicos dependendo de sua categoria
- 8.3.16. Possibilitar o relacionamento das solicitações de mudanças com outros incidentes, problemas, mudanças ou requisições.
- 8.3.17. Disponibilizar a criação de listas de atividades para serem executadas no registro de uma solicitação de mudanças.
- 8.3.18. Disponibilizar ferramenta de workflow para fluxos de mudanças complexos que envolvam integrações com outras soluções.
- 8.3.19. Disponibilizar visualização de workflow, permitindo identificar em que passo o fluxo está parado.
- 8.3.20. Permitir que os analistas incluam tarefas dinamicamente nas listas de atividades de uma solicitação de mudanças em andamento.
- 8.3.21. Permitir nativamente a criação de incidentes a partir de uma solicitação de mudança.
- 8.3.22. Permitir a criação de solicitações de mudanças a partir de modelos pré-definidos.
- 8.3.23. Permitir o fechamento de todas as solicitações de mudanças relacionadas a uma solicitação de mudança pai.
- 8.3.24. Oferecer possibilidade de cadastramento de janelas de manutenção e janelas de blecaute, quando nenhuma mudança pode ser agendada
- 8.3.25. Permitir a criação de uma pesquisa de risco para cada categoria de mudança.
- 8.3.26. Permitir visualizar todos os itens de configuração de uma mudança e seus relacionamentos, possibilitando incluir itens de configuração relacionados que não tenham sido originalmente vinculados à mudança.
- 8.4. Monitoramento de Requisições
  - 8.4.1. A solução deverá gerenciar requisições através de um processo próprio para estes objetos.
  - 8.4.2. Permitir categorizar Requisições.
  - 8.4.3. Possuir Interface WEB para o analista.
  - 8.4.4. Permitir configurar alertas no caso de alterações no conteúdo das requisições.
  - 8.4.5. Permitir que o usuário final ou analistas anexem links para documentos à requisição.
  - 8.4.6. Permitir que o usuário final ou analistas anexem documentos completos à requisição.
  - 8.4.7. Permitir a priorização das requisições.
  - 8.4.8. Permitir que as requisições sejam direcionadas para grupos específicos dependendo de sua categoria.
  - 8.4.9. Possibilitar o relacionamento das requisições com outros incidentes, problemas, mudanças ou requisições.
  - 8.4.10. Permitir a criação de incidentes e mudanças a partir de uma requisição.
  - 8.4.11. Permitir que as solicitações de mudanças possam ser associadas aos itens de configuração cadastrados no CMDB.
  - 8.4.12. Possibilitar o registro das soluções das requisições e disponibilizar a geração de documentos de conhecimento a partir destes registros.
  - 8.4.13. Monitorar e emitir relatórios sobre a as requisições.
- 8.5. Monitoramento de Configurações
  - 8.5.1. Possuir Interface WEB para o analista.
  - 8.5.2. Permitir o registro dos itens de configuração e seus atributos
  - 8.5.3. Permitir a manutenção de diferentes atributos para diferentes tipos de itens de configuração.
  - 8.5.4. Possuir interface gráfica para demonstrar o relacionamento entre os itens de configuração.
  - 8.5.5. Permitir visualizar somente os itens afetados por um item de configuração (Análise de Impacto).
  - 8.5.6. Permitir visualizar somente os itens que afetam um item de configuração (Análise de Causa Raiz).
  - 8.5.7. Permitir filtrar os tipos de itens de configuração a se visualizar. Ex (Visualizar somente itens de configuração do tipo Serviço ou NMS).
  - 8.5.8. Permitir pesquisar os itens de configuração diretamente na interface de visualização dos relacionamentos.
  - 8.5.9. Permitir a criação de relacionamentos diretamente na interface gráfica de visualização.
  - 8.5.10. Mostrar o status do item de configuração na interface gráfica (Ex. Ativo, Indisponível, em manutenção, ...).
  - 8.5.11. Permitir a pesquisa de itens de configuração por status operacional (Normal, Parado, Warning etc.).

- 8.5.12. Permitir a pesquisa de itens de configuração por status administrativo (Normal, Em Estoque, Alugado, Em Manutenção etc.).
- 8.5.13. Permitir a pesquisa de itens de configuração por prioridade.
- 8.5.14. Permitir a listagem dos itens de configuração que sofreram mudanças no último dia, última semana ou último mês.
- 8.5.15. Permitir visualizar facilmente quantas requisições, incidentes, problemas e solicitações de mudanças estão relacionados ao item de configuração.
- 8.5.16. Permitir visualizar os relacionamentos em formato de lista.
- 8.5.17. Permitir a associação de SLAs aos itens de configuração para a contabilização do tempo de atendimento a estes itens.
- 8.5.18. Permitir nativamente a importação de itens de configuração a partir de ferramentas de inventário de ativos.
- 8.5.19. Permitir a abertura de incidentes relacionados a itens de configuração do CMDB ou a ativos não gerenciados pelo CMDB.
- 8.6. Monitoramento da Base de Conhecimento
- 8.6.1. Possuir Interface WEB para o analista.
- 8.6.2. Permitir pesquisa em linguagem natural.
- 8.6.3. Permitir que o analista visualize se o usuário final pesquisou a base de conhecimentos na abertura de um incidente ou requisição.
- 8.6.4. A solução deverá permitir que sempre seja solicitada a pesquisa na base de conhecimento para o usuário final antes da abertura de um incidente ou requisição.
- 8.6.5. Permitir a seleção dos campos para pesquisa como título, sumário do documento, problema ou solução encontrada.
- 8.6.6. Permitir a inserção de figuras e links nos documentos da base de conhecimento.
- 8.6.7. Permitir a criação de requisições ou incidentes a partir de um documento da base de conhecimento.
- 8.6.8. Permitir associar ao log do incidente ou problema o link para o documento de conhecimento utilizado.
- 8.6.9. Informar quantas requisições, incidentes ou problemas estão relacionados a cada documento de conhecimento.
- 8.6.10. Permitir indexar a base de conhecimento para disponibilizar pesquisas por palavras-chave.
- 8.6.11. Permitir aos analistas enviarem comentários sobre o documento de conhecimento.
- 8.6.12. Controlar o acesso de escrita aos documentos baseado em perfil de usuários.
- 8.6.13. Possuir um calendário de gestão dos documentos para facilitar a gestão e planejamento das publicações na base de conhecimento.
- 8.6.14. Permitir que os documentos mais utilizados sejam disponibilizados automaticamente na interface dos analistas.
- 8.6.15. Monitorar e emitir relatórios sobre os documentos da base de conhecimento.
- 8.7. Monitoramento de Níveis de Serviço de Atendimento
- 8.7.1. Possibilitar a criação de eventos e macros associados a NMSs que serão utilizados para notificação e para escalar o chamado.
- 8.7.2. Permitir a criação de níveis de serviço por usuário, item de configuração, categoria do objeto e prioridade.
- 8.7.3. Medir e emitir relatórios sobre os níveis de serviço atingidos.
- 8.7.4. Permitir que ações de envio de e-mail sejam disparadas no caso de violações de NMSs.
- 8.7.5. Permitir que ações de envio de e-mail sejam disparadas no caso de alertas para possíveis violações de NMSs.
- 8.7.6. Permitir que os tickets sejam escalados no caso de violações de NMSs.
- 8.7.7. Permitir que os tickets sejam escalados no caso de alertas para possíveis violações de NMSs.
- 8.7.8. Permitir que um mesmo ticket tenha mais de um NMS sendo monitorado ao mesmo tempo.
- 8.7.9. Registrar a ocorrência de cada alerta e das violações ocorridas nas informações do incidente, problema, mudança ou requisição ao qual o NMS está associado.
- 8.7.10. Permitir que gestores possam alterar os prazos de NMSs durante a sua execução.
- 8.7.11. Permitir que gestores possam cancelar a verificação de um NMS associado a um incidente, problema, mudança ou requisição.
- 8.8. Automação do Atendimento

- 8.8.1. Permitir que um técnico possa atender mais de um cliente usuário, ao mesmo tempo, ou convidar outros técnicos ou supervisores a participar das sessões de atendimento.
- 8.8.2. Possuir funcionalidade de escalonamento, facilitando a transferência do cliente usuário a outro técnico, mais especializado, ou a outra fila durante o atendimento on-line.
- 8.8.3. Possuir scripts prontos e permitir criar scripts, para automação de tarefas
- 8.8.4. Garantir que os dados trafegados entre o analista e o usuário final sejam criptografados.
- 8.8.5. Armazenar informações relacionadas a log de atividades executadas em tickets / chamados novos ou pré-existentes.
- 8.9. Pesquisas de Satisfação
  - 8.9.1. Possuir Interface Web para pesquisas de satisfação.
  - 8.9.2. Deverá armazenar todos os resultados das pesquisas de satisfação para a geração de relatórios.
  - 8.9.3. Permitir a obrigatoriedade da pesquisa.
  - 8.9.4. Permitir o envio de pesquisas de forma intermitente (Ex: a cada 10 incidentes/requisições).
  - 8.9.5. Permitir o envio de pesquisas a um grupo de usuários e a definição de um prazo para as respostas.
  - 8.9.6. Permitir a criação de modelos para facilitar a criação de novas pesquisas.
  - 8.9.7. Permitir a configuração de várias pesquisas simultâneas.
  - 8.9.8. Permitir a configuração de lembretes para alertar os usuários que não responderam à pesquisa.
  - 8.9.9. Permitir a configuração de perguntas obrigatórias nas pesquisas.
  - 8.9.10. Permitir a adição de campos para os comentários finais dos usuários.
  - 8.9.11. Possuir funcionalidade para evitar que o mesmo usuário responda a pesquisa por mais de uma vez.
- 8.10. Administração
  - 8.10.1. Permitir configurar regras e periodicidade para arquivamento ou remoção de dados antigos de contatos, pesquisas de opinião, requisições, incidentes, problemas e solicitações de mudanças.
  - 8.10.2. Permitir restringir o tipo de arquivo que será armazenado no repositório.
  - 8.10.3. Permitir limitar o tamanho dos arquivos que serão armazenados no repositório.
  - 8.10.4. Os arquivos anexos deverão ser comprimidos para diminuição de espaço alocado.
  - 8.10.5. Permitir criar padrões de documentação para abertura de requisições, incidentes, problemas e solicitações de mudanças.
  - 8.10.6. Permitir configurar termos especiais, sinônimos e palavras reservadas para a pesquisa de documentos.
  - 8.10.7. Permitir configurar notificações para analistas e clientes.
  - 8.10.8. Possuir Interface de administração via WEB.
  - 8.10.9. Disponibilizar na instalação modelos completos de atendimento a incidentes, problemas e mudanças baseados em ITIL.
- 8.11. Segurança
  - 8.11.1. Requerer autenticação do usuário para acessar o sistema.
  - 8.11.2. Forçar políticas para uso de senhas (comprimento, caracteres, reuso).
  - 8.11.3. Validar login (expiração de senhas, tentativas múltiplas).
  - 8.11.4. Fornecer segurança que seja adequada a LAN e WAN.
  - 8.11.5. Possibilitar a autenticação de usuários via LDAP.
  - 8.11.6. Definir perfis de usuários de acordo com regras definidas no ambiente.
  - 8.11.7. Permitir a configuração de restrições de acesso dos usuários a determinados tickets dependendo de seu conteúdo.
  - 8.11.8. Permitir restringir acessos a formulários baseando-se no perfil do usuário.
- 8.12. Relatório e Comunicação
  - 8.12.1. Fornecer um conjunto pré-definido de relatórios.
  - 8.12.2. Fornecer visualização gráfica dos dados com suporte a decisão executiva.
  - 8.12.3. Permitir a criação de relatórios dinâmicos de forma simples (drag & drop).
  - 8.12.4. Suportar a definição de KPIs (indicadores de desempenho) baseados em dados do Service desk.
  - 8.12.5. Suportar a criação de filtros e agrupamentos nos relatórios.
  - 8.12.6. Permitir que os relatórios sejam enviados via e-mail.
  - 8.12.7. Permitir a exportação dos relatórios para um dos formatos: MS-Excel, PDF, MS-Word, Texto

- 8.12.8. Permitir o agendamento de relatórios.
- 8.12.9. Permitir que o agendamento envie os relatórios gerados via e-mail.
- 8.12.10. Permitir que o agendamento dos relatórios faça a impressão de forma automática.
- 8.12.11. Permitir a estruturação dos relatórios em pastas com controle de acesso.
- 8.12.12. Permitir que o usuário crie relatórios ou atalhos para relatórios pré-existentes nas pastas as quais tem acesso.
- 8.13. Infraestrutura e Conexão com Outras Ferramentas
  - 8.13.1. Suportar Ipv6
  - 8.13.2. Fornecer integração nativa com a solução de monitoramento da rede WAN para Falhas e desempenho.
  - 8.13.3. Fornecer integração nativa com a solução de monitoramento de inventário de Hardware e Software.
  - 8.13.4. A solução deverá ser compatível com navegadores web amplamente utilizados, suportados e atualizados pelo fabricante, garantindo pleno funcionamento das funcionalidades, observadas as boas práticas de segurança da informação, usabilidade e atualização tecnológica;
  - 8.13.5. Permitir o envio de e-mails automatizados através de SMTP.
  - 8.13.6. Permitir utilizar HTTPS (SSL) no servidor WEB;
  - 8.13.7. Permitir utilizar HTTPS (SSL) nos WEB Services;
  - 8.13.8. Permitir a utilização do HTTPS (SSL) somente no momento da autenticação, melhorando o desempenho do servidor;
  - 8.13.9. Permitir a configuração de Firewall e VPN para acesso ao servidor.

## ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA DA NOVA REDE CORPORATIVA

### 1. Requisitos gerais

- 1.1. É de responsabilidade da CONTRATADA instalar e manter o conjunto de recursos tecnológicos que integrarão a prestação de serviços do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), bem como o acesso seguro à internet, por meio de link independente da rede da CONTRATANTE, destinado exclusivamente ao desempenho das atividades operacionais. A CONTRATANTE só disponibilizará o espaço físico e ponto de energia, não essencial e não estabilizada, para instalar os recursos que estão especificados nos itens e subitens correspondentes contidos neste Termo de Referência;
- 1.2. A rede de dados do Centro Integrado de Inteligência e Segurança Cibernética (CIISC) será de responsabilidade da CONTRATADA e deverá ser isolada da rede da CONTRATANTE. As conexões para inspeção, monitoramento e suporte deverão ser realizadas através de integração segura com a rede da CONTRATANTE. Será permitido que a CONTRATANTE solicite logs de acesso da CONTRATADA a sua rede;
- 1.3. Instalar e manter um conjunto de recursos tecnológicos compostos por soluções de hardware, software e equipes técnicas especializadas para permitir a perfeita execução das atividades do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa requerida e especificadas neste Termo de Referência. Todos esses recursos e serviços serão fiscalizados pela CONTRATANTE técnica ATI;
- 1.4. Realizar o gerenciamento da Nova Rede Corporativa de acordo com as Regras de Prestação de serviços e o Modelo de Gestão definidos nos itens e subitens correspondentes contidos neste Termo de Referência;
- 1.5. O Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa está dividido nos serviços abaixo relacionados, onde os quais serão especificados nos subitens constantes deste Tópico:
  - 1.5.1. Composição do CIISC:
    - 1.5.1.1. Serviço de resposta a incidentes de cibersegurança;
    - 1.5.1.2. Serviço de análise de segurança de primeiro nível;
    - 1.5.1.3. Serviço de análise de segurança especializada;
    - 1.5.1.4. Serviço de acompanhamento de reparos;
    - 1.5.1.5. Serviço de atenção especializada ao cliente;
    - 1.5.1.6. Service desk especializado;
    - 1.5.1.7. Serviço de operação de rede;
    - 1.5.1.8. Serviço de análise de qualidade;

- 1.5.1.9. Serviço de coordenação do CIISC;
- 1.5.1.10. Núcleo de redes e segurança setorial;
- 1.5.1.11. Serviço de evolução da maturidade em segurança da informação.
- 1.6. Os analistas de nível 1 atuarão em regime de trabalho híbrido, com atividades realizadas nas dependências do Centro Integrado de Inteligência e Segurança Cibernética (CIISC). Para garantir a continuidade operacional, a escala deverá assegurar a presença física de, no mínimo, 50% do corpo técnico durante o horário de funcionamento da ATI, sendo o restante da jornada cumprido de forma remota. Da mesma forma, a liderança e a coordenação deverão estabelecer um sistema de revezamento que garanta a presença de, ao menos, dois profissionais destas funções simultaneamente no local.
- 1.7. Para os demais integrantes das equipes, a presença no CIISC será a critério da CONTRATADA, não sendo exigência da CONTRATANTE, permitindo assim o modelo de trabalho remoto para essas funções;
- 1.8. O Centro Integrado de Inteligência e Segurança Cibernética (CIISC) será responsável por todas as atividades necessárias para a configuração, suporte, monitoramento, gerenciamento, elaboração de relatórios, abertura de tickets, execução e controle de planos de ação, bem como quaisquer outras ações essenciais para garantir o pleno funcionamento e a qualidade de todos os serviços previstos neste Termo de Referência e seus respectivos Adendos, incluindo, mas não se limitando a:
- 1.8.1. Serviços de Links de Acesso (LAP, LME e LAT), realizando configurações, monitoramento, operação e aplicação de medidas de segurança para garantir a disponibilidade, desempenho e conformidade com os níveis mínimos de serviço (NMS);
- 1.8.2. Serviços de Conectividade para Datacenter (L2L e LIT), realizando todas as configurações, aplicação de medidas de segurança, gestão e operação das interconexões entre datacenters, garantindo parâmetros técnicos, alto desempenho e disponibilidade das conexões críticas;
- 1.8.3. Serviços de Contact Center, abrangendo suporte a chamados, monitoramento do atendimento e qualidade do atendimento e conformidade com os níveis de serviço estabelecidos no contrato;
- 1.8.4. Tráfego extrarrede e comunicação unificada, garantindo a estabilidade, integridade e segurança das comunicações corporativas, incluindo interface SIP/SIP Trunk, chamadas locais, inter-regionais, internacionais e DDG (0800);
- 1.8.5. Gestão das soluções de Wi-Fi, assegurando a operação ininterrupta, segurança dos acessos e resposta rápida a incidentes que comprometam a qualidade do serviço;
- 1.8.6. Serviço de Pontos de Voz Fixos (PVF), supervisionando a disponibilidade e integridade das chamadas, além do correto funcionamento dos dispositivos e softwares associados;
- 1.9. A CONTRATADA deverá assegurar que o CIISC possua plena visibilidade sobre todos os serviços contratados, garantindo:
- 1.9.1. Monitoramento contínuo e em tempo real da infraestrutura de conectividade, telefonia, segurança e demais serviços da Nova Rede Corporativa;
- 1.9.2. Acesso remoto seguro e controlado a todas as plataformas e equipamentos utilizados na prestação dos serviços, incluindo logs de acesso e trilhas de auditoria;
- 1.9.3. Registro e análise de incidentes técnicos ocorridos em qualquer um dos serviços fornecidos, visando à rápida detecção e mitigação de falhas;
- 1.9.4. Correlação e cruzamento de informações entre os diferentes serviços para otimizar diagnósticos e acelerar a solução de problemas;
- 1.10. A CONTRATADA deverá garantir que o CIISC atue de maneira proativa e reativa na gestão de todos os serviços previstos da Nova Rede Corporativa, assegurando:
- 1.10.1. Análise contínua de desempenho dos serviços contratados, identificando padrões que possam indicar riscos de degradação da qualidade do serviço;
- 1.10.2. Identificação antecipada de falhas e ações preventivas para mitigação de impactos operacionais nos serviços de dados, voz e segurança cibernética;
- 1.10.3. Execução e coordenação da resposta a incidentes técnicos e de segurança, acionando os níveis de suporte e escalonamento necessários dentro dos NMSs estabelecidos no contrato;
- 1.10.4. Correções, ajustes e otimizações nos serviços e plataformas utilizadas pela CONTRATADA, garantindo sua plena aderência aos níveis mínimos de serviço exigidos.

1.11. A CONTRATADA deverá disponibilizar ao CIISC ferramentas que possibilitem a auditoria, acompanhamento e geração de relatórios detalhados sobre a qualidade de todos os serviços contratados, contemplando:

1.11.1. Painéis de monitoramento (dashboards) online e em tempo real para análise de desempenho dos serviços de Contact Center, telefonia, links de acesso, Wi-Fi e segurança;

1.11.2. Relatórios periódicos sobre qualidade, disponibilidade e conformidade dos serviços, incluindo estatísticas sobre atendimento a chamados, tempo médio de resposta e tempo médio de resolução;

1.11.3. Histórico de registros e logs de incidentes ocorridos e suas respectivas resoluções, permitindo auditoria e rastreabilidade dos problemas reportados;

1.11.4. Geração automatizada de relatórios técnicos mensais para análise de aderência aos níveis mínimos de serviço (NMS) estabelecidos no contrato.

1.12. A CONTRATADA deve comunicar a ATI da necessidade do aumento da velocidade da banda dos Serviços, quando o uso da banda atingir picos de consumo, em Horário de Maior Movimento (HMM), de 80% da capacidade CONTRATADA, através de documento com análises e medições previamente elaboradas, e será executada mediante Parecer Técnico e Ordem de Serviço específica, emitida pela ATI;

1.13. O CIISC, sob responsabilidade da CONTRATADA, terá atuação direta na gestão de tickets e solicitações relacionadas a todos os serviços contratados, garantindo:

1.13.1. Abertura, triagem, categorização e priorização automática de chamados técnicos relacionados a falhas ou degradação nos serviços prestados;

1.13.2. Gestão e acompanhamento da resolução dos chamados, garantindo conformidade com os prazos estabelecidos nos NMSs;

1.13.3. Acompanhamento da implementação de planos de ação corretivos e preventivos, assegurando melhorias contínuas nos serviços contratados;

1.13.4. Encaminhamento de problemas complexos para os níveis superiores de suporte e engenharia da CONTRATADA, garantindo ações de mitigação apropriadas;

1.14. A CONTRATADA deverá manter atualizados, de forma contínua, os dados do responsável técnico indicado pela CONTRATANTE (gestor de telemática) referente aos blocos de IP sob sua responsabilidade. Essa atualização deve incluir tanto os endereços IP delegados pelo Sistema Autônomo (AS) da ATI quanto os do AS próprio da CONTRATADA.

1.14.1. Deverá ser mantido um histórico das alterações de responsáveis técnicos, e cada IP delegado deve estar vinculado ao endereço físico da localidade correspondente.

1.14.2. A CONTRATADA também deverá importar os dados históricos atualmente registrados no contrato em vigor.

1.14.3. Todas essas informações devem estar disponíveis para consulta pela CONTRATANTE durante toda a vigência do contrato e ser entregues integralmente ao seu encerramento;

1.14.4. A CONTRATADA poderá utilizar os endereços IP pertencentes ao Sistema Autônomo (AS) da ATI para atendimento das Localidades classificadas como Ponto Conectado Seguro – PCS. A ATI disponibilizará os blocos de IP necessários, excluindo aqueles reservados para os serviços críticos do Data Center e para as Localidades que realizam publicação de sistemas e aplicações.

1.15. A CONTRATADA será integralmente responsável por fornecer recursos humanos especializados e infraestrutura tecnológica para garantir o funcionamento eficiente do CIISC, incluindo:

1.15.1. Equipes técnicas certificadas em segurança cibernética, telemática, comunicação corporativa, telecomunicações, redes e suporte técnico;

1.15.2. Ferramentas e plataformas de monitoramento, análise e auditoria dos serviços, assegurando integração, rastreabilidade e total visibilidade operacional sobre todos os serviços contratados para a Nova Rede Corporativa, conforme especificado neste Termo de Referência;

1.15.3. Ambiente computacional seguro e independente da rede da CONTRATANTE, com acesso controlado e segregado para proteção contra acessos não autorizados.

1.16. A CONTRATADA deverá apoiar na gestão e guarda dos chips e aparelhos de internet móvel de forma presencial no ambiente CIISC na CONTRATANTE;

1.17. A CONTRATADA deverá atuar de forma integrada com a solução de Mobile Device Management (MDM) contratada pela CONTRATANTE junto à empresa responsável pelo Serviço Móvel Pessoal (SMP) e internet móvel, compreendendo, no mínimo:

1.17.1. Apoiar a padronização das políticas de segurança, regras de uso e governança dos dispositivos móveis, em alinhamento com as diretrizes da CONTRATANTE técnica (ATI-PE) e com o apoio da equipe de segurança do Centro Integrado de Inteligência e Segurança Cibernética (CIISC);

1.17.2. Apoiar a elaboração de relatórios e a difusão de informações aos usuários sobre os recursos e serviços disponíveis na Nova Rede Corporativa;

1.17.3. Prestar atendimento por meio das ferramentas de gestão e comunicação, fornecendo informações atualizadas sobre os chamados abertos e tratados pelo CIISC e demais equipes envolvidas;

1.17.4. Registrar todos os chamados e ocorrências relacionados aos serviços;

1.17.5. Encaminhar chamados para suporte especializado ou presencial, quando necessário, assegurando a rastreabilidade do processo;

1.17.6. Interagir com o usuário até a conclusão do chamado, mantendo comunicação contínua e registro atualizado do status;

1.17.7. Utilizar a base de conhecimento para aprimorar continuamente o atendimento;

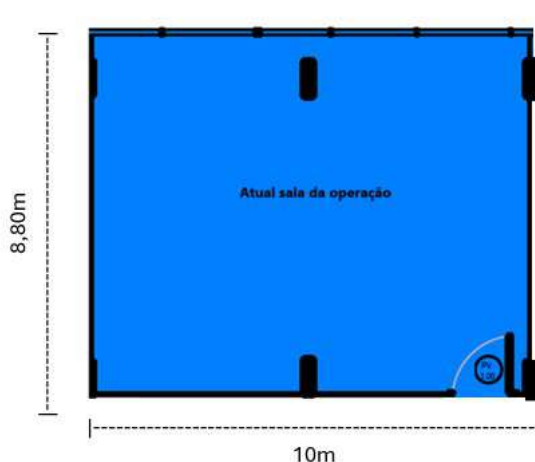
1.17.8. Alimentar o sistema de gestão antes, durante e após o suporte, garantindo integridade, histórico e rastreabilidade das informações;

1.18. O acompanhamento do serviço MDM poderá abranger, ao longo da vigência contratual, até 10.000 (dez mil) dispositivos móveis gerenciados pela solução MDM da CONTRATANTE, observando-se as responsabilidades, limites e diretrizes estabelecidos neste Termo de Referência;

1.19. A CONTRATADA deverá disponibilizar à CONTRATADA do LOTE 2, quando formalmente requisitado, acesso para coleta de informações (via SNMPv3 ou superior), com perfil restrito e seguro, exclusivamente para monitoramento da fibra apagada (fibra cega) dos Data Centers, por meio das interfaces dos switches aos quais tais fibras estejam conectadas. O acesso deverá contemplar autenticação e criptografia, restrição por endereço de origem, escopo limitado de OIDs compatível com a finalidade de monitoramento e demais controles de segurança aplicáveis, sendo vedado qualquer acesso direto aos sistemas internos do CIISC.

## **2. Serviço do Centro Integrado de Inteligência e Segurança Cibernética**

2.1. A CONTRATANTE irá disponibilizar espaço físico para implantação do CIISC, conforme representação a seguir:



2.2. A CONTRATADA deverá fornecer e disponibilizar todo o mobiliário funcional necessário à instalação e operação dos postos de trabalho, organizados em formato de ilhas, com capacidade para acomodar de 4 (quatro) a 6 (seis) colaboradores por ilha. Os postos deverão atender à alocação de profissionais da CONTRATADA, considerando o regime de trabalho híbrido adotado;

2.2.1. Os mobiliários deverão estar em conformidade com os requisitos ergonômicos estabelecidos na Norma Regulamentadora nº 17 (NR-17) do Ministério do Trabalho e na norma ABNT NBR 13962, sendo adequados ao suporte dos equipamentos de Tecnologia da Informação e Comunicação (TIC);

2.2.2. Cada posto de trabalho deverá conter, no mínimo:

2.2.2.1. Mesa e/ou bancada;

2.2.2.2. Ponto de energia elétrica embutido, padrão ABNT NBR 14136;

2.2.2.3. Ponto de rede LAN (Ethernet) embutido;

2.2.2.4. Cadeira ergonômica conforme NR-17.

2.3. É dever da CONTRATADA fornecer todos os equipamentos necessários para o trabalho do seu time, como notebooks, desktops, monitores, mouse, teclado, estabilizador e/ou filtro de linha;

2.4. Todos os softwares utilizados pela equipe da CONTRATADA deverão ser licenciados, durante todo o período do contrato, evitando violação dos direitos autorais e vulnerabilidade na segurança com softwares não legalizados;

2.5. A infraestrutura deverá incluir uma sala de gerenciamento de crises, de responsabilidade da CONTRATADA, conforme especificado abaixo:

2.5.1. Dimensões mínimas de 4x2 metros;

2.5.2. Configurada no formato "aquário". Três de suas paredes deverão ser inteiramente de vidro, proporcionando visibilidade completa da sala de operações e do painel de videowall. Para garantir a privacidade, a sala deve contar com recursos como cortinas persianas ou outra solução adequada, sujeita à aprovação prévia da equipe técnica da CONTRATANTE ATI;

2.5.3. A sala de gerenciamento de crises deve estar equipada com mobiliário apropriado, incluindo uma mesa central grande o suficiente para acomodar no mínimo seis pessoas com cantos arredondados padrão NR 17, com caixa de embutir para 6 (seis) pontos de energia padrão ABNT NBR 14136 para suportar notebooks, carregadores e outros dispositivos necessários durante as operações. E acabamento mais resistente à riscos na sua superfície, facilitando a limpeza em seu uso diário (tecnologia anti-riscos e manchas);

2.5.4. Cadeiras ergonômicas padrão NR17 com altura e braços ajustáveis, encosto reclinável, base giratória e pés com rodas;

2.5.5. Deve incluir um painel para desenhos e representações livres com caneta hidrográfica, com área útil mínima de 120 cm x 90 cm, com superfície lisa, não porosa e resistente a manchas e estrutura de suporte robusta, preferencialmente em alumínio ou aço para maior durabilidade. Cuja remoção seja completa das marcas de caneta hidrográfica sem deixar resíduos, resistente a riscos e danos, garantindo longevidade mesmo com uso frequente,

antirreflexo para minimizar o brilho e facilitar a visualização de qualquer ângulo. Deve ter bandeja de armazenamento integrada para organização de canetas e apagadores;

2.5.6. Pontos de rede LAN (Ethernet) para conexão de dispositivos, além de suporte para Wi-Fi de alta velocidade;

2.5.7. Iluminação LED ajustável para reduzir o cansaço visual e proporcionar um ambiente de trabalho bem iluminado com luzes distribuídas de forma uniforme, evitando sombras e garantindo visibilidade adequada em todas as áreas de trabalho;

2.6. Prover e manter uma solução denominada de Geração de Imagens (Video Wall + Software), bem como todos os sistemas e/ou ferramentas automatizadas, para permitir a realização das atividades do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, incluindo o serviço de manutenção e assistência técnica desta solução, assim como a reposição de componentes defeituosos desse sistema e reposição de outros recursos necessários ao seu pleno funcionamento. Esta solução de geração de imagens deverá funcionar em regime de operação 24 x 7 x 365, e deve ser considerada pela CONTRATADA de forma que, as ferramentas de softwares adotadas pela mesma sejam visualizadas, incluindo todos os módulos de operação e gerenciamento, contendo a facilidade de geração de gráficos a serem exibidos nos monitores;

2.6.1. A CONTRATADA deverá disponibilizar recurso de painel de Videowall de visualização conforme as especificações abaixo:

2.6.1.1. Telas do Video Wall:

2.6.1.1.1. Composto por 16 telas, de mesmo fabricante, modelo e características técnicas, para Video Wall em mosaico 2x8 (2 linhas x 8 colunas), tecnologia LED, IPS (In-Plane Switching), formando uma única matriz de vídeo, para operar em regime horário 24x7;

2.6.1.1.2. Cada monitor deve possuir, no mínimo, tamanho diagonal 49 polegadas, do tipo WideScreen;

2.6.1.1.3. Possuir Resolução Full HD (1920 X 1080);

2.6.1.1.4. Largura da borda: ≤ 2,0 mm (soma das bordas na junção dos monitores, de tela a tela);

2.6.1.1.5. Revestimento antirreflexo;

2.6.1.1.6. Regime de Operação: Contínuo - 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

2.6.1.1.7. Deve possuir capacidade de processamento (CPU) para gerenciar as imagens de todos os monitores;

2.6.1.1.8. Deve possuir placa de vídeo com recurso suficiente para gerenciamento das imagens de todos os monitores;

2.6.1.1.9. Unidade de Controle Remoto: Permitir controle e ajuste geral via menu interativo;

2.6.1.1.10. Padrão VESA de distância horizontal e vertical entre o centro dos furos com rosca interna localizados na face traseira da tela;

2.6.1.1.11. Devem vir acompanhados de todos os acessórios necessários para instalação e configuração;

2.6.1.1.12. Disponibilizar teclado sem fio, Padrão ABNT-2 português/Brasil; Padrão: QWERTY. Gravação Laser ou outra tecnologia resistente à abrasão e uso prolongado;

2.6.1.1.13. Disponibilizar mouse sem fio, modelo óptico, resolução maior ou igual a 1000dpi, possuir 3 Botões (incluindo de Rolagem "wheel") e configuração ambidestra;

2.6.1.2. Software de Gerenciamento Gráfico para Video Wall

2.6.1.2.1. Software de Operação de Cenários gráficos, deverá ser entregue com licença de uso para todo o período do contrato;

2.6.1.2.2. Deverá capturar imagens ou aplicativos gráficos em quaisquer estações de trabalho local ou remota;

2.6.1.2.3. O software deverá permitir a captura de regiões de múltiplas janelas de cada aplicativo, bem como, de regiões específicas da área de trabalho, permitindo que as regiões capturadas sejam exibidas em qualquer área e em qualquer tamanho no painel do Video Wall;

2.6.1.2.4. Deverá permitir que sejam utilizadas várias estações de trabalho, simultaneamente, limitado ao número de licenças disponíveis;

2.6.1.2.5. Deverá permitir que o usuário opere a máquina endereçada diretamente com o mouse e o teclado do gerenciador gráfico e atue diretamente dentro da janela aberta sobre o Video Wall;

2.6.1.2.6. Deve ter a opção de Preview para preparar todo o mosaico para depois enviar ao painel;

2.6.1.2.7. Deverá permitir a captura de aplicativos oriundos de estações de trabalho pela rede local;

2.6.1.2.8. Deverá permitir a captura de janelas abertas nas estações de trabalho, de modo que seja exibida apenas a aplicação desejada e não a estação em completo;

- 2.6.1.2.9. Deverá permitir a criação e operação de cenários, permitindo o gerenciamento do painel do Videowall remotamente;
- 2.6.1.2.10. Deverá permitir o controle automático do tamanho e posição das janelas de todas as aplicações visualizadas no painel Videowall;
- 2.6.1.2.11. Deverá permitir a criação de múltiplos layouts que permitam ao operador, conforme suas permissões, fazer mudanças rápidas e simultâneas de uma ou mais janelas de aplicações visualizadas no painel Videowall;
- 2.6.1.2.12. Deverá permitir o agendamento de troca de cenários (layouts), para que em tempos predeterminados ocorra mudança automática de layouts sem interferência dos operadores;
- 2.6.1.2.13. As imagens capturadas devem ser exibidas nos painéis Videowall em taxa mínima de 30 (trinta) frames (quadros) por segundo;
- 2.6.1.2.14. O software de controle deverá possuir arquitetura cliente-servidor com interface intuitiva Drag and Drop (arrastar e soltar);
- 2.6.1.2.15. O software não deve impedir ou dificultar o uso das estações de trabalho pelos operadores em outras atividades;
- 2.6.1.2.16. Possuir recursos nativos de controle para aplicativos \*.pdf, \*.jpg, \*.avi, \*.wmv, \*.mp4 e pacotes Microsoft Office e Libre Office;
- 2.6.1.2.17. Permitir atualização do software sem custos durante a vigência do contrato.
- 2.6.1.3. Estrutura de Montagem do Painel Videowall
- 2.6.1.3.1. Conjunto para fixação e montagem diretamente sobre o piso e a laje do teto para dar sustentação a estrutura do mosaico das telas deste Termo de Referência;
- 2.6.1.3.2. Deverá possuir sistema de deslizamento, nivelamento, e ajuste fino de regulagem de altura e profundidade, de modo que o alinhamento entre os monitores seja mantido;
- 2.6.1.3.3. O acesso para manutenção deverá ser frontal (suporte pantográfico), sendo os módulos extraíveis individualmente da matriz sem a necessidade de intervenção nos módulos adjacentes;
- 2.6.1.3.4. Distância entre o piso e o início da área de visualização do Videowall deverá ser de no mínimo 95 cm;
- 2.6.1.3.5. Área de visualização do Videowall não poderá ser obstruída por qualquer parte da estrutura;
- 2.6.1.3.6. A estrutura deverá ser confeccionada em aço carbono com pintura eletrostática na cor preta, permitindo que partes sejam confeccionadas em alumínio;
- 2.6.1.3.7. A moldura na área entorno do Videowall e o fechamento Inferior e lateral, deverão ser confeccionados com painéis de alumínio composto (ACM) na cor preto fosco;
- 2.6.1.3.8. A moldura deverá ser instalada de forma faceada ao Painel de Videowall, formando um único plano;
- 2.6.1.3.9. As molduras superior e inferior deverão possuir venezianas, de forma a permitir a ventilação dos equipamentos. As dimensões deverão ser definidas pela CONTRATADA, de forma a garantir a dissipação de calor dos equipamentos e manter a garantia destes;
- 2.6.1.3.10. O painel deverá ter uma porta com sistema fecho toque para acesso aos equipamentos, no mesmo material do painel, devendo estar localizada nas laterais ou parte inferior da tela. A aceitação, estará condicionada à aprovação do projeto executivo a ser apresentado pela CONTRATADA;
- 2.6.1.3.11. O cabeamento entre rack e telas deverá estar devidamente fixado na estrutura;
- 2.6.1.3.12. A estrutura deverá ser montada na sala do Centro Integrado de Inteligência e Segurança Cibernética.
- 2.7. Prover soluções de softwares que disponibilizem de forma transparente e em tempo real informações e dados para o Centro Integrado de Inteligência e Segurança Cibernética na ATI poder monitorar e gerenciar a rede como um todo. Utilizar, obrigatoriamente, os mesmos softwares e servidores de gerência, tanto nas soluções adotadas para o conjunto de ferramentas do Centro Integrado de Inteligência e Segurança Cibernética, como nas soluções adotadas para gerenciar os ativos de rede dos PCs, visando monitorar todos os recursos instalados nos PCs, isto é, Firewalls, switches, access points, servidores, e todos os dispositivos que integram a Nova Rede Corporativa. Esta exigência tem o objetivo de garantir que o Centro Integrado de Inteligência e Segurança Cibernética instalado na ATI possa visualizar todos os dispositivos da rede na mesma console, permitindo que os eventos estejam associados e seja possível fazer análise de impacto e causa origem entre equipamentos e dispositivos diferentes;
- 2.8. Disponibilizar todas as soluções de softwares adotadas em um Portal da Rede Corporativa onde os sistemas possam ser localizados e acessados de forma centralizada, o Portal poderá ser hospedado no DATACENTER da ATI;
- 2.9. Responsabilizar-se por efetuar a instalação, configuração e manutenção lógica das plataformas e dos recursos e

aplicações necessárias ao desenvolvimento das atividades dos demais grupos de trabalho pertencentes ao Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

2.10. Prover todos os recursos necessários para o pleno funcionamento das ferramentas de softwares integrantes dos serviços do Centro Integrado de Inteligência e Segurança Cibernética, incluindo servidores, storages, suporte técnico, atualizações, mecanismos de segurança e demais recursos de infraestrutura de rede local como switches, racks, cabeamento estruturado, entre outros correlatos;

2.11. Prover soluções de hardwares que permitam suportar todas as atividades especificadas no serviço do Centro Integrado de Inteligência e Segurança Cibernética, todos os recursos de softwares, incluindo processamento, armazenamento e memória, e equipes especializadas para instalar, configurar, operar e manter os recursos integrantes desta solução;

2.12. Sistema de controle de acesso e videomonitoramento do Centro Integrado de Inteligência e Segurança Cibernética:

2.12.1. Fornecer uma solução de controle de acesso com recursos de biometria para o ambiente operacional do Centro Integrado de Inteligência e Segurança Cibernética, instalado na CONTRATANTE técnica ATI;

2.12.1.1. A solução deve utilizar biometria (impressão digital, reconhecimento facial ou leitura de íris) como método principal de autenticação de usuários;

2.12.1.2. A solução deverá garantir alta precisão e segurança, com tempo de resposta inferior a 2 segundos;

2.12.1.3. A capacidade de armazenamento de perfis biométricos deverá ser dimensionada para atender integralmente ao quantitativo de usuários da sala de monitoramento, bem como dos fiscais e gestores do contrato da CONTRATANTE técnica ATI, contemplando adicionalmente margem técnica para expansão futura, sem degradação de desempenho ou necessidade de reconfiguração estrutural;

2.12.1.4. O sistema de controle de acesso deve fornecer logs detalhados de todas as entradas e saídas, com registro de data, hora e identificação dos usuários;

2.12.1.5. O acesso aos logs deve ser restrito a administradores com autorização adequada;

2.12.1.6. O sistema deve ser integrado ao sistema de vigilância e aos alarmes da instalação para bloqueio automático de portas em caso de incidentes de segurança.

2.12.2. A CONTRATADA deverá utilizar sistema de gerenciamento de CFTV para rastreamento de pessoas dentro do ambiente do Centro Integrado de Inteligência e Segurança Cibernética, garantindo a recuperação das imagens;

2.12.2.1. Filmar toda a área e manter as imagens armazenadas por no mínimo 90 (noventa) dias;

2.12.2.2. Registrar a entrada e saída de visitantes, com identificação individual, em todos os acessos ao Centro Integrado de Inteligência e Segurança Cibernética e manter os registros por no mínimo 90 (noventa) dias;

2.12.2.3. Proteger o perímetro contra intrusão e acesso indevido;

2.12.3. Os softwares de controle de acesso e gerenciamento de CFTV deverão estar licenciados durante o período do contrato com as features de integração e capacidade conforme quantitativos deste projeto;

2.12.4. As soluções devem incluir mecanismos de redundância e backup, garantindo que os sistemas de controle de acesso e gerenciamento de CFTV continuem operacionais mesmo em caso de falha de energia ou falha de hardware;

2.13. Realizar as atividades de configurações de todos os recursos imprescindíveis envolvidos, inclusive os pontos de energia elétrica para ativação deles, as adequações de rede estabilizada, o cabeamento, as calhas e os racks que se fizerem imprescindíveis para o seu pleno funcionamento;

2.14. Garantir o sigilo e a integridade dos dados e imagens transmitidos através destes nos padrões da Nova Rede Corporativa;

2.15. Garantir o pleno funcionamento dos recursos instalados e toda a infraestrutura integrante da solução proposta para a Nova Rede Corporativa de forma integral, com cobertura de 24x7, de forma ininterrupta, de segunda a domingo, inclusive feriados, devendo ter acesso a todos os equipamentos roteadores e switches componentes da Nova Rede Corporativa.

### **3. Processos do Centro Integrado de Inteligência e Segurança Cibernética**

3.1. A CONTRATADA deverá adotar práticas de gestão de serviços de TI alinhadas ao ITIL 4 ou versão superior, contemplando, no mínimo, as seguintes práticas: Gerenciamento de Incidentes, Gerenciamento de Requisições de Serviço, Gerenciamento de Problemas, Habilitação de Mudança, Gerenciamento de Implantação, Gerenciamento de Nível de Serviço, Gerenciamento do Catálogo de Serviços, Monitoramento e Gerenciamento de Eventos, Gerenciamento de Capacidade e Desempenho, Gerenciamento de Disponibilidade, Gerenciamento da Continuidade

de Serviços, Gerenciamento de Segurança da Informação, Gerenciamento de Configuração de Serviços, Gerenciamento de Ativos de TI, Validação e Teste de Serviço e Melhoria Contínua;

3.2. Promover atividades de nivelamento técnico e laboratório, em atenção ao previsto no modelo ITIL, para todas as equipes de serviço vinculadas à operação e à prestação dos serviços do Centro Integrado de Inteligência e Segurança Cibernética (CIISC);

3.3. Todos os processos devem ser estruturados considerando a evolução da maturidade em segurança da informação. Além disso, deve ser elaborado um catálogo de incidentes e serviços, o qual deverá ser previamente aprovado pela equipe técnica da CONTRATANTE antes de sua implementação. A emissão dos relatórios de saída de cada processo deverá seguir, mas não se limitar, à periodicidade definida pela equipe técnica da CONTRATANTE;

3.4. Em complemento aos processos de gerenciamento de serviços e operação acima listados, a CONTRATADA deverá implantar e seguir no mínimo, mas não se limitando a eles, os seguintes processos em suas operações diariamente, ou conforme alinhado com a CONTRATANTE técnica ATI:

3.4.1. Gestão de Ativos:

3.4.1.1. A CONTRATADA deverá realizar o registro detalhado e contínuo de todos os dispositivos conectados à rede da CONTRATANTE, coletando informações essenciais, tais como modelo, sistema operacional, endereço IP, MAC Address, versão de firmware, além de quaisquer outras características relevantes para a gestão e segurança dos ativos. O inventário deverá ser atualizado automaticamente, sempre que houver modificações na rede, e auditado regularmente para garantir sua precisão e integridade;

3.4.1.2. A CONTRATADA deverá implementar e configurar soluções robustas de proteção, detecção e resposta para servidores (EDR/XDR), assegurando que todos os dispositivos estejam protegidos e em conformidade com as políticas de segurança da CONTRATANTE. Essas soluções deverão incluir mecanismos para a detecção de ameaças avançadas e respostas automatizadas. A CONTRATADA também deverá monitorar continuamente a saúde e a eficácia dessas soluções, tomando ações corretivas imediatas em casos de não conformidade ou falha na proteção;

3.4.1.3. A CONTRATADA será responsável por assegurar que todas as atualizações de segurança, correções de vulnerabilidades e patches críticos sejam aplicados tempestivamente nos ativos que possuírem a solução de proteção, detecção e resposta para desktops e servidores, observando os prazos e recomendações estabelecidos pelos respectivos fabricantes, de modo a mitigar a exposição a riscos decorrentes de vulnerabilidades conhecidas;

3.4.1.4. A CONTRATADA deverá implementar políticas de controle de acesso rigorosas para todos os dispositivos, incluindo as soluções unificadas de segurança de rede, garantindo que somente usuários devidamente autorizados tenham acesso aos ativos e informações críticas. Essas políticas deverão incluir autenticação multifator (MFA), além de restrições baseadas em privilégios e funções, conforme as necessidades operacionais da CONTRATANTE. A CONTRATADA deverá auditar e revisar periodicamente esses acessos para assegurar conformidade com as políticas de segurança;

3.4.1.5. A CONTRATADA deverá integrar todos os endpoints ao sistema centralizado de monitoramento da CONTRATANTE, garantindo que os eventos suspeitos, anomalias e potenciais violações de segurança sejam detectados e respondidos em tempo hábil. Todos os logs e dados relevantes dos endpoints deverão ser encaminhados para uma plataforma de análise contínua, com retenção adequada conforme as normas de conformidade da CONTRATANTE e requisitos regulatórios;

3.4.1.6. A CONTRATADA deverá gerar relatórios periódicos, detalhando o status de cada dispositivo monitorado, incluindo informações sobre a integridade, desempenho, conformidade com políticas de segurança e atualizações realizadas. Esses relatórios deverão ser utilizados para auditorias internas, identificação de áreas de melhoria e para o cumprimento das exigências normativas e regulatórias aplicáveis à gestão de ativos.

3.4.2. Campanhas de conscientização:

3.4.2.1. A CONTRATADA deverá realizar uma avaliação preliminar antes do início das campanhas de conscientização, considerando o cenário atual da CONTRATANTE, o perfil de seus colaboradores e os principais riscos aos quais as informações estão expostas. Essa avaliação servirá como base para a elaboração de um plano de ação personalizado e eficaz, visando mitigar os riscos identificados;

3.4.2.2. Com a avaliação concluída e as vulnerabilidades principais identificadas, a CONTRATADA deverá realizar um teste inicial (como phishing simulado ou outra técnica adequada) para estabelecer uma linha de base de comportamento dos colaboradores. Isso permitirá a comparação dos resultados antes e depois da campanha,

possibilitando a medição da eficácia das ações implementadas;

3.4.2.3. A CONTRATADA deverá desenvolver conteúdos didáticos e progressivos em segurança da informação, adaptados ao público-alvo da CONTRATANTE. O conteúdo deverá ser disseminado por meio de diversos canais, como e-mails, vídeos, apresentações, cartazes ou outras mídias apropriadas, e deve ser elaborado em colaboração com a equipe técnica da CONTRATANTE técnica ATI e o time de segurança. Os temas abordados deverão incluir conceitos essenciais de segurança, ameaças comuns e práticas recomendadas para prevenir incidentes;

3.4.2.4. Após a definição do plano de ação e cronograma, a CONTRATADA será responsável pela realização dos treinamentos e pela distribuição do material de conscientização através dos canais definidos. Deve-se garantir que todo o público-alvo seja devidamente alcançado e que os conteúdos estejam acessíveis e claros para todos os colaboradores;

3.4.2.5. Após a aplicação dos treinamentos e divulgação dos materiais, a CONTRATADA deverá realizar novos testes para medir a eficácia das campanhas. Esses testes poderão incluir simulações de ataques, pesquisas de conhecimento ou outros métodos de avaliação. Feedback dos colaboradores e métricas de segurança deverão ser coletados para assegurar que as mensagens foram bem compreendidas e que as práticas de segurança foram melhoradas;

3.4.2.6. A CONTRATADA deverá manter um processo de comunicação contínua, atualizando as campanhas de conscientização conforme necessário. Novos testes e ajustes de conteúdo deverão ser implementados com base nos resultados obtidos e nas mudanças no cenário de segurança da CONTRATANTE;

3.4.2.7. As políticas, comunicações e treinamentos fornecidos pela CONTRATADA deverão ser claros, compreensíveis e acessíveis a todos os colaboradores da CONTRATANTE, independentemente do nível técnico ou cargo;

3.4.2.8. A CONTRATADA deverá personalizar as mensagens de conscientização com base no perfil dos colaboradores ou nos diferentes departamentos e áreas de atuação da CONTRATANTE, garantindo que as campanhas sejam relevantes e eficazes para cada grupo;

3.4.2.9. A CONTRATADA deverá ter a capacidade técnica de coletar dados de comportamento dos usuários (por exemplo, incidentes de segurança e interações com os conteúdos de treinamento) e, de forma automatizada, recomendar módulos específicos de treinamento em comportamento seguro corporativo. Além disso, deverá acompanhar indicadores de adesão e conclusão dos treinamentos, gerando relatórios de cumprimento e desempenho;

3.4.2.10. Devem ser realizados testes de phishing com os usuários da Nova Rede Corporativa, utilizando uma ferramenta que atenda, no mínimo, aos seguintes requisitos:

3.4.2.11. A CONTRATADA deve considerar 5.000 (cinco mil) usuários alvos dos testes de phishing com a ferramenta automatizada e um tempo mínimo de retenção de 1 (um) ano;

3.4.2.11.1. Recursos de Treinamento e Capacitação

3.4.2.11.1.1. Conteúdos Interativos: Disponibilidade de materiais didáticos em diversos formatos (vídeos, quizzes, simulações);

3.4.2.11.1.2. Programas de Treinamento Personalizados: Capacidade de criar trilhas de aprendizagem customizadas de acordo com as necessidades específicas dos colaboradores e falhas identificadas;

3.4.2.11.1.3. Avaliações de Desempenho: Ferramentas para avaliação contínua do progresso dos treinandos, incluindo relatórios detalhados de desempenho;

3.4.2.11.1.4. Feedback em Tempo Real: Fornecimento de feedback imediato para os usuários após a conclusão de módulos e avaliações.

3.4.2.11.2. Integração com Soluções de Segurança

3.4.2.11.2.1. Conectividade com Sistemas de Segurança Cibernética: Integração com diversas ferramentas de segurança já utilizadas pela empresa para obtenção de dados e telemetria;

3.4.2.11.2.2. Identificação de Falhas de Segurança: Análise automática de incidentes de segurança relacionados ao comportamento do usuário, identificando áreas que necessitam de treinamento;

3.4.2.11.2.3. Ações Corretivas Automáticas: Sugestão automática de módulos de treinamento específicos com base nas falhas de segurança detectadas.

3.4.2.11.3. Gestão e Relatórios

3.4.2.11.3.1. Painel de Controle Centralizado: Interface de gestão para administradores acompanharem o progresso dos colaboradores e gerirem os conteúdos e usuários;

3.4.2.11.3.2. Relatórios Customizáveis: Geração de relatórios detalhados e personalizáveis sobre a eficácia dos

treinamentos e o impacto nas falhas de segurança;

3.4.2.11.3.3. Alertas e Notificações: Sistema de notificações automáticas para administradores e colaboradores sobre novas tarefas, falhas detectadas e progresso dos treinamentos.

3.4.2.11.4. Usabilidade e Acessibilidade

3.4.2.11.4.1. Interface Amigável: Design intuitivo e de fácil navegação para todos os níveis de usuários;

3.4.2.11.4.2. Acesso Multiplataforma: Disponibilidade de acesso via dispositivos móveis e desktop, permitindo flexibilidade no treinamento;

3.4.2.11.4.3. Suporte Técnico: Disponibilidade de suporte técnico 24/7 para auxiliar na resolução de problemas e dúvidas.

3.4.2.11.5. Segurança e Conformidade

3.4.2.11.5.1. Proteção de Dados: Garantia de segurança dos dados dos usuários conforme as regulamentações aplicáveis (ex: LGPD, GDPR);

3.4.2.11.5.2. Auditorias e Compliance: Ferramentas para auditoria e conformidade com políticas internas de segurança e regulamentações externas.

3.4.2.11.6. Tipos de Dados e Telemetria a Serem Coletados

3.4.2.11.6.1. Eventos de Login e Logout

3.4.2.11.6.1.1. Fonte: Sistemas de autenticação e controle de acesso.

3.4.2.11.6.1.2. Dados: Tentativas de login, horários de acesso, duração das sessões, falhas de autenticação.

3.4.2.11.6.2. Atividades de Navegação e Interação

3.4.2.11.6.2.1. Fonte: Navegadores web e aplicativos da plataforma.

3.4.2.11.6.2.2. Dados: Páginas visitadas, tempo gasto em cada página, interações com os conteúdos (cliques, respostas a quizzes etc.).

3.4.2.11.6.3. Uso de Recursos de Rede

3.4.2.11.6.3.1. Fonte: Firewalls, proxies e sistemas de monitoramento de rede.

3.4.2.11.6.3.2. Dados: Padrões de tráfego, tentativas de acesso a sites bloqueados, transferência de dados não autorizada.

3.4.2.11.6.4. Detecção de Malware e Phishing

3.4.2.11.6.4.1. Fonte: Sistemas de anti-malware, filtros de e-mail e plataformas de prevenção contra phishing.

3.4.2.11.6.4.2. Dados: Incidentes de detecção, arquivos infectados, links suspeitos clicados.

3.4.2.11.6.5. Comportamento de Uso de Aplicativos

3.4.2.11.6.5.1. Fonte: Sistemas de gestão de dispositivos e aplicativos.

3.4.2.11.6.5.2. Dados: Aplicativos mais utilizados, tentativas de uso de aplicativos não autorizados, padrões de uso fora do horário de trabalho.

3.4.2.12. As campanhas de conscientização deverão acompanhar o cronograma e evolução da maturidade em segurança da informação;

3.4.2.13. Todas as campanhas deverão ter autorização prévia da CONTRATANTE técnica ATI;

3.4.3. Monitoramento de alertas:

3.4.3.1. A CONTRATADA deverá realizar uma análise detalhada do ambiente da CONTRATANTE após a implantação do SIEM, ajustando as regras de detecção de ameaças para personalizá-las conforme as especificidades da rede. Somente as regras relevantes para a infraestrutura da CONTRATANTE deverão ser ativadas, evitando ruídos operacionais (falsos positivos) e garantindo o foco em eventos de maior relevância. Essa personalização deve levar em consideração as melhores práticas do mercado e as diretrizes de segurança vigentes;

3.4.3.2. A CONTRATADA será responsável por configurar o envio contínuo e seguro dos logs dos ativos críticos, conforme definido pela equipe técnica da CONTRATANTE técnica ATI. A solução deverá abranger todos os principais componentes da infraestrutura de TI e garantir que os logs sejam coletados e transmitidos sem interrupções, assegurando que os dados sejam armazenados de maneira segura e estejam disponíveis para análise;

3.4.3.3. A CONTRATADA deverá garantir que o monitoramento do ambiente seja realizado 24 horas por dia, 7 dias por semana, com uma equipe dedicada de analistas. O foco deve ser a priorização dos alertas conforme a criticidade dos ativos, aplicando rigor na identificação de falsos positivos e assegurando que somente os eventos que representam uma ameaça real sejam investigados. A equipe deverá estar preparada para responder rapidamente a incidentes em qualquer momento, mantendo a segurança do ambiente;

3.4.3.4. Todos os alertas gerados deverão ser devidamente registrados pela CONTRATADA após a triagem inicial. Esse registro deve conter informações detalhadas, como descrição do evento, origem do alerta, ativos afetados e as ações iniciais tomadas, de modo a facilitar a análise detalhada posterior e permitir o acompanhamento completo da evolução do incidente;

3.4.3.5. Durante a investigação de um alerta, a CONTRATADA deverá coletar informações detalhadas sobre os ativos impactados, o tráfego de rede envolvido, endereços IP ou URLs externas associadas, e qualquer outra informação relevante. A investigação deverá classificar o nível de criticidade e risco do evento, visando determinar se houve atividade maliciosa e, se confirmada, qual a extensão e impacto da ameaça no ambiente da CONTRATANTE;

3.4.3.6. Após a confirmação de uma atividade maliciosa, a CONTRATADA deverá aplicar imediatamente as medidas corretivas necessárias, que podem incluir bloqueios de IPs, ajustes de políticas de segurança ou outras ações de contenção. Para incidentes críticos, o time de especialistas da CONTRATADA deverá ser acionado para prestar suporte na resposta a incidentes de alta gravidade, sempre com a colaboração da equipe técnica da CONTRATANTE;

3.4.3.7. Após a resolução de cada incidente, a CONTRATADA deverá documentar todos os detalhes, incluindo as ações tomadas e os resultados obtidos. Além disso, deve realizar uma análise crítica para identificar oportunidades de melhoria no processo de monitoramento e resposta. As diretrizes da matriz MITRE ATT&CK devem ser seguidas para maximizar a eficiência das defesas e aprimorar a capacidade de detecção e resposta a futuras ameaças.

#### 3.4.4. Gestão de Riscos:

3.4.4.1. A CONTRATADA deverá realizar a identificação detalhada dos eventos e situações que possam gerar potenciais perdas à CONTRATANTE, considerando os ativos críticos e processos sensíveis da organização. Essa identificação deverá incluir riscos cujas fontes estejam sob controle ou fora do controle da CONTRATANTE, mesmo que as causas não sejam imediatamente aparentes, e deverá especificar claramente como, onde e por que essas perdas podem ocorrer;

3.4.4.2. A CONTRATADA deverá conduzir a análise dos riscos com grau de detalhamento apropriado à criticidade dos ativos e à vulnerabilidade existente. O processo de análise poderá utilizar metodologias qualitativas, quantitativas ou uma combinação de ambas, devendo ser baseado em dados específicos de incidentes anteriores, bem como nas vulnerabilidades identificadas no ambiente da CONTRATANTE;

3.4.4.3. A CONTRATADA deverá, em conjunto com a CONTRATANTE, realizar a comparação dos riscos estimados com os critérios previamente estabelecidos durante a definição do contexto de gestão de riscos. Os critérios de avaliação deverão ser consistentes com os objetivos estratégicos e operacionais da CONTRATANTE e levar em consideração os interesses de todas as partes envolvidas. Esta etapa deverá permitir a priorização dos riscos com base em seu impacto e probabilidade de ocorrência;

3.4.4.4. Com base nos resultados da avaliação, a CONTRATADA deverá recomendar as opções mais adequadas para o tratamento de cada risco, levando em consideração a viabilidade econômica, o custo de implementação e os benefícios esperados. As opções de tratamento devem incluir, mas não se limitar a: mitigação, transferência, aceitação ou evitação dos riscos;

3.4.4.5. A CONTRATADA será responsável pela aplicação prática dos controles de segurança selecionados durante a análise de riscos. Esta fase deverá seguir um ciclo contínuo de aprimoramento, considerando as mudanças no ambiente tecnológico e de negócios, de forma a garantir que os controles se mantenham eficazes ao longo do tempo;

3.4.4.6. A CONTRATADA deverá estabelecer um processo contínuo de monitoramento e revisão dos riscos identificados, assegurando-se de que novas ameaças sejam rapidamente identificadas e que os controles existentes sejam ajustados conforme necessário. Quaisquer melhorias ou ajustes deverão ser comunicados formalmente à CONTRATANTE, com o objetivo de garantir que todas as medidas corretivas sejam implementadas com eficácia;

3.4.4.7. A CONTRATADA deverá promover a troca de informações sobre os riscos entre todas as partes interessadas, incluindo a alta administração, para assegurar que todos estejam cientes da natureza e gravidade dos riscos, bem como das ações tomadas para mitigá-los. Essa comunicação deverá incluir a apresentação regular de relatórios e reuniões de alinhamento, visando aumentar a conscientização organizacional sobre o tema;

3.4.4.8. A CONTRATADA deverá documentar detalhadamente todas as etapas do processo de gestão de riscos, incluindo a identificação de ameaças, vulnerabilidades, impactos e avaliações realizadas. Todos os controles recomendados, bem como as medidas adotadas, deverão ser registrados e relatados à CONTRATANTE com informações sobre sua implementação e resultados esperados;

3.4.4.9. A CONTRATADA deverá revisar periodicamente o processo de gestão de riscos, garantindo que ele seja

atualizado conforme as mudanças no ambiente de negócios e segurança. Essas revisões deverão identificar oportunidades de melhoria e ajustes nos procedimentos, visando a maximização da eficiência e a minimização dos riscos residuais.

3.4.5. Gestão da conformidade:

3.4.5.1. A CONTRATADA deverá identificar, de forma sistemática, todos os sistemas, processos, ou aplicativos que não estejam em conformidade com os requisitos estabelecidos pela CONTRATANTE. Isso inclui, mas não se limita a sistemas com vulnerabilidades conhecidas, ausência de patches de segurança ou quaisquer outras deficiências que comprometam o atendimento às normas e regulamentações aplicáveis à segurança da informação;

3.4.5.2. A CONTRATADA deverá classificar as falhas de conformidade de acordo com seu impacto no negócio e a criticidade dos recursos necessários para sua correção. A priorização deve ser feita com base em uma análise de risco detalhada, considerando tanto o potencial de danos quanto a complexidade e urgência de remediação, em alinhamento com a equipe técnica da CONTRATANTE técnica ATI;

3.4.5.3. Quando forem detectados problemas de conformidade, a CONTRATADA deverá coordenar com a equipe de gerenciamento da CONTRATANTE para determinar a melhor abordagem de resposta. As opções incluem transferir a responsabilidade da correção para a equipe de TI ou outra equipe relevante, ou aceitar o risco associado à não conformidade e deixá-lo sem solução. Essa decisão deve ser tomada de comum acordo entre a CONTRATADA e a equipe técnica da CONTRATANTE técnica ATI, levando em consideração os riscos e o impacto no negócio;

3.4.5.4. Após a implementação das correções necessárias, a CONTRATADA deverá conduzir uma nova avaliação dos sistemas para garantir que estejam em conformidade. Um relatório detalhado deverá ser gerado, confirmando que as mudanças foram aplicadas com sucesso e que todos os sistemas e processos avaliados atendem aos requisitos normativos. Esse relatório deve ser entregue à equipe técnica da CONTRATANTE e utilizado para auditoria e validação de conformidade;

3.4.5.5. A CONTRATADA deverá implementar um processo de monitoramento contínuo da conformidade, capaz de identificar rapidamente tendências e problemas recorrentes, além de fornecer atualizações em tempo real sobre o status de resoluções e exceções. Esse monitoramento contínuo garantirá que novos problemas de não conformidade sejam detectados rapidamente e que as ações corretivas sejam aplicadas de maneira eficiente e oportuna.

3.4.6. Gestão da qualidade da segurança da informação:

3.4.6.1. A CONTRATADA deverá identificar e definir, em conjunto com a CONTRATANTE técnica ATI, os padrões e métricas de qualidade a serem utilizados para avaliar a segurança da informação. Esses padrões devem estar alinhados com os requisitos normativos aplicáveis (como LGPD, ISO/IEC 27001) e as melhores práticas de mercado, garantindo a conformidade e a eficiência das medidas de segurança implementadas;

3.4.6.2. A CONTRATADA deverá definir objetivos claros, específicos e mensuráveis para garantir que os processos e sistemas de segurança da informação atendam a padrões elevados de qualidade. Esses objetivos deverão ser revisados periodicamente para se manterem alinhados com as mudanças no ambiente de TI e nas necessidades da CONTRATANTE;

3.4.6.3. A CONTRATADA será responsável pela criação, implementação e revisão contínua das políticas e procedimentos que suportem a manutenção e a melhoria contínua da qualidade da segurança da informação, em conformidade com as exigências técnicas e regulatórias da CONTRATANTE;

3.4.6.4. A CONTRATADA deverá promover treinamentos regulares para a equipe de TI e segurança, garantindo que todos os colaboradores envolvidos estejam cientes das políticas, procedimentos e melhores práticas de segurança da informação. O treinamento deverá ser atualizado constantemente para refletir novas ameaças e tecnologias emergentes;

3.4.6.5. Após a implementação do sistema de monitoramento de segurança, a CONTRATADA deverá configurar as regras de monitoramento em alinhamento com as especificidades da rede e dos ativos de TI da CONTRATANTE. Essas regras devem ser ajustadas para detectar eventos de segurança com precisão e eficiência, evitando falsos positivos e alertas irrelevantes;

3.4.6.6. A CONTRATADA deverá configurar o envio contínuo e seguro dos logs dos ativos de TI previamente determinados pela CONTRATANTE técnica ATI. Esses logs devem ser armazenados de maneira segura e auditável, garantindo a rastreabilidade e a retenção adequada conforme as políticas de segurança e conformidade;

3.4.6.7. A CONTRATADA será responsável pelo monitoramento contínuo de sistemas e processos de segurança,

analisando os logs e alertas em tempo real para identificar possíveis problemas de qualidade e mitigar riscos de segurança antes que se tornem incidentes críticos;

3.4.6.8. Deverão ser realizadas auditorias periódicas para avaliar a conformidade com os padrões de qualidade definidos. Essas auditorias devem identificar áreas de melhoria e oportunidades para ajustes que garantam a eficácia dos controles de segurança e a aderência aos requisitos normativos;

3.4.6.9. A CONTRATADA deverá realizar análises contínuas do desempenho dos processos de segurança da informação, utilizando as métricas e padrões previamente estabelecidos. O objetivo é identificar desvios e gargalos, propondo melhorias para elevar a qualidade dos controles e procedimentos de segurança;

3.4.6.10. A CONTRATADA deverá gerar relatórios periódicos detalhando o estado da qualidade da segurança da informação. Esses relatórios devem incluir análises sobre o cumprimento dos padrões estabelecidos, identificando áreas de conformidade e aquelas que necessitam de atenção para futuras correções;

3.4.6.11. A CONTRATADA deverá implementar ações corretivas para resolver rapidamente problemas de qualidade identificados, além de propor ações preventivas com base em uma análise crítica dos eventos de segurança, evitando a recorrência de novos problemas ou vulnerabilidades;

3.4.6.12. A CONTRATADA deverá revisar e atualizar regularmente as políticas e procedimentos de segurança da informação, de forma a refletir as mudanças no ambiente de TI, nas ameaças de segurança e nas exigências regulatórias. A atualização contínua deve ser alinhada com a gestão técnica da CONTRATANTE, garantindo que os controles permaneçam eficazes e relevantes.

#### 3.4.7. Inteligência de ameaças cibernéticas

3.4.7.1. A CONTRATADA deverá realizar o monitoramento contínuo e ininterrupto de termos e ativos digitais acessíveis e públicos na internet nos níveis de surface (superfície), deep (profunda) e dark web, monitorando canais como fóruns, redes de compartilhamento de textos e códigos, aplicativos de mensagens, lojas de aplicativos, feeds, phishing, typosquatting, redes sociais, videostreaming, vítimas de malwares e páginas de comércio eletrônico. Deve gerar dados processados, organizados e enriquecidos, obedecendo um ciclo de refinamento e enriquecimento de inteligência de dados, com equipe especializada em threat hunting e inteligência de ameaças cibernéticas (Threat Intelligence);

3.4.7.1.1. O licenciamento da solução deverá contemplar, no mínimo, 5.000 (cinco mil) queries mensais e 1.000 (mil) ativos digitais monitorados. O monitoramento deverá abranger termos, palavras-chave, domínios, subdomínios e outros identificadores relacionados às 3.000 (três mil) localidades governamentais incluídas no escopo, com suporte a, no mínimo, 30 (trinta) fontes de dados, abrangendo os níveis de surface web, deep web e dark web. A solução deverá realizar atualizações em tempo real ou em intervalos de, no máximo, 15 (quinze) minutos.

3.4.7.2. A CONTRATADA deverá adotar metodologias alinhadas com as melhores práticas do mercado para a gestão da inteligência contra ameaças cibernéticas;

3.4.7.3. O processo deve seguir um ciclo de coleta de dados, análise, disseminação e feedback sobre ameaças cibernéticas, com as etapas de planejamento, coleta, processamento, análise, disseminação e feedback;

3.4.7.4. Analisar táticas, técnicas e procedimentos (TTPs) dos atacantes para entender comportamentos e desenvolver medidas de defesa eficazes;

3.4.7.5. Utilizar padrões de mercado para compartilhar e estruturar informações sobre ameaças cibernéticas;

3.4.7.6. Identificar artefatos forenses que indiquem atividades maliciosas;

3.4.7.7. Identificar e priorizar ameaças potenciais utilizando técnicas como STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege). A aplicação da técnica STRIDE será realizada de forma analítica pela equipe de CTI para categorizar e organizar as ameaças identificadas, permitindo um foco direcionado nas ameaças mais relevantes ao ambiente da CONTRATANTE;

3.4.7.8. Detectar anomalias em padrões de comportamento que possam indicar atividades maliciosas. A detecção de anomalias será realizada por meio de análise manual e em conjunto com alertas gerados por ferramentas de SIEM disponíveis no CIISC, permitindo que a equipe de CTI identifique e responda proativamente a potenciais ameaças ao ambiente da CONTRATANTE;

3.4.7.9. Fornecer uma matriz de táticas e técnicas usadas por cibercriminosos para mapear comportamentos de atacantes;

3.4.7.10. Descrever e analisar as fases de um ataque cibernético, desde o reconhecimento até a exfiltração de dados, para interromper ataques em diferentes estágios;

3.4.7.11. O escopo do serviço de Inteligência de Ameaças Cibernéticas inclui, mas não se limita às seguintes fases e etapas, de responsabilidade da CONTRATADA:

3.4.7.11.1. Estratégia:

- 3.4.7.11.1.1. Definição de objetivos claros e específicos para o programa de CTI;
- 3.4.7.11.1.2. Identificação e engajamento das partes interessadas (stakeholders);
- 3.4.7.11.1.3. Planejamento de recursos humanos e tecnológicos necessários;
- 3.4.7.11.1.4. Desenvolvimento de políticas e procedimentos para a gestão de CTI;
- 3.4.7.11.1.5. Elaboração de um plano de comunicação para disseminação da estratégia e objetivos.

3.4.7.11.2. Estruturação:

- 3.4.7.11.2.1. Análise do panorama atual de ameaças e identificação de necessidades específicas;
- 3.4.7.11.2.2. Desenho da arquitetura técnica e operacional de CTI;
- 3.4.7.11.2.3. Seleção e configuração de ferramentas para coleta, análise e disseminação de inteligência;
- 3.4.7.11.2.4. Desenvolvimento de processos e workflows operacionais;
- 3.4.7.11.2.5. Treinamento dos principais stakeholders sobre os fluxos e indicadores do CTI;
- 3.4.7.11.2.6. Integração das novas ferramentas de CTI com os sistemas de segurança existentes;
- 3.4.7.11.2.7. Estabelecimento de indicadores de desempenho (KPIs) para medir a eficácia do programa.

3.4.7.11.3. Implantação:

- 3.4.7.11.3.1. Implementação e configuração das ferramentas de CTI;
- 3.4.7.11.3.2. Início da coleta de dados de fontes externas e integração para consumo de feeds internos;
- 3.4.7.11.3.3. Execução das primeiras análises de ameaças;
- 3.4.7.11.3.4. Desenvolvimento de Dashboards para visualização de inteligência;
- 3.4.7.11.3.5. Realização de testes de funcionamento e ajustes necessários;
- 3.4.7.11.3.6. Criação de templates e processos para relatórios regulares.

3.4.7.11.4. Sustentação:

- 3.4.7.11.4.1. Monitoramento contínuo sobre novas ameaças e vulnerabilidades;
- 3.4.7.11.4.2. Aplicação de atualizações de software e patches de segurança nas ferramentas e plataformas de CTI;
- 3.4.7.11.4.3. Verificação e manutenção regular das ferramentas de CTI;
- 3.4.7.11.4.4. Identificação de tendências de ameaças emergentes;
- 3.4.7.11.4.5. Capacitação contínua da equipe em novas técnicas e ferramentas;
- 3.4.7.11.4.6. Resposta rápida e eficaz a incidentes de segurança detectados.

3.4.7.11.5. Governança:

- 3.4.7.11.5.1. Revisão periódica das políticas de CTI para garantir relevância e eficácia;
- 3.4.7.11.5.2. Realização de auditorias para assegurar conformidade com regulamentos e políticas internas;
- 3.4.7.11.5.3. Análise dos KPIs e ajuste das estratégias conforme necessário;
- 3.4.7.11.5.4. Comunicação regular de resultados e insights para a alta administração;
- 3.4.7.11.5.5. Identificação e mitigação contínua de riscos;
- 3.4.7.11.5.6. Revisão e atualização contínua da estratégia de CTI baseada em novas ameaças e oportunidades.

3.4.7.12. O escopo do serviço contempla o seguinte contexto mínimo de alcance do serviço de Inteligência de Ameaças Cibernéticas:

- 3.4.7.12.1. Monitoramento de surface web, deep web e dark web: Até 400 pessoas de interesse por mês;
- 3.4.7.12.2. Site e contas fraudulentas: 20 takedowns por mês;
- 3.4.7.12.3. Monitoramento de fonte de informações: 100 domínios e subdomínios por mês;

3.4.7.13. Especificações da ferramenta a ser utilizada:

- 3.4.7.13.1. A solução deve coletar inteligência de várias fontes, como Darkweb, Open Source e Technical Research;
- 3.4.7.13.2. A inteligência deve ter uma classificação de confiança com base no padrão da indústria, como (Sistema do Almirantado) para todos os relatórios publicados;
- 3.4.7.13.3. Todos os relatórios de inteligência devem ser pontuados com base em critérios de relevância específicos para o cenário de ameaças do cliente;
- 3.4.7.13.4. A Inteligência de Ameaças enviada deve abranger todas as ameaças relevantes para o Cliente;
- 3.4.7.13.5. A inteligência de ameaças enviada deve cobrir todas as ameaças relevantes ao setor governamental e ataques a organizações semelhantes da CONTRATANTE, tanto em âmbito nacional quanto internacional.

- 3.4.7.13.6. A solução deve monitorar e relatar ameaças em Novas vulnerabilidades e explorações que são discutidas ativamente na Dark Web e em fontes abertas;
- 3.4.7.13.7. A inteligência de ameaças deve ser mapeada para a estrutura MITRE ATT&CK;
- 3.4.7.13.8. A inteligência deve ser fornecida e atualizada em tempo real à medida que novas informações ou contextos são coletados de várias fontes;
- 3.4.7.13.9. A solução deve fornecer informações sobre vazamentos de credenciais por meio de violações de terceiros em uma visualização limpa da linha do tempo;
- 3.4.7.13.10. A solução deve ter uma forte presença em sites da Darknet examinados e somente para convidados, como fóruns e mercados;
- 3.4.7.13.11. A solução deve fazer um amplo monitoramento da Dark Web para inteligência específica da organização, monitorando salas de bate-papo ocultas, sites privados, redes ponto a ponto, plataforma de mídia social, sites do mercado negro e botnets;
- 3.4.7.13.12. A solução deve fazer a descoberta de dados vazados na Dark web, incluindo arquivos confidenciais, dados financeiros/de cartão de crédito, dados pessoais (PII), etc;
- 3.4.7.13.13. A solução deve ser capaz de demonstrar a capacidade de interagir com atores na Dark Web e coletar informações por meio do HUMINT;
- 3.4.7.13.14. A solução deve ter a capacidade de girar para a inteligência em termos de vários filtros, tais como, no mínimo:
- 3.4.7.13.14.1. Nome do adversário;
- 3.4.7.13.14.2. Motivação do adversário;
- 3.4.7.13.14.3. Indústria de destino;
- 3.4.7.13.14.4. Geografia alvo;
- 3.4.7.13.14.5. Tipos de relatórios;
- 3.4.7.13.14.6. Classificações de relevância;
- 3.4.7.13.15. A solução deve ter a capacidade de produzir relatórios de alerta precoce com base em ataques iniciais e futuros e novas táticas, técnicas e procedimentos (TTP);
- 3.4.7.13.16. A solução deve ter a capacidade de relatar exclusivamente Ransomware e ataques TTP relacionados;
- 3.4.7.13.17. A solução deve ter a capacidade de realizar investigação inicial dentro do sistema usando enriquecimentos em tempo real para procurar indicadores de comprometimento (IOCs);
- 3.4.7.13.18. A solução deve ter a capacidade de rastrear e monitorar marcas como:
- 3.4.7.13.18.1. Detecte credenciais violadas, ou seja, e-mails. (No caso de clientes do Banco, os dados do Cartão também podem ser incluídos);
- 3.4.7.13.18.2. Identificar credenciais vazadas que estão disponíveis na dark web;
- 3.4.7.13.18.3. Identifique a fonte da violação de dados (incluindo terceiros);
- 3.4.7.13.18.4. Detecte informações vazadas e dados confidenciais;
- 3.4.7.13.18.5. Capacidade de monitorar o cliente como uma marca para identificar e mitigar quaisquer ataques de phishing iminentes originados externamente, como sites fraudulentos, e-mails maliciosos ou domínios suspeitos que tentem representar a marca;
- 3.4.7.13.18.6. Faça a detecção de sites de phishing através do uso de marcas d'água digitais;
- 3.4.7.13.18.7. Identifique o endereço IP e e-mails de usuários de phishing por meio de campanhas de phishing;
- 3.4.7.13.18.8. Capacidade de identificar nomes de domínio de aparência semelhante que correspondam ao cliente;
- 3.4.7.13.18.9. Serviço de remoção: remoção de conteúdo suspeito (sites/perfil/etc.);
- 3.4.7.13.19. A solução deve fazer a exposição e varredura de Shadow IT: varreduras de portas, dispositivos mal configurados, varreduras de certificados SSL etc.;
- 3.4.7.13.20. A solução deve ter suporte para categorizar as descobertas de inteligência de ameaças por meio do MITRE ATT&CK Framework etc.;
- 3.4.7.13.21. A solução deve ter relatórios de ativos vulneráveis e ativos de sombra de TI;
- 3.4.7.13.22. A solução deve ter a capacidade de escanear e monitorar a infraestrutura de Internet do Cliente para:
- 3.4.7.13.22.1. Identificação de ativos externos relacionados ao Cliente (ex.: domínios, subdomínios, endereços IP públicos e serviços visíveis);
- 3.4.7.13.22.2. Detecção de mudanças nos ativos externos, como novos subdomínios, alterações de DNS, portas

abertas, ou serviços ativos;

3.4.7.13.22.3. Identifique qualquer certificado SSL expirado ou prestes a expirar;

3.4.7.13.23. A solução deve ter as seguintes funcionalidades de gestão:

3.4.7.13.24. Deve ter funções para analisar e investigar indicadores de comprometimento (IOCs) sob demanda, como pesquisas de reputação de IP/Domínio/Hash/CVE para vários parâmetros, tais como, no mínimo:

3.4.7.13.24.1. Informação básica;

3.4.7.13.24.2. Pesquisa na lista negra;

3.4.7.13.24.3. Localização geográfica;

3.4.7.13.24.4. Informações de rede;

3.4.7.13.24.5. Relatórios de inteligência anteriores.

3.4.7.13.25. A plataforma deve ter recursos para fornecer acesso baseado em função, alertas personalizados, alertas flash etc.;

3.4.7.13.26. Deve ter a capacidade de fornecer analista sob demanda para qualquer pesquisa personalizada e requisitos de esclarecimento;

3.4.7.13.27. Você deve dar suporte à segurança adicional fornecendo autenticação de dois fatores para o portal da web;

3.4.7.13.28. A solução deve monitorar pessoas importantes da organização (VIPs), principalmente em sites de Doxing. As redes sociais suportadas deverão ser, no mínimo: Facebook, Instagram, X (antigo Twitter) e LinkedIn;

3.4.7.13.29. A solução deve estar em conformidade com o MITRE, mostrando as ameaças e como elas estão localizadas na matriz;

3.4.7.13.30. A solução deve apresentar uma lista atualizada de agentes de ameaças comuns e palavras-chave da deep e dark web;

3.4.7.13.31. A solução deve trazer informações de inteligência sobre Stealers, mostrando possíveis funcionários e clientes das organizações infectados por esse tipo de malware;

3.4.7.13.32. A solução deve apresentar uma página web com estatísticas de disponibilidade do Portal Web da solução;

3.4.7.13.33. Solução deve oferecer acesso e exportação de informações via Rest API;

3.4.7.13.34. A solução deve oferecer Logs de Auditoria, incluindo informações de logon;

3.4.7.13.35. A solução deve permitir que o analista pesquise na deep e darkweb, incluindo fóruns, sites de colagem, aplicativos de mensagens e outras fontes;

3.4.7.13.36. A solução deverá apresentar, para cada domínio detectado, um relatório de integridade do DNS, abrangendo exclusivamente servidores e registros DNS externos visíveis publicamente;

3.4.7.14. A CONTRATADA deverá disponibilizar um relatório mensal a ser entregue até 10 dias corridos do mês subsequente, contendo no mínimo o detalhamento das ações solicitadas, em andamento e concluídas, bem como suas justificativas e soluções;

3.4.7.15. O serviço deverá ser planejado, implantado e acompanhado de acordo com o que for definido no item de Evolução da maturidade em segurança da informação, a ser aprovado pela CONTRATANTE técnica ATI.

#### 3.4.8. Rotina de Backup

3.4.8.1. A CONTRATADA deverá implementar e operar um processo de rotina de backup, abrangendo todos os sistemas críticos do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), incluindo plataformas de segurança (EDR, SOAR, SIEM, firewalls, entre outros), bancos de dados e documentações estratégicas, garantindo a integridade e disponibilidade dos dados. A solução deverá assegurar a execução de backups incrementais e completos, conforme cronograma definido, e possibilitar a recuperação eficiente em caso de falhas ou desastres;

3.4.8.2. A CONTRATADA será responsável por estabelecer uma política de retenção de dados que contemple:

3.4.8.2.1. Backups incrementais: Retenção mínima de 90 dias;

3.4.8.2.2. Backups completos: Retenção durante todo o período do contrato;

3.4.8.2.3. A retenção deverá seguir as normas de conformidade aplicáveis à CONTRATANTE e atender aos requisitos regulatórios em vigor;

3.4.8.3. A CONTRATADA deverá implementar um modelo de backup em três níveis, conforme descrito abaixo:

3.4.8.3.1. Backup Primário: Armazenamento local em infraestrutura de alta disponibilidade dentro do ambiente da CONTRATADA;

- 3.4.8.3.2. Backup Secundário: Armazenamento em nuvem privada ou híbrida, com criptografia em trânsito e em repouso;
- 3.4.8.3.3. Backup Terciário: Armazenamento offline em mídia física segura, em local isolado, para proteção contra ameaças como ransomware, em ambiente da CONTRATADA;
- 3.4.8.4. A CONTRATADA deverá assegurar que todos os backups sejam criptografados com algoritmos robustos (no mínimo AES-256) e protegidos por autenticação multifator (MFA) para acessos administrativos. Além disso, deverá configurar monitoramento contínuo para detectar falhas nos processos de backup, notificando a CONTRATANTE em tempo real e adotando medidas corretivas imediatas;
- 3.4.8.5. A CONTRATADA será responsável por executar testes regulares de recuperação de desastres para validar a eficácia dos backups. Esses testes deverão ocorrer com a seguinte frequência:
- 3.4.8.5.1. Mensal: Testes parciais de recuperação de sistemas individuais;
- 3.4.8.5.2. Semestral: Testes completos de recuperação de desastres simulados;
- 3.4.8.5.3. Relatórios detalhando os resultados dos testes deverão ser enviados à CONTRATANTE, contendo métricas como RTO (Objetivo de Tempo de Recuperação) e RPO (Objetivo de Ponto de Recuperação);
- 3.4.8.6. A CONTRATADA deverá gerar relatórios periódicos sobre o status dos backups realizados, incluindo dados sobre falhas, conformidade com políticas de retenção, integridade dos dados e ações corretivas tomadas. Esses relatórios deverão ser apresentados à CONTRATANTE em frequência mínima mensal e deverão atender a requisitos de auditorias internas e normativas regulatórias aplicáveis;
- 3.4.8.7. A CONTRATADA será responsável por revisar continuamente o processo de backup e propor melhorias tecnológicas e operacionais à CONTRATANTE, alinhando-se à evolução da maturidade em segurança da informação e às necessidades específicas do CIISC, garantindo a robustez da estratégia de recuperação de desastres.
- 3.4.9. Gestão de vulnerabilidades
- 3.4.9.1. A CONTRATADA deverá monitorar, planejar e executar ações para corrigir ou mitigar as vulnerabilidades, que poderão incluir, mas não se limitam a:
- 3.4.9.1.1. Aplicação de patches de segurança recomendados pelos fabricantes dos firewalls, APs e demais ativos contratados;
- 3.4.9.1.2. Atualização de firmwares e softwares de segurança;
- 3.4.9.1.3. Reconfiguração de dispositivos e políticas de sistemas conforme melhores práticas;
- 3.4.9.1.4. Outras medidas necessárias para garantir a integridade e a segurança dos ativos da Nova Rede Corporativa.
- 3.4.9.2. A CONTRATADA deverá realizar testes de verificação para garantir que as vulnerabilidades foram devidamente corrigidas ou mitigadas, sem introduzir novas falhas ou comprometer a estabilidade da rede;
- 3.4.9.3. A CONTRATADA deverá implementar monitoramento contínuo dos ativos para detectar novas vulnerabilidades, utilizando ferramentas de varredura e monitoramento em tempo real. A equipe alocada deverá acompanhar ativamente novas ameaças e tendências de segurança;
- 3.4.9.4. A CONTRATADA deverá realizar revisões periódicas nos processos de gestão de vulnerabilidades, avaliando a eficácia das medidas adotadas e identificando oportunidades de melhoria. Relatórios detalhados deverão ser elaborados e apresentados à CONTRATANTE;
- 3.4.9.5. A CONTRATADA deverá ajustar e atualizar continuamente as políticas e os procedimentos de segurança, considerando as lições aprendidas, as novas ameaças identificadas e as melhores práticas do setor.
- 3.4.10. Configuração das soluções unificadas de segurança em Alta Disponibilidade (HA)
- 3.4.10.1. A CONTRATADA deverá prover em seu catálogo o serviço de configuração de Alta Disponibilidade (HA) para as Soluções Unificadas de Segurança de Rede;
- 3.4.10.2. O serviço consiste em configurar os Firewalls para operar em modo de alta disponibilidade, garantindo que um dispositivo possa assumir automaticamente as funções do outro em caso de falha;
- 3.4.10.3. A CONTRATANTE aderente poderá solicitar a qualquer momento durante a vigência do contrato, o serviço de Alta Disponibilidade (HA) para a Solução Unificada de Segurança de Rede;
- 3.4.10.4. A configuração deve garantir a continuidade do serviço de rede e a integridade dos dados durante e após o processo de failover;
- 3.4.10.5. O monitoramento e gerenciamento da Solução Unificada de Segurança de Rede e da Solução Unificada de Segurança para Datacenter permanecerá dentro do escopo de serviços do Centro Integrado de Inteligência e

Segurança Cibernética, de responsabilidade da CONTRATADA;

3.4.10.6. A CONTRATADA deverá realizar uma análise inicial da infraestrutura de rede e dos Firewalls existentes para identificar requisitos específicos para a configuração de Alta Disponibilidade (HA);

3.4.10.7. A CONTRATADA deverá desenvolver um plano detalhado para a configuração de HA, incluindo topologia de rede, procedimentos de failover, testes de funcionalidade e plano de contingência;

3.4.10.8. A CONTRATANTE aderente será responsável por custear a contratação e implantação dos links e soluções unificadas de segurança de rede, assegurando que possuam redundância para suportar a configuração de Alta Disponibilidade (HA);

3.4.10.9. A CONTRATADA será integralmente responsável pelo fornecimento, implantação, suporte e manutenção de toda a infraestrutura necessária para prestação deste serviço de Alta Disponibilidade (HA), sem que isso acarrete custos adicionais para a CONTRATANTE aderente;

3.4.10.10. Todos os equipamentos necessários para ativação do serviço de Alta Disponibilidade (HA), como cabos e transceptores adequados à devida configuração do ambiente deverão ser fornecidos pela CONTRATADA;

3.4.10.11. Requisitos mínimos do serviço, de responsabilidade da CONTRATADA, mas não se limitando a eles:

3.4.10.12. A configuração de HA deverá ser realizada em modo "Ativo-Passivo" ou "Ativo-Ativo", devendo ser definido no plano de configuração a ser apresentado pela CONTRATADA à CONTRATANTE para validação antes da execução do serviço;

3.4.10.13. Configuração de heartbeat entre os Firewalls para detectar falhas rapidamente;

3.4.10.14. O intervalo do heartbeat a ser configurado deve ser de 1 segundo e a contagem deve ser entre 3 e 5 heartbeats para acionamento do failover;

3.4.10.15. Sincronização de sessões ativas e tabelas de estado para garantir continuidade sem perda de dados;

3.4.10.16. Implementação de monitoramento de interfaces e links críticos para detecção de falhas;

3.4.10.17. Configuração para failover automático em caso de falha de hardware ou software;

3.4.10.18. O tempo de failover deverá ser inferior a 10 segundos;

3.4.10.19. Realização de testes de failover planejados para verificar a funcionalidade e a confiabilidade da configuração de HA;

3.4.10.20. Verificação do desempenho dos Firewalls em modo HA sob cargas simuladas de tráfego de rede;

3.4.10.21. Manter os Firewalls atualizados com as últimas versões de firmware para garantir que todas as melhorias de desempenho e correções de bugs estejam implementadas, realizando testes de firmware antes da atualização no ambiente de produção do cliente;

3.4.10.22. Fornecer a CONTRATANTE técnica ATI documentação detalhada de todas as etapas da configuração do serviço de HA, incluindo procedimentos de failover e recuperação, diagramas de rede e relatórios de teste.

#### **4. Serviço de análise de segurança de primeiro nível**

4.1. A equipe deve realizar o monitoramento proativo do Centro Integrado de Inteligência e Segurança Cibernética além de executar atividades relacionadas à configuração de segurança, geração de relatórios, atendimento reativo de incidentes e requisições;

4.2. O time deverá atuar em regime de 24 x 7 x 365 (24 horas por dia, 7 dias por semana, todos os dias do ano);

4.3. Responsabilidades do analista de primeiro nível incluem, mas não se limitam a:

4.3.1. Monitoramento contínuo dos alertas de segurança: Vigilância constante dos sistemas para detectar atividades suspeitas ou anômalas;

4.3.2. Caça e identificação de anomalias que possam indicar atividades maliciosas: Análise proativa de padrões e comportamentos para identificar potenciais ameaças;

4.3.3. Identificação, registro e investigação de alertas de segurança, incluindo classificação e priorização com base no impacto potencial: Avaliação de alertas para determinar gravidade e urgência, registrando informações relevantes;

4.3.4. Análise de incidentes de segurança para determinar a natureza e a extensão das ameaças: Investigação detalhada da origem, método e escopo de um ataque;

4.3.5. Coleta de informações relevantes e escalonamento de incidentes críticos para o grupo de especialistas: Compilação de dados essenciais para o encaminhamento de casos graves a analistas experientes;

4.3.6. Execução de procedimentos de resposta a incidentes pré-definidos e aplicação de correções para mitigar o impacto: Adoção de ações corretivas conforme os protocolos estabelecidos, visando minimizar os danos;

- 4.3.7. Geração de relatórios pós-incidentes para análise e melhoria contínua: Criação de documentação detalhada para revisão e aprimoramento dos processos;
- 4.3.8. Participação contínua em treinamentos para desenvolver habilidades e enfrentar novos desafios: Envolvimento regular em capacitações para manter-se atualizado sobre as últimas ameaças e técnicas;
- 4.3.9. Contribuição na atualização das regras de detecção de eventos de segurança: Colaboração na revisão e aprimoramento das regras de detecção para garantir respostas eficazes a novas ameaças;
- 4.3.10. Atendimento a solicitações: Resposta eficiente e profissional a pedidos e consultas relacionados à segurança da informação oriundas do Service Desk ou diretamente pela CONTRATANTE técnica ATI;
- 4.3.11. Atendimento de incidentes reativos: Resolução de incidentes relatados diretamente pelos clientes;
- 4.3.12. Emissão de relatórios periódicos: Preparação e distribuição regular de relatórios que detalhem o status atual e histórico de incidentes de segurança;
- 4.3.13. Emissão de relatórios personalizados conforme solicitação do cliente: Criação de relatórios específicos, proporcionando insights sob demanda.

## 5. Serviço de análise de segurança especializada

- 5.1. A equipe deverá ser composta por um grupo multidisciplinar de profissionais, incluindo especialistas com qualificações em diferentes áreas de tecnologia da informação e segurança cibernética;
- 5.2. O grupo deverá atuar em regime de expediente nos dias úteis, de segunda a sexta-feira, das 7h às 19h, com a disponibilidade de regime de plantão para cobertura de incidentes e acionamentos fora desse horário, conforme demanda oriunda dos Analistas de Primeiro Nível;
- 5.3. As atividades e responsabilidades do grupo de especialistas incluirão, mas não se limitarão a:
  - 5.3.1. Realizar análise e resposta a incidentes críticos, avaliando a gravidade e o impacto dos incidentes e implementando as ações corretivas necessárias;
  - 5.3.2. Documentar as táticas, técnicas e procedimentos (TTPs) dos atacantes, registrando detalhadamente os métodos utilizados para aprimorar a capacidade de defesa cibernética;
  - 5.3.3. Identificar e desenvolver novos indicadores de comprometimento (IOCs) com base em análises de incidentes e inteligência de ameaças, visando à detecção precoce e mitigação de riscos;
  - 5.3.4. Configurar, otimizar e ajustar ferramentas de segurança e sistemas de detecção para garantir sua eficácia operacional;
  - 5.3.5. Desenvolver e aprimorar scripts ou ferramentas de automação para tarefas repetitivas, com o objetivo de aumentar a eficiência dos processos;
  - 5.3.6. Fornecer treinamento técnico especializado aos Analistas de Primeiro Nível, capacitando-os em práticas avançadas de segurança cibernética;
  - 5.3.7. Participar ativamente da definição de estratégias de segurança cibernética, desenvolvendo e implementando planos de segurança alinhados aos objetivos organizacionais e aos riscos específicos;
  - 5.3.8. Gerenciar ameaças avançadas, como Ataques Persistentes Avançados (APT), desenvolvendo contramedidas eficazes para enfrentar ameaças complexas e persistentes;
  - 5.3.9. Conduzir pesquisas sobre novas ameaças, vulnerabilidades e métodos de remediação, acompanhando as últimas tendências em segurança da informação;
  - 5.3.10. Avaliar a implementação de novas tecnologias e medidas que contribuam positivamente para o fortalecimento da segurança da informação;
  - 5.3.11. Contribuir para o desenvolvimento e revisão de políticas, procedimentos e diretrizes de segurança, garantindo sua atualização e adequação às melhores práticas;
  - 5.3.12. Participar de auditorias de segurança, garantindo conformidade com regulamentações e normas vigentes, além de contribuir para o processo de certificação quando aplicável;
  - 5.3.13. Realizar a implantação de equipamentos e soluções de segurança cibernética, de acordo com as especificações técnicas estabelecidas;
  - 5.3.14. Atender a incidentes e solicitações escalonadas pelos Analistas de Primeiro Nível, providenciando a resolução ou o encaminhamento necessário;
  - 5.3.15. O grupo de especialistas deverá possuir conhecimento comprovado e atuar nas seguintes áreas:
    - 5.3.15.1. Segurança de endpoint;

- 5.3.15.2. Segurança de rede sem fio;
- 5.3.15.3. Configuração e gestão de Firewalls;
- 5.3.15.4. Segurança de perímetro de redes locais;
- 5.3.15.5. Sistemas de monitoramento e análise de eventos de segurança (SIEM);
- 5.3.15.6. Firewalls de aplicações web (WAF);
- 5.3.15.7. Solução de automação de resposta a incidentes de segurança (SOAR);
- 5.3.15.8. Conformidade com normas e regulamentos de segurança;
- 5.3.15.9. Diagnóstico de falhas e desempenho de sistemas;
- 5.3.15.10. Redes de computadores e sua segurança.
- 5.3.15.11. Consultoria de Redes Sem Fio
  - 5.3.15.11.1 O serviço de consultoria de redes sem fio tem como objetivo fornecer orientação estratégica e operacional para a infraestrutura de rede sem fio da Nova Rede Corporativa;
  - 5.3.15.11.2. O consultor poderá ser compartilhado com outros clientes da CONTRATADA, prestando ao menos 8h semanais de serviço ao CIISC;
  - 5.3.15.11.3. Definir e supervisionar a arquitetura e governança da rede sem fio, assegurando que as políticas de segurança e desempenho estejam alinhadas às necessidades da CONTRATANTE;
  - 5.3.15.11.4. Desenvolver recomendações para melhorias na infraestrutura de rede sem fio, considerando a implantação de novas tecnologias;
  - 5.3.15.11.5. Avaliar soluções de segurança para redes sem fio, incluindo autenticação, criptografia, segmentação e detecção de ameaças;
  - 5.3.15.11.6. Planejar e supervisionar a implementação de soluções de otimização de redes sem fio, incluindo balanceamento de carga, QoS e mitigação de interferências;
  - 5.3.15.11.7. Apoiar investigações de incidentes de segurança e anomalias na rede sem fio, garantindo a rastreabilidade e resposta eficaz;
  - 5.3.15.11.8. Propor estratégias para expansão e modernização da rede sem fio, alinhadas com as necessidades futuras da CONTRATANTE;
  - 5.3.15.11.9. Apoiar na elaboração de relatórios periódicos sobre o status, desempenho e segurança da rede sem fio.

## 6. Serviço de acompanhamento de reparos

- 6.1. A CONTRATADA deverá disponibilizar analista(s) de suporte residente(s), com alocação presencial no CIISC nas dependências da CONTRATANTE, no horário de funcionamento da ATI, com capacidade técnica compatível com a criticidade e volumetria do ambiente, sendo responsável(is) pela gestão ponta a ponta do ciclo de vida de incidentes e requisições relacionados à rede corporativa;
- 6.2. O(s) analista(s) de suporte residente(s) deverá(ão) atuar como ponto focal técnico-operacional, assegurando o controle, a rastreabilidade e o cumprimento dos Níveis Mínimos de Serviço (NMS), bem como a integração entre Service Desk, operação do CIISC e prestadores de serviços;
- 6.3. Constituem atribuições mínimas:
- 6.3.1. Receber, qualificar, classificar e priorizar todos os tickets oriundos do Service Desk, NOC, SOC ou demais áreas autorizadas, assegurando o correto enquadramento quanto à criticidade, impacto e urgência, conforme matriz de priorização definida pela CONTRATANTE;
  - 6.3.2. Realizar o escalonamento formal junto aos prestadores de serviços, garantindo a completa instrução dos chamados com evidências técnicas, logs, testes realizados e demais informações necessárias para diagnóstico célere;
  - 6.3.3. Executar o acompanhamento ativo e contínuo dos tickets escalonados, com atuação proativa na cobrança de prazos, validação de diagnósticos e direcionamento de ações corretivas, de forma a assegurar o cumprimento integral dos NMS estabelecidos;
  - 6.3.4. Manter comunicação estruturada, tempestiva e auditável com todas as partes envolvidas, incluindo atualizações periódicas de status, notificações de incidentes críticos, relatórios de progresso e comunicação de normalização;

- 6.3.5. Atuar na gestão de incidentes críticos e de alta severidade, incluindo coordenação de salas de guerra, acionamento de múltiplos níveis de suporte e garantia de resposta em tempo compatível com os requisitos de continuidade do serviço;
- 6.3.6. Validar tecnicamente as soluções aplicadas pelas equipes, incluindo testes de restabelecimento, análise de causa raiz e verificação de aderência aos padrões de qualidade exigidos;
- 6.3.7. Realizar análise contínua de incidentes, identificando recorrências, desvios de desempenho e oportunidades de melhoria, devendo propor ações corretivas, preventivas e evolutivas baseadas em dados;
- 6.3.8. Produzir e manter relatórios gerenciais e técnicos, incluindo indicadores de desempenho, tempo médio de atendimento (MTTA), tempo médio de reparo (MTTR), reincidência de falhas e conformidade com NMS;
- 6.3.9. Garantir a adequada documentação de todos os atendimentos, interações e evidências em sistema de gestão de serviços, assegurando rastreabilidade, auditoria e conformidade com boas práticas de governança;
- 6.3.10. Atuar em conformidade com políticas, normas e procedimentos de segurança da informação, continuidade de negócios e operação definidos pela CONTRATANTE, incluindo requisitos aderentes a frameworks como ITIL e controles compatíveis com ISO 27001;
- 6.3.11. Apoiar tecnicamente a CONTRATANTE na validação de mudanças, janelas de manutenção e intervenções programadas que possam impactar a conectividade;
- 6.3.12. Garantir disponibilidade compatível com o regime operacional da rede corporativa, incluindo atuação em horários estendidos, sobreaviso ou plantões, quando requerido.
- 6.3.13. Realizar diagnóstico técnico aprofundado, incluindo análise de rede, testes de conectividade, verificação de equipamentos e correlação de eventos, visando identificar a causa raiz do problema;
- 6.3.14. Executar as ações corretivas necessárias para restabelecimento do serviço, incluindo intervenções remotas e acionamento de equipes de campo, quando aplicável;
- 6.3.15. Escalonar internamente os chamados, garantindo tratamento adequado conforme complexidade e criticidade.

## **7. Serviço de atenção especializada ao cliente**

- 7.1. O Especialista de Atenção será responsável por oferecer atendimento especializado e personalizado aos clientes, compreendendo claramente suas necessidades específicas e atuando como ponto focal para demandas complexas relacionadas à conectividade e segurança da informação;
- 7.2. O Especialista deverá realizar uma análise detalhada dos requisitos de conectividade e segurança dos clientes, identificando vulnerabilidades, oportunidades de melhoria e propondo soluções técnicas que atendam tanto às necessidades imediatas quanto às estratégias de longo prazo dos clientes;
- 7.3. Será necessário prestar suporte técnico especializado, assegurando a resolução eficaz de problemas e questionamentos, com foco na qualidade do atendimento, garantindo uma comunicação clara e transparente com os clientes;
- 7.4. O Especialista será responsável pela coordenação das equipes técnicas envolvidas na implementação das soluções propostas, garantindo que as melhores práticas do setor sejam aplicadas durante todo o processo, e assegurando que as entregas ocorram dentro dos prazos e padrões de qualidade previamente estabelecidos;
- 7.5. O Especialista deverá monitorar continuamente o desempenho das soluções implementadas, assegurando seu correto funcionamento e realizando manutenções preventivas e corretivas sempre que necessário. Além disso, será necessário que o Especialista se mantenha atualizado quanto a novas tecnologias e tendências, propondo melhorias contínuas que possam maximizar a eficiência e a segurança dos sistemas dos clientes.

## **8. Serviço de análise de qualidade**

- 8.1. O Analista de Qualidade deverá acompanhar e avaliar a execução dos serviços contratados com base nos Níveis Mínimos de Serviço (NMSs) estabelecidos neste Termo de Referência, utilizando indicadores de desempenho e metas

previamente definidos;

8.2. Prestar o serviço de Monitoração de Níveis Mínimos de Serviço, realizando atividades de gestão de Níveis Mínimos de Serviço do contrato, coletando, medindo, monitorando e reportando os indicadores de Níveis Mínimos de Serviços contratados (NMS), para todos os pontos clientes da Nova Rede Corporativa, disponibilizando os dados em repositório de dados para a mensuração dos dados de indicadores;

8.2.1. Acompanhar e avaliar os serviços contratados utilizando Níveis Mínimos de Serviços (NMS) estabelecidos neste Termo de Referência, baseando-se em indicadores e metas, definidos para o processo;

8.2.2. Disponibilizar um catálogo de serviços para permitir apresentar os indicadores associados a cada um desses itens de serviços;

8.2.3. Apresentar e gerenciar melhorias dos serviços oferecidos dentro do processo de Monitoração de Níveis Mínimos de Serviço;

8.2.4. Criar processos e padronizar os modelos de relatórios e documentos, com indicadores de desempenho;

8.2.5. Fazer a gestão do Nível Mínimo de Serviço de todas as métricas dos serviços contratados;

8.2.6. Disponibilizar relatórios gerenciais regulares dos NMS dos serviços monitorados;

8.2.7. Monitorar os indicadores dos serviços para avaliar desvios e tendências do comportamento desejável;

8.2.8. Apresentar em portal via WEB, permanentemente, os indicadores de NMS disponíveis dos serviços da Nova Rede Corporativa;

8.2.9. Elaborar e efetuar a apresentação mensal de livros de registros, contendo capítulos que evidenciem através de relatório, os eventos tratados no âmbito de cada serviço de operação e suporte do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

8.2.10. Sugerir planos de ação de melhoria para os componentes gerenciados que estiverem apresentando tendências de desvio do comportamento desejável;

8.2.11. Realizar anualmente a medição da maturidade em gerenciamento de projetos, através de pesquisas, auditorias e elaboração de planos para a elevação contínua da qualidade do gerenciamento;

8.2.12. Disponibilizar suporte ao gerenciamento visual dos Níveis Mínimos de Serviço;

8.2.13. Definir e calcular os principais indicadores de desempenho a partir de uma perspectiva de negócio;

8.2.14. Permitir calcular penalidades financeiras a serem aplicadas à CONTRATADA ou a outros contratados para execução dos serviços da Nova Rede Corporativa;

8.2.15. Disponibilizar um painel integrado, de onde seja possível monitorar, em tempo real, os serviços e o desempenho naquele momento do NMS;

8.2.16. Permitir a integração com a solução de gerenciamento utilizada para obter os dados de gerenciamento dos ativos, comparar com as metas dos indicadores e disponibilizar na solução.

8.3. A CONTRATADA deverá disponibilizar um catálogo de serviços que apresente de forma clara os indicadores associados a cada item de serviço, facilitando o monitoramento e a avaliação contínua;

8.4. O analista de qualidade será responsável por desenvolver e padronizar processos, relatórios e documentos, estabelecendo modelos consistentes que incluam indicadores de desempenho, assegurando uma visão estruturada e completa dos serviços prestados;

8.5. Deverá gerenciar eficientemente os NMSs de todas as métricas relacionadas aos serviços contratados, garantindo que estejam em conformidade com os acordos estabelecidos entre as partes;

8.6. A CONTRATADA deverá fornecer relatórios gerenciais regulares, documentando o desempenho dos NMSs dos serviços monitorados, possibilitando o acompanhamento contínuo e a tomada de decisões embasadas;

8.7. O Analista deverá monitorar constantemente os indicadores de desempenho dos serviços, identificando possíveis desvios e tendências, e assegurando que as metas e padrões acordados sejam mantidos;

8.8. Caso sejam identificados desvios nos serviços em relação ao desempenho desejado, o analista de qualidade deverá propor e implementar planos de ação corretivos ou preventivos, visando a melhoria contínua dos processos e da prestação dos serviços;

8.9. Será disponibilizado um painel integrado de monitoramento para o acompanhamento em tempo real dos serviços e do desempenho dos NMSs, garantindo visibilidade imediata e transparência sobre o status operacional;

8.10. O analista deverá garantir a integração da solução de gerenciamento de ativos com os sistemas de monitoramento, facilitando a comparação dos dados gerados com as metas estabelecidas e garantindo que essas informações estejam acessíveis e claras para todas as partes envolvidas;

- 8.11. O setor de qualidade será responsável por assegurar a excelência na execução do projeto e a satisfação do cliente, coordenando as equipes envolvidas e garantindo que os processos estejam alinhados com as melhores práticas do mercado;
- 8.12. Deverá definir, implementar e manter processos de qualidade, assegurando sua adesão por todas as equipes envolvidas no projeto e promovendo uma cultura de qualidade em todas as fases do serviço;
- 8.13. O analista deverá realizar inspeções regulares e avaliações detalhadas, assegurando a conformidade das entregas e dos serviços com os padrões de qualidade estabelecidos neste Termo de Referência;
- 8.14. O analista de qualidade deverá identificar e implementar oportunidades de melhoria contínua nos processos e nas entregas, com foco na excelência operacional e na satisfação do cliente;
- 8.15. Será de responsabilidade do analista identificar e mitigar riscos relacionados à qualidade do projeto, assegurando que os serviços sejam entregues dentro dos padrões acordados, sem comprometer a segurança ou a integridade da operação;
- 8.16. O analista deverá manter uma comunicação eficaz com as equipes internas e com o cliente, garantindo o alinhamento das expectativas e transparência no gerenciamento dos serviços;
- 8.17. A CONTRATADA será responsável pela emissão de relatórios detalhados e pelo gerenciamento dos indicadores de desempenho dos serviços, fornecendo uma visão clara do progresso e da conformidade dos NMSs;
- 8.18. Os analistas de qualidade da CONTRATADA deverão participar de reuniões mensais com a CONTRATANTE técnica ATI, com o objetivo de avaliar o cumprimento dos NMSs e garantir a conformidade com os padrões de qualidade estabelecidos;
- 8.18.1. As reuniões deverão ocorrer mensalmente, dentro de um prazo de até 15 (quinze) dias corridos após o fechamento do mês anterior, com a participação ativa dos analistas de qualidade e da GRC da CONTRATANTE técnica ATI;
- 8.18.2. Durante essas reuniões, serão discutidos os resultados operacionais, os níveis de serviço atingidos e quaisquer desvios ou problemas identificados, assegurando a implementação de ações corretivas rápidas e eficazes;
- 8.18.3. A CONTRATADA deverá apresentar relatórios detalhados sobre o desempenho do conjunto de sistemas e processos que integram o gerenciamento da rede, proporcionando uma visão abrangente do status dos serviços. Esses relatórios deverão incluir informações completas sobre os NMSs, desempenho operacional, incidentes e quaisquer outras métricas relevantes para a gestão da qualidade;
- 8.18.4. Os relatórios deverão ser enviados por e-mail e disponibilizados em um repositório digital acessível, com capacidade para armazenar todos os dados e documentos gerados durante o período de execução dos serviços;
- 8.18.5. O repositório digital deverá ser acessível à CONTRATANTE técnica ATI, garantindo transparência e permitindo auditoria e verificação contínua das informações e do desempenho dos serviços;
- 8.18.6. O prazo máximo para a disponibilização dos relatórios será até o 5º dia útil do mês subsequente após a coleta e análise dos dados, podendo ser ajustado os intervalos, caso haja acordo prévio entre a ATI e a CONTRATADA;

## **9. Serviço de coordenação do CIISC**

- 9.1. Gerenciamento do projeto:
- 9.1.1. Efetuar o gerenciamento contínuo do portfólio do projeto, abrangendo todas as atividades necessárias para a coordenação e acompanhamento dos subprojetos e iniciativas associadas;
- 9.1.2. Conduzir workshops para validação das prioridades do portfólio, promovendo a sensibilização e o alinhamento com os interlocutores designados;
- 9.1.3. Consolidar o portfólio final de projetos, garantindo a definição clara de objetivos, prazos e responsabilidades;
- 9.1.4. Implantar e configurar uma ferramenta de planejamento e acompanhamento de projetos, que permita a gestão eficiente e transparente do progresso das atividades;
- 9.1.5. Realizar o gerenciamento contínuo do portfólio de subprojetos da Nova Rede Corporativa, assegurando a integração e sinergia entre os diferentes elementos e frentes de trabalho;
- 9.1.6. Planejar a implementação dos processos de entrega, manutenção e gestão de mudanças, bem como elaborar o catálogo de serviços e a matriz de responsabilidades, contemplando clientes e fornecedores envolvidos;
- 9.1.7. Desenvolver um cronograma detalhado para execução do projeto, com etapas e marcos intermediários bem definidos;
- 9.1.8. Identificar e alocar os recursos humanos, tecnológicos e financeiros necessários para a execução das atividades

previstas;

9.1.9. Assegurar a disponibilidade contínua dos recursos durante todo o ciclo de vida do projeto, com planejamento e substituições adequadas quando necessário;

9.1.10. Acompanhar o progresso do projeto em relação ao cronograma estabelecido, reportando eventuais desvios e tomando medidas corretivas;

9.1.11. Identificar riscos potenciais e desenvolver estratégias de mitigação apropriadas, com revisões periódicas;

9.1.12. Monitorar o orçamento do projeto e realizar o controle dos custos, garantindo aderência ao orçamento aprovado;

9.1.13. Facilitar a comunicação entre todas as partes interessadas, estabelecendo um fluxo de informações claro e eficiente;

9.1.14. Assegurar que todas as partes envolvidas estejam informadas sobre o progresso do projeto, com atualizações regulares;

9.1.15. Manter registros detalhados e organizados de todas as atividades do projeto, para referência futura e conformidade com as melhores práticas de gestão de projetos;

9.1.16. Preparar relatórios regulares de status do projeto, contemplando a análise de progresso, desafios e decisões tomadas;

9.1.17. Garantir que todas as entregas do projeto atendam aos padrões de qualidade estabelecidos, com validação formal dos resultados;

9.1.18. Implementar processos de controle de qualidade ao longo das fases do projeto, com critérios de aceitação definidos;

9.1.19. Documentar as lições aprendidas e as recomendações para projetos futuros, consolidando as práticas que contribuíram para o sucesso ou identificando áreas de melhoria;

9.2. Liderança dos times:

9.2.1. O profissional será responsável por liderar e gerenciar as operações do Centro Integrado de Inteligência e Segurança Cibernética, garantindo que as atividades sejam executadas de forma eficiente, eficaz e alinhadas com as metas estratégicas da CONTRATANTE;

9.2.2. As principais responsabilidades do líder incluem:

9.2.2.1. Exercer a liderança técnica das equipes, orientando-as sobre as melhores práticas e soluções tecnológicas em segurança cibernética;

9.2.2.2. Direcionar os times em relação às suas responsabilidades, assegurando que todos os membros compreendam claramente suas funções, metas e objetivos;

9.2.2.3. Motivar, supervisionar e coordenar as equipes para alcançar os objetivos definidos, promovendo um ambiente de trabalho produtivo, colaborativo e inovador;

9.2.2.4. Identificar as necessidades de treinamento e capacitação dos membros da equipe, facilitando o desenvolvimento profissional contínuo e alinhado às novas tecnologias e tendências de segurança;

9.2.2.5. Assegurar que as equipes tenham acesso aos recursos técnicos, ferramentas e suporte adequados para desempenhar suas funções com excelência, eficiência e agilidade;

9.2.2.6. Monitorar a execução das atividades operacionais para garantir que sejam realizadas de maneira eficaz, dentro dos prazos estabelecidos e de acordo com os padrões de qualidade e segurança acordados;

9.2.2.7. Colaborar na definição, implementação e aprimoramento contínuo dos processos, políticas e diretrizes de segurança cibernética, visando a melhoria da eficiência operacional e da proteção dos sistemas;

9.2.2.8. Implementar e garantir a adesão às melhores práticas e normas de segurança cibernética reconhecidas, assegurando a conformidade com regulamentos nacionais e internacionais;

9.2.2.9. Coordenar respostas rápidas e eficazes a incidentes críticos de segurança, minimizando os impactos operacionais e assegurando a rápida restauração da normalidade;

9.2.2.10. Gerenciar o recrutamento, treinamento e desenvolvimento de novos profissionais para o Centro Integrado de Inteligência e Segurança Cibernética, garantindo que a equipe esteja bem preparada para enfrentar os desafios atuais e futuros da segurança cibernética;

9.2.2.11. Fornecer assessoria técnica e estratégica à CONTRATANTE técnica ATI sobre medidas de segurança cibernética e investimentos em tecnologias de proteção, garantindo o alinhamento das necessidades de segurança com os objetivos do negócio;

- 9.2.2.12. Identificar e propor oportunidades de melhorias nos processos de resposta a incidentes de segurança, buscando aumentar a eficiência e a rapidez na resolução de incidentes;
- 9.2.2.13. Participar de auditorias de segurança e conformidade, garantindo que as operações e processos do CIISC estejam alinhados com as exigências regulatórias e com os padrões de mercado;
- 9.2.2.14. Assegurar que todas as entregas sob sua coordenação sejam preparadas em conformidade com os padrões de qualidade estabelecidos, submetendo-as ao fluxo de validação formal do CIISC e ao devido aceite no Sistema de Gestão de Ordem de Serviço (SGOS).
- 9.3. Coordenação do Centro Integrado de Inteligência e Segurança Cibernética:
- 9.3.1. A CONTRATADA deverá prestar o serviço de coordenação do Centro Integrado de Inteligência e Segurança Cibernética em horário comercial, de segunda a sexta-feira, das 08h00 às 18h00, e, eventualmente, em horários extraordinários, conforme demanda da CONTRATANTE técnica ATI ou em casos de necessidade operacional do serviço;
- 9.3.2. A CONTRATADA deverá apresentar relatórios periódicos à CONTRATANTE técnica ATI sobre o cumprimento dos Níveis Mínimos de Serviço (NMS), conforme especificado no ADENDO II deste Termo de Referência. Estes relatórios devem incluir todas as informações relevantes sobre a operação e o desempenho do conjunto de sistemas gerenciados na rede, a serem disponibilizados em meio digital (rtf, xls, pdf e txt), via e-mail e em repositório digital com capacidade para manter o histórico durante todo o período de vigência contratual. A periodicidade máxima para disponibilização será de até o 5º (quinto) dia útil, podendo ser reduzida mediante acordo entre ATI e CONTRATADA;
- 9.3.3. Apoiar a integração das atividades realizadas pelas equipes especializadas do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa com as atividades da equipe da ATI, promovendo coesão e alinhamento nos processos de segurança;
- 9.3.4. Realizar o planejamento e gestão das equipes especializadas, acompanhando os recursos computacionais necessários para o desenvolvimento das atividades do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;
- 9.3.5. Assegurar a observância aos fluxos de trabalho, procedimentos operacionais e diretrizes de comunicação estabelecidos para o Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, garantindo a conformidade da CONTRATADA com as exigências deste Termo de Referência;
- 9.3.6. Manter e executar processos padronizados para elaboração de relatórios e documentos contendo indicadores de desempenho, com foco na melhoria contínua dos serviços prestados;
- 9.3.7. Validar os indicadores mensais de desempenho, eventos tratados e informações registradas no Livro de Registros para cada item de serviço de operação e suporte dentro do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;
- 9.3.8. Realizar anualmente a medição dos indicadores de eventos e monitorar a evolução da infraestrutura instalada em cada item de serviço, com relatórios de tendências e recomendações de melhorias;
- 9.3.9. Acompanhar mensalmente os atendimentos de eventos, solicitações e requisições de mudanças, assegurando a qualidade contínua dos serviços prestados;
- 9.3.10. Manter atualizado o catálogo de serviços e a matriz de responsabilidade dos parceiros envolvidos nos serviços da Nova Rede Corporativa, abrangendo clientes e fornecedores;
- 9.3.11. Receber e gerenciar informações provenientes da ATI, orientando e coordenando as atividades das equipes especializadas, com foco no cumprimento de responsabilidades atribuídas a cada equipe técnica;
- 9.3.12. Apoiar o nivelamento técnico e o acompanhamento de desempenho das equipes, promovendo a capacitação contínua e monitorando a aderência aos padrões exigidos;
- 9.3.13. Acompanhar o desempenho de todos os indicadores de qualidade estabelecidos pela ATI, com atenção especial ao tratamento de falhas, solicitação de serviços e novas instalações, além de elaborar relatórios de conformidade;
- 9.3.14. Apoiar o cumprimento das normas e padrões operacionais definidos para a prestação dos serviços, incluindo a promoção de reuniões periódicas de alinhamento com a ATI para revisão e ajuste das normas conforme necessário;
- 9.3.15. Acompanhar a instalação, configuração e manutenção das plataformas e dos recursos de aplicação necessários para o desempenho eficaz das atividades do Centro Integrado de Inteligência e Segurança Cibernética da

Nova Rede Corporativa;

9.3.16. Disponibilizar suporte técnico recorrente às ferramentas e ao ambiente operacional do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, garantindo o bom funcionamento de todos os sistemas e recursos;

9.3.17. Supervisionar e garantir a execução regular de backups das bases cadastradas nos servidores e aplicações do Centro Integrado de Inteligência e Segurança Cibernética, com revisão periódica para assegurar a integridade dos dados;

9.3.17.1. Fornecer informações técnicas detalhadas sobre as ferramentas de gestão disponíveis para as equipes do Centro Integrado de Inteligência e Segurança Cibernética e ATI, garantindo suporte contínuo às operações estratégicas de segurança e inteligência.

9.4. Serviço de CISO (Chief Information Security Officer)

9.4.1. O objetivo do serviço é fornecer orientação estratégica e operacional em segurança da informação, assegurando a proteção dos ativos digitais, a conformidade com regulamentações e a mitigação de riscos de cibersegurança;

9.4.2. Deverá atuar alinhado ao Serviço de Evolução da Maturidade em Segurança da Informação;

9.4.3. O CISO poderá ser compartilhado com outros clientes da CONTRATADA, prestando ao menos 8h semanais de serviço ao CIISC;

9.4.4. Definir e supervisionar a estrutura de governança de segurança da informação do Centro Integrado de Inteligência e Segurança Cibernética, assegurando que as políticas e procedimentos estejam alinhados com as estratégias de governo;

9.4.5. Participar ativamente de reuniões do conselho ou comitês executivos do Centro Integrado de Inteligência e Segurança Cibernética e da CONTRATANTE técnica para garantir que a segurança cibernética esteja integrada aos objetivos estratégicos;

9.4.6. Avaliar e supervisionar a implementação de novas tecnologias e tendências em segurança da informação, como inteligência artificial e machine learning para análise de ameaças do Centro Integrado de Inteligência e Segurança Cibernética;

9.4.7. Coordenar a colaboração entre o CIISC e a CONTRATANTE para promover uma abordagem holística e integrada de segurança;

9.4.8. Colaborar em investigações relacionadas a fraudes e comportamento malicioso, abordando ameaças externas e internas;

9.4.9. Coordenar a comunicação externa em caso de incidentes de grande escala, incluindo interação com a mídia e stakeholders, para proteger a reputação da CONTRATANTE;

9.4.10. O serviço de CISO incluirá, mas não se limitará, aos seguintes aspectos técnicos:

9.4.10.1. Apoiar na criação de políticas e procedimentos de segurança da informação, alinhados às melhores práticas e às regulamentações vigentes, como LGPD e ISO 27001;

9.4.10.2. Apoiar no desenvolvimento de uma política de resposta a incidentes de segurança, incluindo planos de comunicação e medidas corretivas;

9.4.10.3. Apoiar o desenvolvimento e atualização do plano de continuidade de negócios e recuperação de desastres que aborde possíveis interrupções de sistemas críticos;

9.4.10.4. Coordenar testes regulares de recuperação de desastres, garantindo a resiliência dos sistemas da organização;

9.4.10.5. Monitorar e garantir a conformidade com normas e regulamentações relevantes, como LGPD;

9.4.10.6. Apoiar nas auditorias internas de segurança da informação, preparando relatórios para a alta administração com os resultados e recomendações;

9.4.10.7. Coordenar e gerenciar respostas a incidentes de segurança críticos, documentando as etapas e assegurando o fechamento dos incidentes;

9.4.10.8. Apoiar na elaboração de relatórios periódicos de avaliação de riscos, conformidade e status de segurança da informação;

9.4.10.9. Apoiar na elaboração de indicadores de desempenho, como tempo de resposta a incidentes, redução de vulnerabilidades críticas e adesão às políticas de segurança;

9.4.10.10. Apoiar na elaboração de relatórios de auditoria interna, com recomendações de melhorias e planos de

ação, garantindo que a organização mantenha um nível elevado de maturidade em segurança da informação.

## 10. Núcleo de redes e segurança setorial

10.1. O serviço do núcleo de redes e segurança setorial visa atender os CONTRATANTES aderentes à Nova Rede Corporativa;

10.1.1. O escopo deste serviço inclui a manutenção e suporte exclusivamente dos recursos da Nova Rede Corporativa. Outros recursos, como softwares, equipamentos e infraestrutura de rede que não estejam relacionados aos serviços especificados neste Termo de Referência, serão de responsabilidade do CONTRATANTE aderente;

10.1.2. O serviço do núcleo de redes e segurança setorial da Nova Rede Corporativa abrange:

10.1.2.1. A operação da rede e atividades de segurança, utilizando os recursos tecnológicos fornecidos pela Nova Rede Corporativa;

10.1.2.2. O serviço deverá contar com recursos tecnológicos suficientes para suportar até 200 PCs, conforme os itens contratados no serviço da Nova Rede Corporativa;

10.1.2.3. Caso necessário, o CONTRATANTE poderá contratar um pacote adicional do serviço Núcleo de redes e segurança setorial, com capacidade para até 50 PCs;

10.1.3. Os serviços serão compostos pelos itens contemplados no ADENDO III – SEGURANÇA DE REDE LOCAL e ADENDO VI – SEGURANÇA DE DATACENTER, realizando atividades de monitoramento, acompanhamento e elaboração de relatórios associados aos serviços contratados. Este serviço é limitado aos serviços fornecidos pela Nova Rede Corporativa e aos ativos de interesse do CONTRATANTE aderente;

10.1.4. Um técnico qualificado será alocado nas dependências do CONTRATANTE aderente, de segunda a sexta-feira, no horário das 07:00 às 19:00. Nos demais horários, a critério da CONTRATADA, com cobertura 24/7, incluindo finais de semana e feriados, o serviço poderá ser realizado remotamente, utilizando as instalações do CIISC na ATI, sem ônus para a administração;

10.2. Os recursos mínimos de hardware e software necessários para este serviço são:

10.2.1. Hardware:

10.2.1.1. Sistema de visualização de imagens com tela plana de, no mínimo, 42 polegadas, tecnologia LED ou equivalente, com resolução mínima de 1.920 x 1.080, entrada VGA ou DVI, e suporte para fixação;

10.2.1.2. Estação de trabalho com as licenças necessárias para o sistema de visualização de imagens;

10.2.1.3. Estação de trabalho para cada técnico, conforme a alocação de pessoal nas dependências do CONTRATANTE aderente.

10.2.2. Software:

10.2.2.1. Soluções de software que registrem e ofereçam informações e dados em tempo real, utilizando as mesmas ferramentas do Centro Integrado de Inteligência e Segurança Cibernética, para garantir visibilidade integrada dos dispositivos monitorados;

10.3. O serviço do núcleo de redes e segurança setorial realizará todas as atividades necessárias para a configuração dos recursos envolvidos, incluindo instalações de energia, cabeamento, calhas e racks, garantindo o sigilo e a integridade dos dados e imagens, conforme os padrões da Nova Rede Corporativa;

10.4. Atividades do serviço do núcleo de redes e segurança setorial:

10.4.1. Atuar como extensão do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), agilizando o tratamento de reparos dos serviços contratados;

10.4.2. Servir como interface técnica entre o CONTRATANTE e o CIISC, operando a partir da ATI;

10.4.3. Manter atualizado o catálogo de serviços e a matriz de responsabilidades dos parceiros da Nova Rede Corporativa;

10.4.4. Elaborar relatórios gerenciais de acompanhamento dos serviços contratados;

10.4.5. Monitorar ativos e fornecer suporte proativo ao CONTRATANTE;

10.4.6. Receber e tratar solicitações e registros de ocorrências encaminhados pelo service desk ou outras equipes;

10.4.7. Testar serviços e reparos para garantir pleno funcionamento;

10.4.8. Facilitar a comunicação entre o CONTRATANTE aderente e o CIISC;

10.4.9. Monitorar a infraestrutura e acionar os responsáveis indicados para correções e ajustes;

10.4.10. Atuar proativamente na detecção e reporte de falhas e anomalias que possam indicar atividades suspeitas ou maliciosas;

- 10.4.11. Identificar, registrar e investigar alertas de segurança, incluindo classificação e priorização com base no impacto potencial;
- 10.4.12. Analisar incidentes de segurança para determinar a natureza e a extensão das ameaças;
- 10.4.13. Coletar informações relevantes e escalonar incidentes críticos para o grupo de especialistas;
- 10.4.14. Executar procedimentos de resposta a incidentes e aplicar correções para mitigar o impacto;
- 10.4.15. Gerar relatórios pós-incidentes para análise e melhoria contínua dos processos;
- 10.4.16. Participar de treinamentos para desenvolver habilidades e enfrentar novos desafios;
- 10.4.17. Contribuir na atualização das regras de detecção de eventos de segurança;
- 10.4.18. Responder a solicitações e incidentes reportados diretamente pelo cliente;
- 10.4.19. Emitir relatórios periódicos e personalizados conforme solicitação do cliente.

## 11. Service Desk Especializado

- 11.1. A CONTRATADA deve fornecer atendimento especializado de service desk para todos os usuários da Nova Rede Corporativa, permitindo que eles possam reportar, registrar e encaminhar soluções de maneira integrada com a Nova Rede Corporativa;
- 11.2. O atendimento especializado de service desk deve atender a todos os usuários dos Órgãos CONTRATANTES aderentes da Nova Rede Corporativa, incluindo clientes com serviços de transmissão de dados, voz, segurança e telefonia móvel em regime de 24x7. O serviço de atendimento deve ser gratuito via 0800, com a abertura de chamados técnicos para resolver ou solicitar reparação de serviços contratados, em caso de indisponibilidade;
- 11.3. A CONTRATADA deve prover e manter o ambiente do service desk com todos os recursos tecnológicos e de telecomunicações adequados;
- 11.4. O atendimento deve ser gratuito, por meio de serviço tipo 0800, abrangendo todas as áreas da Nova Rede Corporativa, com um consumo estimado de 120.000 minutos/mês para chamadas extra-rede;
- 11.5. A CONTRATADA deve prover um sistema de informação para o service desk, com base de dados e acessos integrados às equipes do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, permitindo o registro e acompanhamento dos atendimentos e correções realizadas, bem como a geração de relatórios de desempenho e cumprimento dos níveis mínimos de serviço;
- 11.6. Os usuários poderão solicitar atendimento via telefone gratuito (0800), e-mail, WhatsApp, chat ou outros canais digitais centralizados em uma única plataforma multicanal;
- 11.7. A CONTRATADA deve fornecer um serviço de voz para o service desk, com funcionalidades como Unidade de Resposta Audível (URA) e Fila de Espera;
- 11.8. O sistema deve permitir a inclusão de mensagens de aviso sobre falhas de grande impacto, informando os usuários e oferecendo opções de atendimento via URA, evitando a necessidade de abrir chamados manuais;
- 11.9. Todas as ligações atendidas devem ser gravadas por 60 dias para auditorias e monitoramento de qualidade;
- 11.10. A CONTRATADA deve prover a identificação de chamadas, permitindo a identificação do nome do usuário, número da linha e gestor do contrato do CONTRATANTE aderente;
- 11.11. O atendimento deve considerar 5.000 chamados/mês;
- 11.12. A capacidade de atendimento deve considerar o número total de dispositivos na rede;
- 11.13. Um técnico deve ser designado para coordenar o service desk, apoiar a integração das equipes e auditar a qualidade do atendimento;
- 11.14. A CONTRATADA deve supervisionar o atendimento, realizando monitorias mensais para cada operador, visando melhorias no atendimento;
- 11.15. O service desk será a "porta de entrada" técnica para solicitações e registros de falhas nos pontos clientes, fazendo parte do atendimento reativo do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;
- 11.16. A CONTRATADA deve realizar testes preliminares para restabelecer serviços inoperantes e, se necessário, encaminhar demandas para o grupo apropriado;
- 11.17. O service desk deverá realizar abertura de chamados de forma centralizada para os Serviços de Internet Corporativa, Telefonia de Tráfego extrarrede e extrarrede reverso, Conectividade de Datacenter, Telefonia Móvel Pessoal (SMP) e internet móvel, realizando o encaminhamento para a CONTRATADA do serviço em questão;

## 12. Serviço de operação de rede

- 12.1. O serviço de operação de redes deve incluir suporte técnico para cada segmento relacionado à transmissão de dados e voz, conforme descrito abaixo;
- 12.2. Fornecer ferramentas para gerenciamento de falhas, que atendam aos seguintes requisitos e funcionalidades:
- 12.2.1. Configurar a ferramenta de gerenciamento de falhas como um gerenciador geral, permitindo o controle de dispositivos ativos (dados, voz e segurança), integrando informações de outras ferramentas de gerenciamento e consolidando a visualização numa única console;
- 12.2.2. A gerência de falhas deve incluir software, hardware e servidores que monitoram todos os recursos da Nova Rede Corporativa;
- 12.2.3. Monitorar os links dos clientes da rede, com consoles que exibam a situação (status) dos elementos, facilitando a triagem de ocorrências;
- 12.2.4. Detectar, identificar e registrar eventos anômalos na rede;
- 12.2.5. Fornecer informações em tempo real para avaliar se os links de acesso (LA) e serviços estão de acordo com as especificações CONTRATADAS;
- 12.2.6. Apresentar visualizações que indicam o status dos elementos da rede (ativos ou inativos) por meio de cores e ícones, destacando se os parâmetros operacionais estão dentro dos limites estabelecidos;
- 12.2.7. Prover e disponibilizar uma solução integrada de monitoramento de falhas com recursos para visualização de ocorrências e serviços especificados;
- 12.2.8. Exibir um mapa da rede em diferentes níveis, oferecendo visões específicas para análise detalhada dos elementos, com suporte a protocolos como SNMP para gerenciamento de falhas nas redes WANs, serviços de voz e demais dispositivos;
- 12.2.9. Executar scripts automáticos para respostas a eventos específicos;
- 12.2.10. Monitorar variáveis das interfaces locais e remotas dos links de acesso (LA) em operação;
- 12.2.11. Exibir taxas de erro dos canais em tempo real;
- 12.2.12. Realizar isolamento de falhas;
- 12.2.13. Permitir filtragem de alarmes para facilitar a análise;
- 12.2.14. Usar tecnologia SNMP para monitoramento de dispositivos de rede, como roteadores, UTM's e serviços de voz;
- 12.2.15. Fornecer funcionalidades para filtragem configurável de falhas e integração com sistemas de tratamento de ocorrências (trouble tickets);
- 12.2.16. Documentar as características técnicas dos dispositivos da rede para controle de inventário;
- 12.2.17. Oferecer visões de desempenho de dispositivos tanto de maneira geral quanto por portas específicas;
- 12.2.18. Permitir a visualização em tempo real do status da rede em consoles e sistemas de projeção, identificando com cores os estados operacionais e eventos dos ativos, links de acesso (LA) e serviços;
- 12.2.19. Realizar descobrimento automático da topologia da rede (níveis 2 e 3), suportando tecnologias como ATM, Frame Relay, VPN MPLS, e Multicast, além de métodos de consulta, como:
- 12.2.19.1. Tabelas ARP;
- 12.2.19.2. Tabelas de Endereçamento IP;
- 12.2.19.3. Protocolos de descoberta como LLDP (Link Layer Discovery Protocol);
- 12.2.19.4. Tabelas de roteamento;
- 12.2.19.5. Informações de Spanning Tree;
- 12.2.20. Implementar mecanismos de correlação de eventos para geração de alarmes:
- 12.2.20.1. Pares de Eventos: identificar eventos que ocorrem sem seus respectivos pares, gerando alarmes;
- 12.2.20.2. Sequência de Eventos: monitorar sequências específicas que indicam falhas, gerando alarmes quando necessário;
- 12.2.20.3. Combinação de Eventos: permitir a especificação de combinações de eventos que, quando detectadas, geram alarmes;
- 12.2.20.4. Taxa de Eventos: alarmes devem ser gerados quando múltiplos eventos do mesmo tipo ocorrerem em curto intervalo;
- 12.2.20.5. Condicional: gerar alarmes quando condições específicas forem atendidas, com base em uma lista de

eventos e condições;

12.2.20.6. Permitir realizar isolamento de falhas para um dado segmento da topologia, indicando a causa raiz e suprimindo eventos de dispositivos dependentes resultantes da falha principal. A análise de causa raiz por isolamento de falhas deverá ocorrer com base na topologia de nível 2 e 3, sem a necessidade de cadastramento e manutenção de tabelas de relacionamento entre dispositivos pais e filhos. Esta análise deverá ser compatível com recebimento de alertas, devendo suportar, no mínimo, as seguintes tecnologias: WLAN, VLAN, Multicast, MPLS, HFC, SNMP, Syslog, TL1, DWDM, Corba, Docsis, Servers, XML, VPN, Ethernet, Sonet e Aplicações;

12.2.20.7. Permitir fornecer análise do impacto de determinada falha em toda a infraestrutura. Esta análise deverá gerar uma nota de impacto para cada alarme gerado, com base nos dispositivos dependentes de uma causa raiz, considerando os serviços e clientes associados a esta falha e considerando também os sintomas apresentados;

12.2.20.8. Permitir a integração nativa com a ferramenta de gerência de desempenho, possibilitando:

12.2.20.9. O encaminhamento e mapeamento dos alarmes de desempenho para a ferramenta de gerência de falhas;

12.2.20.10. A atualização da situação (status) de um dispositivo na gerência de falhas, baseado na ocorrência de um alarme de desempenho reportado pela gerência de desempenho;

12.2.20.11. Chamada, em contexto de relatórios de desempenho, para os dispositivos de rede, a partir da topologia apresentada pela ferramenta de gerência de falhas;

12.2.20.12. Prover relatórios via web de: planta instalada, disponibilidade e histórico de ocorrências dos ativos de rede que estão sendo gerenciados, de forma a permitir identificar os mais problemáticos e os tipos de eventos mais recorrentes, como também, identificar os dispositivos frequentemente indisponíveis e os mais disponíveis;

12.2.20.13. Permitir a integração com a ferramenta de gerência de infraestrutura da rede, possibilitando monitorar:

12.2.20.13.1. A infraestrutura de rede do ponto cliente especificando os serviços para os seus respectivos clientes, permitindo associar a combinação dos serviços/clientes a um determinado Nível Mínimo de Serviço, de modo que, na ocasião da falha do recurso monitorado, seja indicado tanto o serviço quanto o(s) cliente(s) afetado(s);

12.2.20.13.2. O Nível de Serviço em função de: Disponibilidade, Tempo Médio de Reparo (MTTR), Tempo Médio entre Falhas (MTBF), Tempo Máximo de Parada e Tempo de Resposta;

12.3. Prover ferramentas para gerenciamento de infraestrutura da rede, conforme requisitos e funcionalidades elencadas a seguir:

12.3.1.1. Gerar visualizações que permitam monitorar a saúde dos serviços em tempo real, relacionando os serviços a clientes afetados pelas falhas da infraestrutura;

12.3.1.2. Gerar alarmes associados a “saúde” do serviço, a violação e a degradação de níveis de serviços acordados;

12.3.1.3. Gerar informações que permitam realizar análise de causa raiz de qualquer degradação de serviço, sob a perspectiva de alarmes da infraestrutura;

12.3.1.4. Permitir a facilidade de configurar períodos pré-determinados para a realização de manutenção do serviço, excluindo qualquer possibilidade de solicitação de parada do serviço neste período, evitando impactos nos Níveis Mínimos de Serviços requeridos no ADENDO II, deste Termo de Referência;

12.3.1.5. Gerar informações que permitam realizar análise de tendência do Nível de Serviço para o período corrente, indicando, de forma gráfica, se o Nível de Serviço será ou não cumprido ao fim do período;

12.4. Prover ferramentas para gerenciamento de desempenho, conforme requisitos e funcionalidades elencadas a seguir:

12.4.1.1. Disponibilizar uma ferramenta para gerência de desempenho que seja, obrigatoriamente, do mesmo fabricante da plataforma da ferramenta de gerência de falhas usada para monitorar os serviços de dados, visando garantir a compatibilidade e viabilidade de integração e visualização das informações na console;

12.4.1.2. Disponibilizar um sistema de gerenciamento de falhas para sinalizar todos os eventos de ocorrência de falhas, via rede TCP/IP, priorizando os tipos de falhas, sinalizando os alarmes urgentes;

12.4.1.3. Prover facilidades e recursos técnicos de forma a permitir o gerenciamento da largura de banda na rede, visando garantir os Níveis Mínimos de Serviços requeridos no ADENDO II, deste Termo de Referência, contratados para os PCs, isto é, que a largura de banda entre PCs e destinos significativos, como Pontos de Troca de Tráfego (PTT) ou servidores de referência da internet (localizados no Brasil) seja igual ao valor da banda e velocidade (throughput), da conectividade CONTRATADA.

12.4.1.4. Ter a facilidade de monitorar os seguintes fatores:

- 12.4.1.4.1. A qualidade do serviço de voz sem picotamento, metalização, eco, ruído e retardos abaixo do indicador definido;
- 12.4.1.4.2. Indicadores de largura de banda CONTRATADA, taxa de erro, perda de pacotes e jitter;
- 12.4.1.4.3. Taxas de disponibilidade dos enlaces;
- 12.4.1.4.4. Limiares excedidos.
- 12.4.1.4.5. Apresentar indicativos proativos de pontos críticos na rede;
- 12.4.1.4.6. Apresentar indicativos para análise de otimização dos recursos da rede;
- 12.4.1.4.7. Gerenciar Níveis de Serviços;
- 12.4.1.4.8. Gerar visões específicas das informações para grupos distintos de usuários da organização, tais como: Gestor de Níveis de Serviço, Gestor Operacional da Rede e Gestor Executivo;
- 12.4.1.4.9. Permitir a emissão de relatórios na forma interativa, através de tabelas e gráficos, e de uma navegação Drill-Down gráfica, abrangendo os fatores de gerenciamento da rede previstos neste item;
- 12.4.1.4.10. Gerar quadro das exceções por período, a partir dos limites de utilização (“thresholds”), atribuídos para os recursos/elementos de rede;
- 12.4.1.4.11. Gerar visão dos principais consumidores de recursos, bem como das maiores mudanças nas utilizações de recursos;
- 12.4.1.4.12. Gerar dados para serem utilizados no planejamento de capacidade da rede, demonstrando a utilização histórica dos recursos, projeção no tempo e apontando os recursos super utilizados e os subutilizados;
- 12.4.1.4.13. Gerar projeções estatísticas, apresentando a evolução dos recursos, apontando o número de dias para serem atingidos os limites estabelecidos (“thresholds”);
- 12.4.1.4.14. Permitir a visualização de nível de fluxo de dados de VLANs;
- 12.4.1.4.15. Permitir a visualização de quantidade de colisões de VLANs;
- 12.4.1.4.16. Permitir a segmentação dos mapas de topologia da rede, por áreas geográficas ou por elementos de uma mesma categoria;
- 12.4.1.4.17. Possuir controle de acesso de usuários com as seguintes especificações:
  - 12.4.1.4.17.1. Gerenciar perfis de usuário;
  - 12.4.1.4.17.2. Limitar quais os dispositivos que o usuário pode acessar;
  - 12.4.1.4.17.3. Limitar quais funcionalidades da aplicação que um usuário pode acessar;
  - 12.4.1.4.17.4. Limitar acesso aos relatórios;
  - 12.4.1.4.17.5. Consultar os relatórios já gerados;
  - 12.4.1.4.17.6. Oferecer recursos para manter uma base histórica com o comportamento padrão do desempenho dos componentes da infraestrutura;
- 12.4.1.5. Permitir fazer “capacity planning” com as seguintes especificações:
  - 12.4.1.5.1. Capacidade para antecipar mudanças ou atualizações de equipamentos, infraestrutura e/ou capacidades;
  - 12.4.1.5.2. Indicar, dada uma janela futura de tempo, elementos da infraestrutura que atingirão limiares pré-estabelecidos;
  - 12.4.1.5.3. Alertar com pelo menos 90 dias de antecedência, caso chegue a níveis críticos de uso dos recursos da Nova Rede Corporativa;
  - 12.4.1.5.4. Capacidade de gerar os alertas analisando contra o tempo o nível das variáveis. Ex.: Se a largura da banda de uma conexão ultrapassar 75% da largura da banda durante 15 minutos na última hora, então um alerta deve ser gerado.
- 12.4.1.6. Oferecer recursos e facilidades para indicar em quanto tempo será alcançado o nível das principais variáveis dos dispositivos, dependendo da tecnologia analisada, indicando, por exemplo:
  - 12.4.1.6.1. CPU, line, buffer utilization, discards, errors para roteadores/switches;
  - 12.4.1.6.2. Memória, partições, paginação etc. para servidores.
  - 12.4.1.6.3. Se o problema é largura da banda, erros, discards etc. para lan/wan;
  - 12.4.1.6.4. O volume dos principais elementos do grupo;
  - 12.4.1.6.5. Se o volume ofensor é de entrada ou de saída;
  - 12.4.1.6.6. Máximos e mínimos históricos, médias de linhas de volume de cada dispositivo.
  - 12.4.1.6.7. Indicar mudanças bruscas no volume;
  - 12.4.1.6.8. Gerar relatórios de tendência;

12.4.1.7. Possibilitar customização de relatórios através de uma ferramenta de BI (Business Intelligence), totalmente integrada à base de dados possibilitando a criação de relatórios. A interface de criação e customização de relatórios deverá ser web, sem necessidade de instalação de módulos cliente na máquina do usuário. Os relatórios criados pela solução de BI deverão ser disponibilizados dentro da mesma interface web da solução de gestão de desempenho.

12.4.1.8. A solução de Gerenciamento de Performance deve ser capaz de gerenciar redes SDN (Software-defined Networking) e NFV (Network Functions Virtualization), coletando dados de performance de redes virtualizadas, com no mínimo os seguintes recursos:

12.4.1.8.1. Monitorar e apresentar todas as camadas físicas e virtuais que suportam VNFs (Virtual Network Functions);

12.4.1.8.2. Deve suportar múltiplos fabricantes e plataformas, monitorando controladores SDN, orquestradores, OpenStack;

12.4.1.8.3. Integrar as métricas de monitoramento SDN/NFV com os analíticos e métricas tradicionais SNMP em uma única console;

12.4.1.8.4. Deve suportar no mínimo os seguintes fabricantes: Aruba Central, Broadcom Broadview, Cisco ACI, Cisco DNAC, Cisco Meraki, Fortinet, Nuage, OpenContrail, OpenDaylight, OpenStack, Open vSwitch, Viptela, VMWare NSX-T, VMware vSphere e VMware VeloCloud;

12.4.1.8.5. Monitorar e apresentar o inventário virtual, com informações como: contagem de VNFs por tipo, cadeia de serviços e tendências do inventário;

12.4.1.8.6. Deve apresentar o uso de recursos computacionais e de storage para as VNFs;

12.4.1.8.7. Deve monitorar os recursos físicos alocados para processar os componentes das redes virtualizadas;

12.4.1.8.8. Permitir visualizar a performance de vSwitches. No mínimo cpu, memória, throughput, disponibilidade e informações de interfaces, como utilização, descarte e erros;

12.4.1.8.9. Monitorar a cadeia de serviços, composta pelos blocos que suportam as VNFs, desde o host físico, passando pelo vSwitch, máquina virtual e as comunicações entre VNFs;

12.4.1.8.10. Os coletores de redes virtualizadas devem possuir automonitoramento, apresentando métricas de performance para identificação de problemas, apresentando consumo dos recursos e estatísticas dos serviços, consumo das APIs e ou filas de processamento de mensagens;

12.4.1.8.11. Deve ser capaz de monitorar redes Wi-Fi para tecnologias suportadas, se conectando ao controlador Wi-Fi e apresentando Dashboards de saúde do ambiente, performance dos APs, métricas de rádio, alertas de problemas e outros;

12.4.1.8.12. Deve permitir integração nativa com pontos de monitoramento de observabilidade de redes e experiência do usuário;

12.4.1.8.13. Deve monitorar soluções e dispositivos SD-WAN para tecnologias suportadas, capturando e apresentando a saúde dos túneis SD-WAN e aplicações;

12.4.1.8.14. Deve apresentar os pontos SD-WAN em um mapa geográfico, permitindo identificar rapidamente os túneis SD-WAN, saúde, performance e problemas com poucos cliques;

12.4.1.8.15. Deve possuir tabelas de inventários para dispositivos e interfaces com alertas e cores que ajudam a identificar de forma rápida e precisa componentes com problemas;

12.4.1.8.16. Permitir drill-down para detalhes de dispositivos e interfaces, apresentando quadro de informações detalhadas para cada item;

12.4.1.8.17. Deve ter visões agregadas de saúde de túneis SD-WAN e aplicações para sítios (sites), roteadores edge, caminhos de aplicações, aplicações e túneis;

12.4.1.8.18. Permitir a comparação de métricas lado a lado;

12.4.1.8.19. Possuir métricas de SLA jitter, latência e perda de pacote, permitindo verificar se os túneis estão atingindo os níveis mínimos de performance estabelecidos;

12.4.1.9. Prover ferramentas de monitoramento de performance de aplicações web e redes, integrada nativamente às ferramentas de Gerenciamento de Falhas e Performance de Redes, de forma que essas soluções em conjunto consigam ampliar a visibilidade da rede, integrando a visão tradicional de monitoramento de redes, com a experiência do usuário sob a óptica da rede (Observabilidade da Rede e visibilidade fim a fim), com no mínimo os seguintes recursos:

12.4.1.9.1. Este monitoramento deve permitir endereçar cenários complexos de monitoramento, tais como:

Experiência de usuários em trabalho remoto, uma localidade que está apresentando problemas no uso da rede ou internet, monitoramento de serviços em nuvem (SaaS), monitoramento ou validação de uma instalação SD-WAN e assim por diante;

12.4.1.9.2. Deve ser configurado de forma que facilite:

12.4.1.9.2.1. Determinar a causa dos problemas de rede

12.4.1.9.2.2. Determinar como está a performance da experiência dos usuários de aplicações web

12.4.1.9.2.3. Determinar como a banda de rede está sendo utilizada por aplicação e por usuário

12.4.1.9.2.4. Determinar se os provedores de serviços estão atendendo os níveis de serviços acordados

12.4.1.9.2.5. Apoiar no planejamento quanto a mudanças nos requisitos de capacidade de uso

12.4.1.9.3. Deve prover visibilidade no acesso dos usuários a aplicações que estão publicadas na web ou nuvem e partes da rede que não são controladas pela CONTRATANTE/CONTRATADA.

12.4.1.9.4. Deve fazer uso de análise contínua de caminhos de comunicação (Continuous Path Analysis – CPA) para determinar se há problemas na rede. Essa análise deve ter baixo overhead na rede.

12.4.1.9.5. Caso sejam detectados problemas, através do CPA, deve permitir realizar testes automáticos para identificar o ponto de problema na comunicação.

12.4.1.9.6. Deve prover dados para ajudar a responder a dúvidas comuns durante o diagnóstico de problemas envolvendo acessos via internet:

12.4.1.9.6.1. Onde no caminho de comunicação de redes está ocorrendo o problema;

12.4.1.9.6.2. Se existem rotas específicas que estão apresentando lentidão;

12.4.1.9.6.3. Quantas rotas estão indisponíveis e quando ocorreram as indisponibilidades;

12.4.1.9.6.4. Quanto de capacidade / banda o meu provedor ISP (Internet Service Provider) está fornecendo;

12.4.1.9.6.5. Quanto da capacidade disponível está sendo utilizada;

12.4.1.9.7. Deve permitir visualizar a performance de aplicações do ponto de vista (experiência) do usuário em uma dada localização.

12.4.1.9.8. Deve executar scripts periódicos via browser para simular interações de usuários com uma aplicação e medir quanto tempo a aplicação demora para responder. Deve separar essa coleta em métricas de tempo do browser, da rede e do servidor rodando a aplicação.

12.4.1.9.9. Deve facilitar a visualização de problemas de lentidão, problemas de rede, problemas de browser, conexão, qual parte da aplicação está lenta ou sem resposta, quais localizações estão apresentando lentidão.

12.4.1.9.10. Deve possuir fluxos HTTP que periodicamente simulam transações entre máquinas, permitindo medir o tempo de resposta de aplicações e retorno de respostas esperadas na comunicação.

12.4.1.9.11. Deve permitir ver informações de tráfego e de como a banda em uma localização está sendo usada para determinadas aplicações, hosts e usuários. Deve mostrar quais aplicações estão sendo usadas e quem as está usando, apresentando a quantidade de banda usada por um usuário ou aplicação.

12.4.1.9.12. Deve permitir configurar SNMP para os dispositivos de rede detectados e que a CONTRATANTE ou uma de suas CONTRATADAS disponibilize acesso para consulta, obtendo mais informações sobre o dispositivo;

12.4.1.9.13. Permitir monitorar aplicações em nuvem pública ou privada a partir do desktop do usuário para determinar onde está ocorrendo um problema;

12.4.1.9.14. Deve possuir alertas visuais, identificando por cores status e problemas, por exemplo vermelho para designar um problema e a cor verde para designar que o funcionamento está dentro do esperado, entre outros;

12.4.1.9.15. Permitir detectar mudanças na rede monitorada, tais como: mudanças de rota, mudanças BGP, mudanças no ISP, mudanças de conexão (rede cabeada para wireless);

12.4.1.9.16. Permitir traçar a rota de rede das aplicações monitoradas através da internet de forma visual, mostrando os saltos e detectando onde está o problema, na ponta do usuário, na rede local, nos serviços de link do ISP, no caminho pela internet ou na ponta da aplicação da nuvem. Deve identificar, também de forma visual, as mudanças de rotas que ocorreram no caminho;

12.4.1.9.17. Ao monitorar a experiência do usuário, deve ser capaz de informar como está a qualidade da rede sem fio, velocidade do link, força do sinal, entre outros, para ajudar a determinar se o usuário está tendo problemas por causa de um ponto de acesso ou se o problema é em outro ponto da comunicação fim-a-fim;

12.4.1.9.18. Para prover uma visão completa da experiência do usuário, deve ser capaz de coletar dados de utilização de memória, cpu e processos mais pesados do desktop do usuário, ajudando a identificar se o problema é o desktop

do usuário;

- 12.4.1.9.19. Possuir recursos para criar políticas de monitoramento;
- 12.4.1.9.20. Capacidade para agrupar políticas de monitoramento;
- 12.4.1.9.21. Possuir recursos para criar tags;
- 12.4.1.9.22. Possuir console central para gerenciamento de pontos de monitoramento e ou agentes;
- 12.4.1.9.23. Deve permitir a configuração de timezones;
- 12.4.1.9.24. Deve permitir a configuração de alertas;
- 12.4.1.9.25. Deve permitir configurar notificações via e-mail;
- 12.4.1.9.26. Deve permitir a configuração de grupos;
- 12.4.1.9.27. Deve possuir controles de gerenciamento de usuários e acessos;
- 12.4.1.9.28. Deve prover alertas e notificações por e-mail;
- 12.4.1.9.29. Deve ser capaz de enviar eventos para um gerenciador externo de eventos;
- 12.4.1.9.30. Deve ser capaz de enviar notificações SNMP para um NMS (Network Monitoring System);
- 12.4.1.9.31. Deve possuir ferramentas de diagnóstico para os seguintes casos de uso: Ping, traceroute e nslookup;
- 12.4.1.9.32. Deve permitir realizar diagnóstico de assessment de dados, para verificação da capacidade da rede em lidar com aplicações que possuem altas taxas de transferência de dados.
- 12.4.1.9.33. Deve permitir realizar diagnóstico para verificação da capacidade da rede em lidar com dados de voz;
- 12.4.1.9.34. Permitir realizar de simulação de chamadas de voz;
- 12.4.1.9.35. Permitir realizar testes de simulação de chamadas de vídeo;
- 12.4.1.9.36. Deve permitir verificar se um link está atingindo a capacidade provisionada pelo provedor de internet (ISP);
- 12.4.1.9.37. Deve permitir gerar testes de carga na rede para medir com precisão as capacidades disponíveis de protocolos TCP, UDP e ICMP e analisar o comportamento da rede sob diferentes condições de cargas de tráfego;
- 12.4.1.9.38. Deve possuir monitoramento e testes que ativam a taxa limite da rede (Rate Limiting), enviando pacotes pela rede em rajadas e capturando informações;
- 12.4.1.9.39. Deve possuir um modo de diagnóstico avançado para aumentar a precisão do monitoramento de testes de perda de pacotes principalmente;
- 12.4.1.9.40. Disponibilizar, por padrão, diversos tipos de relatórios e Dashboards, tais como:
  - 12.4.1.9.40.1. Dashboard com o sumário de violações que ocorreram em aplicações Web monitoradas;
  - 12.4.1.9.40.2. Dashboard com o sumário das violações que ocorreram na rede monitorada;
  - 12.4.1.9.40.3. Dashboard com o mapa geográfico com as violações que estão ocorrendo na rede
  - 12.4.1.9.40.4. Dashboard com a visão geral da performance das aplicações monitoradas
  - 12.4.1.9.40.5. Dashboard com a disponibilidade das aplicações Web monitoradas
  - 12.4.1.9.40.6. Dashboard mostrando a qualidade das aplicações Web monitoradas
  - 12.4.1.9.40.7. Relatório de qualidade dos serviços
  - 12.4.1.9.40.8. Overview de performance dos caminhos de rede monitorados
  - 12.4.1.9.40.9. Relatórios de comparativos de performance de dados
  - 12.4.1.9.40.10. Relatórios comparativos de performance de voz
  - 12.4.1.9.40.11. Relatórios de qualidade da banda por localidade
  - 12.4.1.9.40.12. Relatório detalhado de um caminho de rede monitorado
  - 12.4.1.9.40.13. Relatórios de uso e experiência
- 12.4.1.9.41. Deve fornecer painéis de monitoramento de tráfego de uso das aplicações monitoradas com informações como Top Destinos, Top Origens, Top Hosts, Top Categorias, Top QoS e Top Applications;
- 12.4.1.9.42. Deve trazer dados e informações para investigação de diversos tipos de violações que podem ocorrer durante o monitoramento:
  - 12.4.1.9.42.1. RTT
  - 12.4.1.9.42.2. Voz Jitter
  - 12.4.1.9.42.3. Voz Perda (Loss)
  - 12.4.1.9.42.4. Violações de caminhos de rede
  - 12.4.1.9.42.5. Pontuação Apdex ou outra métrica de mercado relevante
  - 12.4.1.9.42.6. Conectividade (caminho de rede monitorado)

- 12.4.1.9.42.7. Erros HTTP
- 12.4.1.9.42.8. Status HTTP
- 12.4.1.9.42.9. Tempo de carregamento de página
- 12.4.1.9.42.10. Erros de Script
- 12.4.1.9.42.11. Tempo de transação
- 12.4.1.9.42.12. Violações de caminhos de rede monitorados
- 12.4.1.9.42.13. Dados Jitter
- 12.4.1.9.42.14. Dados Perda (Loss)
- 12.4.1.9.42.15. Latência
- 12.4.1.9.42.16. MOS
- 12.4.1.9.42.17. Mudanças QoS
- 12.4.1.9.43. Deve ajudar a determinar o escopo e a origem de um alerta de um caminho de rede monitorado;
- 12.4.1.9.44. Deve ajudar a determinar o quanto um problema está afetando a rede;
- 12.4.1.9.45. Deve ajudar a comparar caminhos (rotas) por onde o tráfego passou;
- 12.4.1.9.46. Deve ajudar a determinar se a violação está ocorrendo ou se é um problema histórico;
- 12.4.1.9.47. A solução deve ser fornecida em nuvem (segundo os requisitos mínimos do ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM), no modelo SaaS (Software as a Service);
- 12.4.1.9.48. A solução deve ser distribuída em pelo menos 03 tipos de pontos de monitoramento:
  - 12.4.1.9.48.1. Ponto de monitoramento do tipo container ou máquina virtual, gerenciados pela CONTRATADA e com flexibilidade de serem alocados em localizações que atendam as necessidades do negócio, como por exemplo dois datacenters privados. Este ponto de monitoramento deve ser do tipo software appliance. Cada ponto de monitoramento deve permitir no mínimo 15 testes;
  - 12.4.1.9.48.2. Pontos de monitoramento do serviço SaaS e gerenciados pelo FABRICANTE da solução, instalados em provedores de nuvens em Território Nacional Brasileiro, permitindo o monitoramento a partir de locais onde a CONTRATANTE / CONTRATADA não possuem infraestrutura. Estes pontos de monitoramento devem consumir de acordo com a licença CONTRATADA;
  - 12.4.1.9.48.3. Agentes (ponto) de monitoramento de usuário para monitoramento de experiência. Cada ponto de monitoramento deve permitir no mínimo 5 testes;
- 12.4.1.9.49. Os agentes devem ter métricas de performance, indicando o seu funcionamento e a carga na realização dos testes, como por exemplo o tempo que leva para executar testes;
- 12.4.1.9.50. Possuir recurso de migração de testes de monitoramento entre pontos de monitoramento, preservando histórico e licenciamento;
- 12.4.1.9.51. Deve possuir API para integração com outras soluções;
- 12.4.1.9.52. Deve permitir o envio de eventos para outras soluções;
- 12.4.1.9.53. Deve possuir API para controle dos agentes de monitoramento;
- 12.4.1.9.54. Deve permitir o uso de scripts embedded (embutidos) para gráficos em outras páginas web
- 12.5. Prover ferramentas para gerenciamento de configuração para permitir a operação e monitoramento dos serviços de dados da rede, conforme requisitos e funcionalidades elencadas a seguir:
  - 12.5.1. Permitir capturar periodicamente a configuração de todos os elementos da rede lógica (roteadores, access points, switches, Firewalls, IDS, cache), armazenando-as em um banco de dados com controle de versão;
  - 12.5.2. Oferecer facilidade para comparar cada nova configuração capturada com a armazenada, permitindo a detecção de alterações não autorizadas nos elementos de rede e possibilitando o rollback (reversão) das configurações em caso de mudanças indevidas;
  - 12.5.3. Permitir a descoberta automática (Discovery) dos elementos de rede;
  - 12.5.4. Proporcionar facilidade na criação de scripts para configuração de elementos e ativação de serviços;
  - 12.5.5. Registrar e manter o histórico das mudanças de configuração, com a possibilidade de retorno a uma configuração anterior;
  - 12.5.6. Operar as ferramentas de gerenciamento de configuração para garantir a operação e monitoramento dos serviços de voz fixa na rede, conforme os requisitos e funcionalidades descritos a seguir:
    - 12.5.6.1. Permitir a customização de relatórios por meio de uma ferramenta de Business Intelligence (BI), integrada

ao banco de dados, com interface web, dispensando a instalação de módulos cliente no usuário. Os relatórios gerados devem estar disponíveis na mesma interface da solução de gerenciamento de desempenho, garantindo que a ATI tenha acesso e possa extrair relatórios conforme necessário;

12.5.6.2. Operar uma solução tecnológica que permita a gestão dos serviços de telefonia fixa, garantindo a qualidade e as facilidades oferecidas por esses serviços;

12.5.6.3. Gerir os recursos e facilidades para configurações, atualizações de categorias de ramais (PVFs), operações de backups, e rotinas de armazenamento dos registros de configuração, bilhetagem e tarifação;

12.5.6.4. Operar recursos que permitam a configuração de todos os serviços de voz fixa e correlatos a partir de um ponto central de configuração de roteamento de voz, propagando as configurações para os demais serviços de voz da rede;

12.5.6.5. Garantir que o(s) servidor(es) do sistema de gerência de configuração mantenham cópias de backup das configurações e bases de dados dos serviços de voz da rede, com capacidade de restaurá-las a partir dessas cópias, e garantir que as configurações críticas tenham cópias redundantes em ambientes distintos do local de operação;

12.5.6.6. Realizar backup em locais físicos diferentes no(s) servidor(es) de gerência de configuração, assegurando redundância de hardware e software, com uso compartilhado (load balance) para garantir a continuidade dos serviços em caso de falhas ou intervenções;

12.5.6.7. Operar uma ferramenta de análise de dados em tempo real que emita alertas proativos, distribuídos via e-mail ou exibidos na tela dos usuários, incluindo alertas sobre a capacidade de uso dos troncos.

12.6. Prover ferramentas para gerenciamento de acesso e contabilidade, conforme requisitos e funcionalidades elencadas a seguir:

12.6.1. Fornecer, instalar, manter e operar uma solução tecnológica que possibilite o gerenciamento de acesso e contabilidade dos serviços operados na Nova Rede Corporativa;

12.6.2. Garantir que, após a entrega e validação dos serviços, todo o controle de acesso seja realizado exclusivamente pelo Centro Integrado de Inteligência e Segurança Cibernética;

12.6.3. Facilitar o registro de todos os comandos executados nos equipamentos ativos de dados que integram a Nova Rede Corporativa;

12.6.4. Manter uma base atualizada de operadores autorizados a acessar os equipamentos;

12.6.5. Permitir a criação de grupos de operadores, vinculando-os a conjuntos de comandos permitidos nos equipamentos;

12.6.6. Prover múltiplos níveis de acesso e autorização, diferenciados conforme o perfil do operador;

12.6.7. Restringir aos grupos de suporte externos ao Centro Integrado de Inteligência e Segurança Cibernética o acesso apenas para consulta. No caso de necessidades específicas que envolvam alterações de configuração, permitir que solicitem ao CIISC um acesso temporário para edição;

12.6.8. Autenticar e auditar todos os acessos realizados aos equipamentos ativos de dados da Nova Rede Corporativa.

12.7. Realizar a operação da rede, com equipes técnicas especializadas residentes, além de prever a disponibilização de equipes técnicas de campo para suporte externo e atividades complementares ao Centro Integrado de Inteligência e Segurança Cibernética, conforme necessidade. Essas equipes serão coordenadas pela CONTRATANTE técnica ATI, com o objetivo de atender às demandas de suporte e manutenção de acordo com os incidentes registrados. Os serviços, horários de trabalho e quantitativos estimados para essas equipes estão descritos nos itens e subitens pertinentes deste Termo de Referência;

12.8. Executar a operação de dados e voz, assegurando uma gestão proativa dos recursos da Nova Rede Corporativa. O regime de trabalho será 24x7, das 00:00 às 23:59, de segunda a domingo, incluindo feriados, sob a coordenação do Centro Integrado de Inteligência e Segurança Cibernética;

12.9. Receber e tratar os Registros de Ocorrências (Tickets) encaminhados pelo Service desk ou por outras equipes de gerenciamento de incidentes;

12.10. Garantir que os indicadores de tempo de recuperação e tempo entre falhas sejam mantidos dentro dos padrões exigidos, utilizando os recursos tecnológicos disponibilizados durante a prestação dos serviços da Nova Rede Corporativa. Isso inclui assegurar o cumprimento dos prazos de atendimento e recuperação de sistemas em caso de falhas, conforme os parâmetros estabelecidos no ADENDO II;

12.11. Restabelecer os serviços, incluindo o fornecimento de peças, componentes de hardware e software, e realizar

os serviços necessários para a recuperação definitiva ou provisória dos sistemas do Centro Integrado de Inteligência e Segurança Cibernética, garantindo seu pleno funcionamento;

12.12. Designar técnicos responsáveis para coordenar os serviços de suporte para dados e voz, com a finalidade de controlar, orientar e alinhar tecnicamente os membros de suas respectivas equipes, prestando apoio à coordenação do Centro Integrado de Inteligência e Segurança Cibernética;

12.12.1. Realizar auditorias nos atendimentos, visando manter o nível de qualidade e conformidade com os processos definidos, sob a responsabilidade de cada grupo de trabalho. O técnico designado deve zelar pela qualidade dos atendimentos, do ambiente de trabalho e dos recursos disponibilizados, além de atuar como ponto de comunicação entre as equipes técnicas da CONTRATADA e a ATI;

12.13. Executar a operação dos serviços, atuando remotamente sobre elementos da rede com falhas, corrigindo os problemas detectados pela gerência de falhas ou reportados pelos usuários ao service desk. Quando necessário, acionar as equipes de manutenção de campo para intervenções locais;

12.14. Mensurar o impacto dos recursos afetados, conforme registrado pelo atendimento especializado do service desk, informando sobre falhas que afetam ou não a qualidade dos serviços prestados. Este processo corresponde ao segundo nível de atendimento, encaminhado via service desk;

12.15. Intervir para solucionar falhas, sejam elas em hardware, software, meios de transmissão ou na infraestrutura utilizada. Em caso de falhas simultâneas que impactem um número significativo de pontos clientes, o acompanhamento deverá ser contínuo, com prioridade máxima para resolução do problema;

12.16. Realizar as atividades de suporte à conectividade, isto é, disponibilizar recursos especializados em serviços de voz e de dados para resolver problemas específicos de conectividade, de interoperabilidade entre serviços de telecomunicação para voz, de dados, de ambientes de redes locais e ambientes de grande porte;

12.17. Receber e tratar registros de ocorrências (tickets) encaminhados pelo service desk ou outras equipes de tratamento de ocorrências;

12.18. Testar os serviços e reparos tratados pelas equipes externas ao Centro Integrado de Inteligência e Segurança Cibernética, para garantir o bom funcionamento dos serviços disponibilizados pela rede;

12.19. Efetuar os testes a fim de restabelecer os serviços inoperantes na infraestrutura de serviços fornecidos aos clientes. Caso não obtenham sucesso, encaminhar as demandas para o grupo responsável, de acordo com a natureza do chamado;

12.20. Ser o elemento de ligação com as equipes de atendimento de campo para fins de tratamento e fechamento dos chamados e seus registros históricos, permitindo a rastreabilidade das informações;

12.21. Realizar e zelar pela execução dos backups e recuperação das configurações dos equipamentos de dados e voz responsáveis pelos serviços prestados, através de um procedimento padrão e periódico definido;

12.22. Testar os serviços e reparos tratados pelas equipes externas ao Centro Integrado de Inteligência e Segurança Cibernética para garantir o bom funcionamento dos serviços disponibilizados pela rede;

12.23. Efetuar as atividades de atendimento proativo aos recursos de dados e voz contratados, utilizando-se, para isso, de ferramentas de gerência que permitam o fiel registro das interrupções e quedas de desempenho nos serviços contratados, bem como seus restabelecimentos;

12.24. Disponibilizar, além das ferramentas de gerenciamento, softwares de apoio ao trabalho de operação de voz, contendo, no mínimo, funcionalidades como: acompanhamento de reparos abertos, para rastreamento de situação técnica do reparo, geração de senha criptografada, para confirmação de solução dos casos na hora do fechamento, módulo de conferência de senha, para ser distribuído entre os parceiros na prestação dos serviços, permitir gerar relatórios em formato aberto (xml, txt, csv, etc.), todos em português do Brasil;

12.25. Verificar e validar as configurações executadas por outras equipes, para garantir que estão aderentes ao padrão definido, bem como homologar o funcionamento do serviço junto ao cliente final.

12.26. A CONTRATADA deverá prestar o serviço de ativação e implantação dos novos serviços, abrangendo as atividades de configuração, instalação e implementação, conforme as especificações abaixo:

12.26.1. Executar o serviço de ativação, configuração e instalação dos novos serviços em regime de 08 horas diárias, 05 dias por semana, no horário das 08:00 às 18:00 horas nos dias úteis. Todas as solicitações para atividades deste item serão coordenadas CONTRATANTE técnica ATI;

12.26.2. Realizar as configurações iniciais dos recursos contratados nos equipamentos de dados, voz e segurança, assegurando visibilidade e controle sobre o processo de entrega, conforme os padrões estabelecidos;

- 12.26.3. Designar profissionais qualificados para coordenar as atividades de ativação, configuração e instalação dos novos serviços. Estes profissionais deverão orientar e nivelar tecnicamente o grupo, apoiar a coordenação do Centro Integrado de Inteligência e Segurança Cibernética, e auditar atendimentos para assegurar a conformidade com os processos e padrões de qualidade estabelecidos. A equipe deverá atuar em sinergia com as equipes técnicas da CONTRATADA e da CONTRATANTE técnica ATI;
- 12.26.4. Disponibilizar recursos tecnológicos e ferramentas que permitam à CONTRATANTE técnica ATI o monitoramento em tempo real dos serviços executados, além de possibilitar a recepção de solicitações, análise de precedência e avaliação de riscos das intervenções planejadas;
- 12.26.5. Fragmentar as solicitações de serviços em ações específicas para cada equipe de gestão envolvida, promovendo a organização e o detalhamento da prestação dos serviços;
- 12.26.6. Colaborar com a CONTRATANTE técnica ATI no acompanhamento das Ordens de Serviço relacionadas à ativação e desativação de elementos da rede, bem como ajustes de configuração. Fornecer visibilidade sobre ocorrências e pendências de atendimento;
- 12.26.7. Gerir o encerramento das Ordens de Serviço, mantendo um histórico das demandas, incluindo contagem de casos de sucesso e insucesso, para acompanhamento e melhoria contínua dos serviços;
- 12.26.8. Permitir o controle abrangente dos processos de ativação e desativação de elementos da rede, com suporte a ajustes de configuração;
- 12.26.9. Oferecer ferramentas que permitam avaliar e monitorar o fluxo de atividades do processo de implantação, proporcionando um sistema de workflow adequado para controle e otimização dos serviços;
- 12.26.10. Fornecer mecanismos para o registro e acompanhamento de todas as demandas por meio de Ordens de Serviço, assegurando a rastreabilidade de cada solicitação;
- 12.26.11. Permitir a priorização e escalonamento das atividades, designação de equipes de atendimento especializadas, e monitoramento da execução das tarefas, detectando e tratando eventuais problemas ou gargalos. Estabelecer parâmetros de qualidade para avaliação dos serviços prestados;
- 12.26.12. Disponibilizar um banco de dados para o registro de problemas e soluções encontrados durante o processo de implantação, permitindo a análise estatística e multidimensional das informações para a gestão do conhecimento e aprimoramento dos serviços;
- 12.27. A CONTRATADA deverá prestar o serviço de operação e manutenção do Sistema de Gestão de Ordem de Serviço (SGOS) proprietário do Estado (atualmente denominados: PE Conecta e Integra), incluindo atividades de operação, análise, manutenção e desenvolvimento do sistema, de forma remota, conforme especificado a seguir:
- 12.27.1. Disponibilizar serviço especializado para análise e manutenção do Sistema de Gestão de Ordem de Serviço, incluindo operação, atualização e suporte técnico em regime comercial (08:00 às 18:00, de segunda a sexta-feira), com equipe qualificada em sistemas de informação ou engenharia de software, sob a supervisão da ATI e SAD;
- 12.27.2. Realizar o desenvolvimento e manutenção do Sistema de Gestão de Ordem de Serviço, sob a coordenação conjunta da ATI e SAD. As atividades incluem especificação, codificação, testes de funcionalidades corretivas e evolutivas, além do suporte de primeiro nível para o sistema e sua base de dados, em regime comercial;
- 12.27.3. Operacionalizar o Sistema de Gestão de Ordem de Serviço durante o horário comercial (08:00 às 18:00, de segunda a sexta-feira), coordenado pela ATI/SAD;
- 12.27.4. Designar técnicos responsáveis para coordenar os serviços de operação, desenvolvimento e manutenção do Sistema de Gestão de Ordem de Serviço, auditando atendimentos e mantendo o padrão de qualidade, além de apoiar a integração técnica entre a equipe da CONTRATADA e ATI;
- 12.27.5. O Sistema de Gestão de Ordem de Serviço deverá contemplar os módulos:
- 12.27.5.1. Cadastro dos órgãos aderentes;
- 12.27.5.2. Cadastro dos serviços prestados;
- 12.27.5.3. Contrato principal, termos de adesão e aditivos;
- 12.27.5.4. Ordem de serviços;
- 12.27.5.5. Integração com o service desk;
- 12.27.5.6. Emissão e impressão de relatórios automatizados;
- 12.27.5.7. Informações gerenciais (BI);
- 12.27.5.8. Novas funcionalidades para atender a todas as demandas da Nova Rede Corporativa.
- 12.27.6. Fornecer suporte técnico ao Centro Integrado de Inteligência e Segurança Cibernética, documentando e

controlando versões e códigos-fonte do Sistema de Gestão de Ordem de Serviço;

12.27.7. Realizar o backup e recuperação dos dados do Sistema de Gestão de Ordem de Serviço conforme procedimentos da ATI/SAD;

12.27.8. Apoiar a gestão de contratos de adesão, Ordens de Serviço e trâmites administrativos sob coordenação da ATI/SAD;

12.27.9. Auxiliar na administração das informações divulgáveis pelo Sistema de Gestão de Ordem de Serviço e controle de prazos e cronogramas dos serviços, em coordenação com a ATI/ SAD;

12.27.10. Disponibilizar uma equipe de especialistas para acompanhar e assegurar o cumprimento dos Níveis Mínimos de Serviço, reportando à coordenação do Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa;

12.27.11. Fornecer informações atualizadas sobre serviços contratados, integrando dados do Sistema de Gestão de Ordem de Serviço com as bases requisitadas pela SAD e ATI;

12.27.12. Responsabilizar-se por:

12.27.12.1. Manter a base de dados do Sistema de Gestão de Ordem de Serviço atualizada, conforme diretrizes da ATI e SAD;

12.27.12.2. Fornecer relatórios detalhados sobre demandas e execução de Ordens de Serviço;

12.27.12.3. Disponibilizar equipe especializada para manutenções corretivas e evolutivas que reflitam com precisão os processos de contratação e gestão da rede;

12.27.12.4. Manter atualizados os dados dos órgãos aderentes e serviços contratados, integrando-os ao Sistema de Gestão de Ordem de Serviço;

12.27.12.5. Fornecer, manter e operar uma ferramenta de Business Intelligence (BI), que se conecte ao Banco de Dados do Sistema de Gestão de Ordem de Serviço, acessível apenas pelos usuários autenticados no Sistema de Gestão de Ordem de Serviço, e permita realizar análises diversas com cruzamento de dados, com a criação de tabelas, gráficos e demais recursos comuns em ferramentas deste tipo;

12.27.12.6. A solução de BI deve ser fácil de navegar, com recursos de apontar e clicar ou arrastar e soltar;

12.27.12.7. A solução de BI deve ser fácil de usar, com uma interface intuitiva que permita que até os usuários não técnicos consigam navegar e utilizar as funcionalidades básicas;

12.27.12.8. A solução de BI deve ser capaz de construir um armazém de dados (Data Warehouse) que centraliza dados históricos, para análise avançada;

12.27.12.9. A CONTRATADA deve construir no mínimo 20 (vinte) Dashboards ou relatórios interativos no sistema de BI, especificados pela SAD em conjunto com a ATI;

12.27.12.10. A solução de BI deve permitir que os usuários criem relatórios personalizados, com filtros dinâmicos, agrupamentos e segmentações de dados;

12.27.12.11. A solução de BI deve permitir agendar relatórios e dashboards automáticos para distribuição regular entre os usuários;

12.27.12.12. A solução de BI deve ser capaz de lidar com o crescimento das bases de dados e ser escalável tanto em termos de volume de dados quanto de usuários;

12.27.12.13. A solução de BI deve fornecer dashboards, relatórios e análises em qualquer dispositivo (computador, tablet ou smartphone), com interfaces adaptadas para dispositivos móveis ou aplicativos dedicados para dispositivos móveis;

12.27.12.14. A solução de BI deve permitir compartilhar relatórios e visualizações com outros usuários da ferramenta, bem como exportar tais relatórios e visualizações em formatos padrões (HTML, PDF, XLS, XLSX, Open Document Format);

12.27.12.15. A solução de BI deve ter conformidade com a Lei Geral de Proteção de Dados do Brasil;

12.27.12.16. A CONTRATADA deve fornecer material de orientação de utilização do Sistema de Gestão de Ordem de Serviço e da ferramenta de BI (manuais, tutoriais, cursos online) para a CONTRATANTE, e dar suporte à CONTRATANTE com o fornecimento de materiais e informações para a CONTRATANTE ministrar cursos de utilização das ferramentas;

12.27.12.17. A CONTRATADA deve fornecer e manter um portal na Web com links de acesso a todas as ferramentas disponibilizadas para os contratos da Rede Corporativa de Telemática, concentrando em um só local o acesso a estes recursos disponibilizados pela CONTRATANTE e CONTRATADAS.

12.27.12.18. Este portal na Web deve ser apresentado e validado pela SAD e ATI.

12.27.13. Os detalhes técnicos relativos à arquitetura, topologia, integrações, segurança, modelo de acesso, infraestrutura e demais aspectos operacionais do Sistema de Gestão de Ordem de Serviço (SGOS) encontram-se descritos no **Anexo F - Arquitetura do Sistema Gestão de Ordens - SGOS**, o qual integra este Termo de Referência para fins de subsidiar a adequada compreensão do ambiente e a elaboração das propostas pelas licitantes.

### **13. Serviço de resposta à incidentes de cibersegurança**

13.1. O serviço de resposta a incidentes de cibersegurança será contratado sob demanda, especificamente para incidentes críticos que exijam a intervenção de um time especializado em conjunto com a operação de segurança do Centro Integrado de Inteligência e Segurança Cibernética. A CONTRATANTE técnica ATI será responsável por definir os casos que requerem essa atuação especializada;

13.2. A CONTRATADA deverá seguir o plano de resposta a incidentes cibernéticos desenvolvido no serviço de evolução da maturidade em segurança da informação;

13.3. No plano deverá conter as seguintes etapas:

13.3.1. Preparação:

13.3.1.1. Desenvolvimento e implementação de políticas de segurança e políticas complementares para os clientes aderentes do projeto da Nova Rede Corporativa;

13.3.1.2. Estabelecimento de uma equipe de resposta a incidentes com responsabilidades definidas;

13.3.1.3. Definição de planos de comunicação internos e externos.

13.3.1.4. Planejamento e execução de treinamentos e testes regulares para a equipe.

13.3.2. Detecção e Análise a ser realizado pelo time de analistas de primeiro nível do Centro Integrado de Inteligência e Segurança Cibernética:

13.3.2.1. Monitoramento contínuo e em tempo real do ambiente.

13.3.2.2. Registro e análise de eventos de segurança.

13.3.2.3. Classificação e priorização de incidentes de segurança de acordo com tipo e gravidade.

13.3.3. Contenção

13.3.3.1. Isolamento dos sistemas e ativos envolvidos em incidentes de segurança.

13.3.3.2. Desconexão ou desativação de serviços comprometidos.

13.3.3.3. Implementação de contramedidas temporárias para redução do impacto.

13.3.4. Erradicação

13.3.4.1. Identificação e remoção completa da causa do incidente.

13.3.4.2. Correção de vulnerabilidades que levaram ao incidente.

13.3.5. Recuperação

13.3.5.1. Restauração de todos os ativos e sistemas ao modo normal.

13.3.5.2. Verificação da integridade dos dados e serviços.

13.3.6. Lições Aprendidas

13.3.6.1. Análise completa do incidente para entendimento da origem, impacto e necessidades de atualização de políticas, processos e controles de segurança.

13.3.6.2. Disseminação do conhecimento adquirido dentro do Centro Integrado de Inteligência e Segurança Cibernética.

13.3.6.3. Documentação e arquivamento de todas as ações e informações sobre o incidente para fins de relatório, auditoria e base de conhecimento.

13.3.7. Comunicação

13.3.7.1. Notificação aos stakeholders sobre o incidente.

13.3.7.2. Comunicação com autoridades ou departamento jurídico, se necessário.

13.3.7.3. Manutenção da transparência para garantir a confiança.

13.3.8. Metodologia

13.3.8.1. Aplicação do ciclo PDCA (Plan-Do-Check-Act) para garantir um processo contínuo de melhoria e alinhamento com ameaças emergentes e mudanças na organização.

13.4. Requisitos Técnicos e Funcionais

13.4.1. Consultores devem possuir certificações reconhecidas no mercado de nível intermediário ou avançado em

segurança da informação.

- 13.4.2. Experiência comprovada de no mínimo 3 anos em resposta a incidentes de cibersegurança.
- 13.4.3. Capacidade de conduzir treinamentos e simulações de incidentes.
- 13.4.4. Ferramentas de monitoramento e análise de segurança devem ser de última geração e compatíveis com a infraestrutura da organização.
- 13.5. A CONTRATADA deverá produzir e entregar os seguintes documentos a CONTRATANTE técnica ATI:
  - 13.5.1. Políticas de segurança documentadas.
  - 13.5.2. Relatórios de identificação de ativos críticos e dados sensíveis.
  - 13.5.3. Planos de comunicação internos e externos.
  - 13.5.4. Relatórios de eventos e incidentes de segurança.
  - 13.5.5. Relatórios de análise de lições aprendidas.
  - 13.5.6. Documentação de procedimentos de resposta a incidentes.
- 13.6. O início do processo de resposta a incidente cibernético se dará, sempre que um evento adverso for detectado e descrito no presente Termo de Referência, porém não se limitando a este. Poderá o corpo técnico de segurança do CONTRATANTE também e a qualquer tempo, abrir um incidente de segurança, o qual deve seguir no mínimo o seguinte fluxo e requisitos:
  - 13.6.1. Após o incidente aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos, a fim de no primeiro instante identificar as fontes geradoras de tais logs;
  - 13.6.2. Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE;
  - 13.6.3. Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade/impacto do incidente. A severidade/impacto do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente;
  - 13.6.4. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware);
  - 13.6.5. Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de ITSM, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente;
  - 13.6.6. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente da CONTRATADA, deverá definir uma estratégia para a mitigação e contenção do ataque em questão;
  - 13.6.7. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA através do grupo de resposta a incidente de segurança, inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso;
  - 13.6.8. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense dele, ainda pelo grupo de resposta a incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto um laudo sobre o incidente cibernético em questão;
  - 13.6.9. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar na ferramenta de ITSM, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos;
  - 13.6.10. A CONTRATADA sempre deverá comunicar a área de segurança da ATI as informações sobre os incidentes e quais as ações foram ou estão sendo tomadas para sua solução;

#### **14. Serviço de evolução da maturidade em segurança da informação**

- 14.1. Este serviço visa aprimorar continuamente a maturidade em segurança da informação dos órgãos do Poder Executivo do Estado de Pernambuco, alinhando-se às melhores práticas de mercado e garantindo uma evolução progressiva do sistema de segurança da Nova Rede Corporativa. A implementação se baseia em normas e frameworks internacionais reconhecidos, proporcionando uma estrutura confiável e robusta para avaliação e melhoria contínua;
- 14.2. O serviço utilizará um conjunto de normas e frameworks específicos para elevar a maturidade em segurança da

informação, conforme descrito abaixo:

14.2.1. MITRE ATT&CK: Este framework será utilizado para mapear técnicas e táticas de atacantes cibernéticos, facilitando a compreensão das ameaças e a avaliação da eficácia dos controles de segurança existentes. A implementação do MITRE ATT&CK permitirá identificar lacunas de segurança, planejar estratégias de defesa e alinhar os sistemas de segurança com as ameaças mais comuns e críticas;

14.2.2. NIST Cybersecurity Framework (CSF): Estruturado em cinco funções principais, o NIST CSF fornecerá uma abordagem cíclica para gerenciar a segurança cibernética. Seu uso permitirá uma visão holística da proteção de ativos críticos, oferecendo uma metodologia organizada para avaliar, gerenciar e reduzir riscos;

14.2.3. ISO/IEC 27001:2022: A norma fornecerá uma base estruturada para estabelecer, implementar e monitorar um Sistema de Gestão de Segurança da Informação (SGSI), garantindo conformidade e integridade dos processos de segurança da informação;

14.2.4. CMMI (Capability Maturity Model Integration): Este modelo guiará a evolução progressiva dos processos organizacionais de segurança da informação em níveis de maturidade, promovendo melhorias contínuas e aumento da eficiência.

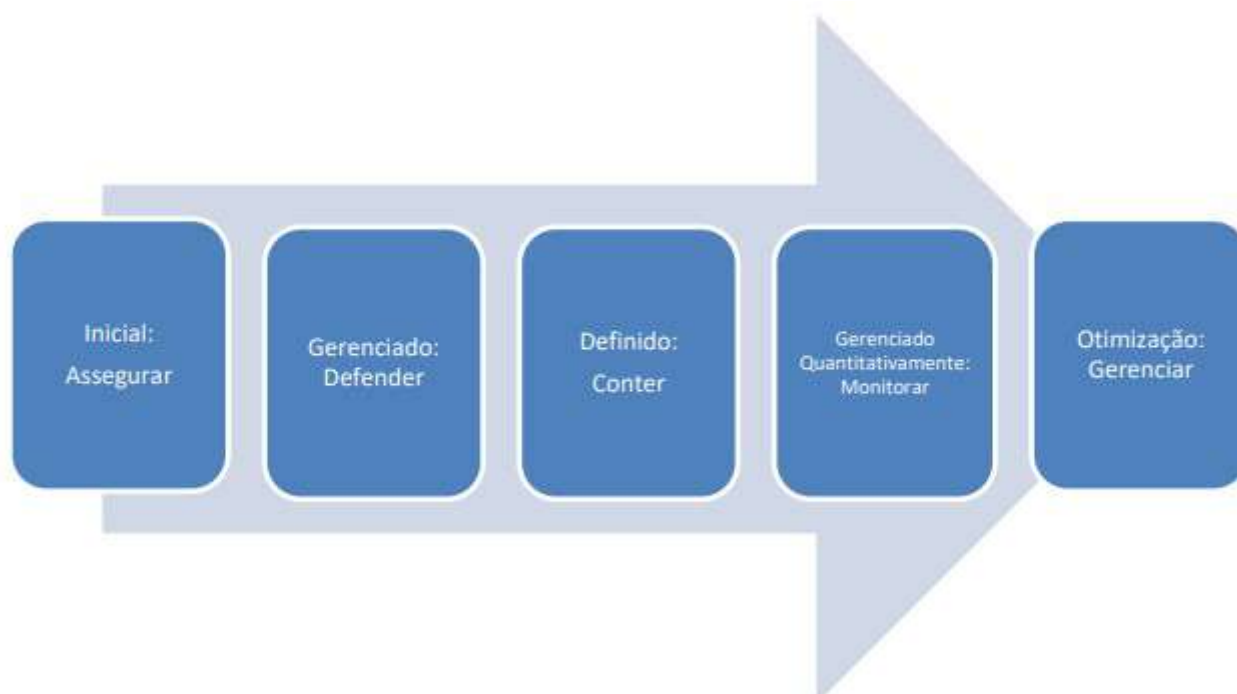
14.3. A CONTRATADA deverá realizar até a entrega do serviço do CIISC:

14.3.1. Realizar uma avaliação e montar o plano de respostas a incidentes cibernéticos;

14.3.2. Realizar uma avaliação da infraestrutura atual e identificação das lacunas de segurança, montar em parceria com a CONTRATANTE técnica ATI o plano de evolução da maturidade em segurança da informação;

14.3.3. Estabelecer as políticas de segurança que o CIISC deverá seguir no monitoramento e gerenciamento da Nova Rede Corporativa.

14.4. Para medir a evolução da maturidade em segurança da informação, será adotada uma escala de maturidade em estágios, contemplando:



14.5. Essa escala de maturidade visa implementar medidas técnicas e organizacionais progressivas no estado, com o objetivo de evoluir continuamente O Serviço de Segurança da Nova Rede Corporativa. Cada etapa será trabalhada ao

longo do contrato, com a implantação das medidas técnicas e organizacionais em períodos determinados, ajustados de acordo com a complexidade de cada fase.

#### 14.6. DESCRIÇÃO DOS NÍVEIS DE MATURIDADE

##### 14.6.1. Nível 01: Início – Foco: Assegurar

14.6.1.1. Este nível de maturidade se concentra em garantir que as políticas, processos e controles de segurança existam e estejam corretamente implementados e funcionais. Envolve a realização de avaliações regulares de segurança, a implementação de medidas proativas para proteger ativos críticos e a certificação de que todos os componentes de segurança estão atualizados e funcionando conforme o esperado. A aplicação de frameworks de segurança, conforme acima delimitado, ajuda a identificar e mitigar vulnerabilidades antes que possam ser exploradas por adversários e devem ser aplicados em consideração ao tripé de processos, pessoas e tecnologias.

14.6.1.2. Nesse contexto, há a necessidade de operações iniciais a serem realizadas visando alcançar esse nível de maturidade consistente em:

14.6.1.2.1. Segmentação de rede: Divisão da rede em segmentos menores para isolar e proteger diferentes áreas, reduzindo o impacto de ataques.

14.6.1.2.2. Proteção de Antivírus/Anti-Malware/Anti-Spam: Implementação de software de segurança para detectar e neutralizar vírus, malwares e spams.

14.6.1.2.3. Inventário Manual: Manutenção de registros manuais de ativos e dispositivos, garantindo que todos os componentes de TI sejam contabilizados e monitorados.

14.6.1.2.4. Backup: Realização de cópias de segurança regulares dos dados críticos para recuperação em caso de perda ou ataque.

14.6.1.3. A implementação de tais atividades devem ser suportadas por meio de instalação de Firewall, de Anti-Malware, Anti-Spam, implementação de Backups, dentre outros recursos.

##### 14.6.2. Nível 02: Gerenciado – Foco: Defender

14.6.2.1. Neste nível a ênfase está na capacidade de identificar e bloquear tentativas de ataque em tempo real. Isso inclui a implementação de sistemas de detecção e prevenção de intrusões (IDS/IPS), a configuração de Firewalls e outras medidas de perímetro, bem como a utilização de técnicas avançadas de análise de comportamento para identificar atividades suspeitas. O uso de táticas e técnicas do MITRE ATT&CK permite que as equipes de segurança antecipem e respondam rapidamente a ameaças emergentes, minimizando o impacto de possíveis incidentes e devem ser aplicados em consideração ao tripé de processos, pessoas e tecnologias.

14.6.2.2. As atividades abaixo podem ser desenvolvidas para obtenção de tal nível de Maturidade:

14.6.2.2.1. Segmentação de perímetro: Implementação de medidas de segurança para proteger a borda da rede, limitando o acesso não autorizado.

14.6.2.2.2. Controle granular de aplicações: Monitoramento e gerenciamento detalhado das aplicações que podem ser executadas nos dispositivos da rede.

14.6.2.2.3. Controle avançado de endpoint (EDR): Utilização de ferramentas para monitorar, detectar e responder a ameaças nos dispositivos finais.

14.6.2.2.4. Controle de Acesso Básico: Definição de políticas básicas de controle de acesso para proteger recursos críticos.

14.6.2.2.5. Gestão de Identidade Básico: Implementação de processos básicos de gestão de identidades para assegurar que apenas usuários autorizados tenham acesso aos sistemas.

14.6.2.2.6. Device Hardening: Fortalecimento da segurança dos dispositivos, desativando serviços desnecessários e aplicando configurações seguras.

14.6.2.2.7. Inventário Automatizado: Uso de ferramentas automatizadas para manter um inventário atualizado de todos os ativos de TI.

14.6.2.2.8. Elaboração do Plano de Continuidade de Negócios e Recuperação de Desastres: A atividade de elaboração de um plano de continuidade de negócios e recuperação de desastres deve ser implementada para garantir a resiliência operacional. Este plano deve incluir procedimentos detalhados para a continuidade das operações críticas do CIISC em caso de incidentes de segurança ou desastres, assegurando que possa rapidamente retomar suas atividades normais. A elaboração do plano deve considerar as ameaças potenciais, recursos necessários para a recuperação e as responsabilidades das equipes envolvidas, promovendo uma resposta estruturada e eficiente em situações adversas. A integração deste plano com as medidas de segurança existentes é fundamental para fortalecer a

defesa e minimizar os impactos de possíveis incidentes.

14.6.2.3. Nessa linha, a implementação de sistemas de duplo fator de autenticação, sistemas de EDR, IPS, App Control, NAC, 2FA, dentre outros recursos, são recomendados, visando o atingimento desse nível.

14.6.3. Nível 03: Definido – Foco: Conter

14.6.3.1. Este nível foca na resposta ativa a incidentes de segurança, com o objetivo de limitar o alcance e o impacto de um ataque. As ações de contenção podem incluir o isolamento de sistemas comprometido, a aplicação de patches de segurança rapidamente, e a utilização de técnicas de segmentação de rede para prevenir a movimentação lateral de adversários. A capacidade de conter uma ameaça efetivamente depende de uma boa preparação e da existência de procedimentos de resposta bem definidos, que podem ser refinados com base nos cenários descritos no MITRE ATT&CK e devem ser aplicados em consideração ao tripé de processos, pessoas e tecnologias.

14.6.3.2. As atividades abaixo devem ser desenvolvidas visando atingir esse nível de maturidade:

14.6.3.2.1. Micro segmentação: Divisão da rede em micro segmentos para isolar ainda mais as cargas de trabalho e limitar a propagação de ameaças.

14.6.3.2.2. Controle avançado de aplicações: Aplicação de políticas rigorosas para a execução de aplicações, evitando a execução de softwares não autorizados.

14.6.3.2.3. Orquestração da proteção de endpoints: Coordenação de várias ferramentas de segurança para proteger dispositivos finais de forma integrada.

14.6.3.2.4. Detonação Remota: Capacidade de analisar arquivos suspeitos em um ambiente seguro e isolado antes de permitir seu acesso à rede.

14.6.3.2.5. Acesso seguro avançado: Implementação de medidas avançadas de controle de acesso, como autenticação multifator e VPNs seguras.

14.6.3.2.6. Secure Web Gateway: Uso de gateways de segurança web para proteger contra ameaças baseadas na internet e controlar o acesso a conteúdo web.

14.6.3.3. Nessa linha, a implementação de recursos com Sandbox, Firewall, IDM, Secure Web Gateway, são recomendados.

14.6.4. Nível 04 – Gerenciado Quantitativo – Foco: Otimização

14.6.4.1. A maturidade em Monitorar envolve a vigilância contínua dos ambientes de TI para detectar anomalias e atividades maliciosas. Isso requer o uso de soluções de monitoramento de segurança, como Security Information and Event Management (SIEM), que agregam e analisam logs de várias fontes para fornecer uma visão holística da postura de segurança da organização. O MITRE ATT&CK fornece um modelo para correlacionar atividades observadas com técnicas conhecidas de ataque, melhorando a capacidade de detecção e resposta e devem ser aplicados em consideração ao tripé de processos, pessoas e tecnologias.

14.6.4.2. As atividades abaixo devem ser desenvolvidas visando atingir esse nível de maturidade:

14.6.4.2.1. Honeypot: Criação de sistemas ou redes fictícias para atrair e detectar atividades maliciosas, desviando ataques de sistemas reais.

14.6.4.2.2. Proteção avançada de endpoints (XDR): Uso de soluções de proteção de endpoint que integram detecção e resposta para fornecer visibilidade e proteção abrangentes.

14.6.4.2.3. Integração com fabricantes: Conexão e integração de ferramentas de segurança com soluções de diferentes fabricantes para uma defesa coordenada.

14.6.4.2.4. Correlação de eventos: Análise e correlação de eventos de segurança para identificar padrões de ataques e responder rapidamente.

14.6.4.2.5. Detecção de Anomalias: Implementação de ferramentas que utilizam machine learning e inteligência artificial para identificar comportamentos anômalos na rede.

14.6.4.3. Nessa linha, a implementação de recursos como XDR, Honeypot, SIEM, CTI, dentre outros auxiliam no atingimento desse nível de maturidade.

14.6.5. Nível 05: Otimizado – Foco: Gerenciar

14.6.5.1. No nível de maturidade gerenciar, as organizações adotam uma abordagem abrangente e estratégica para a segurança cibernética. Isso inclui a gestão proativa de riscos, a integração de segurança em todos os processos de negócios e a promoção de uma cultura de segurança dentro da organização. Envolve também a avaliação contínua e a melhoria dos controles de segurança com base em métricas de desempenho e tendências de ameaças. Utilizando o MITRE ATT&CK, as organizações podem alinhar suas práticas de segurança com padrões reconhecidos, garantindo uma

defesa bem-informada e eficaz contra ciberameaças e devem ser aplicados em consideração ao tripé de processos, pessoas e tecnologias.

14.6.5.2. As atividades abaixo devem ser desenvolvidas visando atingir esse nível de maturidade:

14.6.5.2.1. SOAR: Uso de plataformas de Orquestração, Automação e Resposta de Segurança (SOAR) para automatizar e coordenar a resposta a incidentes;

14.6.5.2.2. Implementação de serviços de monitoramento contínuo e resposta a incidentes com o apoio de especialistas externos.

14.6.5.3. Nessa linha, a implementação de recursos como SOAR e resposta a incidentes, dentre outros auxiliam no atingimento desse nível de maturidade.

14.7. Após a assinatura do contrato do projeto da Nova Rede Corporativa, deverão ser realizadas reuniões regulares de planejamento e consultoria entre a CONTRATADA e a CONTRATANTE técnica ATI;

14.7.1. O objetivo dessas reuniões é desenhar o escopo da evolução da maturidade em segurança da informação que será cobrado mensalmente;

14.7.1.1. Abaixo o escopo inicial sugerido, mas não se limitando a ele:

14.7.1.1.1. Maturidade de segurança:

14.7.1.1.1.1. A CONTRATADA deverá avaliar, através de processos de entrevistas, coleta de evidências e análise de documentos, o nível de conformidade da organização em cada controle do NIST Cyberframework e ISO/IEC 27001;

14.7.1.1.1.2. A CONTRATADA deverá indicar, para cada controle, o nível de maturidade, se inexistente, inicial, conhecida, padronizado, gerenciado ou otimizado;

14.7.1.1.1.3. A CONTRATADA deverá correlacionar esses indicadores com os aspectos globais de um controle como governança, pessoas, processos e tecnologia;

14.7.1.1.1.4. A CONTRATADA deverá incluir no relatório projeções para melhoria do nível de maturidade nos 5 (cinco) anos subsequentes à primeira avaliação, conforme ações de melhoria indicadas e priorizadas pela CONTRATANTE;

14.7.1.1.1.5. A CONTRATADA deverá realizar reavaliações de acompanhamento do nível de maturidade a cada 6 meses;

14.7.1.1.2. Riscos cibernéticos:

14.7.1.1.2.1. A CONTRATADA deverá avaliar a probabilidade das múltiplas e diversas possíveis ameaças cibernéticas de impactarem a organização, com base na análise de cenários mundiais de ameaças, com estatísticas e referências de empresas e instituições renomadas no segmento de cibersegurança;

14.7.1.1.2.2. A CONTRATADA deverá considerar o possível impacto dessas ameaças nas operações, avaliando níveis de incidentes cibernéticos e seus impactos;

14.7.1.1.2.3. A CONTRATADA deverá elaborar um diagnóstico dos riscos cibernéticos considerando agentes ameaçadores, eventos de ameaça, tipo de incidente cibernético, probabilidade de ocorrência e impactos na operação;

14.7.1.1.2.4. A CONTRATADA deverá apresentar uma matriz de riscos e um score de risco, correlacionando-os com o nível de maturidade de segurança;

14.7.1.1.2.5. A CONTRATADA deverá incluir no relatório projeções para melhoria do nível de risco nos 2 anos subsequentes à primeira avaliação, conforme ações de melhoria indicadas e priorizadas pela CONTRATANTE;

14.7.1.1.2.6. A CONTRATADA deverá realizar reavaliações de acompanhamento do nível de risco a cada 6 meses;

14.7.1.1.3. Processos de segurança da informação:

14.7.1.1.3.1. A CONTRATADA deverá realizar uma avaliação dos processos de segurança da informação, associados aos pilares do NIST Cyberframework (Identificar, Proteger, Detectar, Responder, Recuperar, Governar);

14.7.1.1.3.2. A CONTRATADA deverá avaliar esses processos de forma agrupada em macro-processo, processo e descrição;

14.7.1.1.3.3. A CONTRATADA deverá verificar a aplicabilidade do processo à organização, a definição de papéis e responsabilidades, a existência de procedimentos operacionais e a governança por indicadores e resultados;

14.7.1.1.3.4. A CONTRATADA deverá avaliar ao menos 40 processos de segurança;

14.7.1.1.4. Tecnologias de proteção em camadas:

14.7.1.1.4.1. A CONTRATADA deverá avaliar as tecnologias de proteção instaladas no ambiente da CONTRATANTE;

14.7.1.1.4.2. A CONTRATADA deverá constatar um percentual de tecnologias totalmente implementadas, parcialmente implementadas e não implementadas, apresentando esses dados em percentuais;

14.7.1.1.4.3. A CONTRATADA deverá indicar o percentual de maturidade de cada camada de segurança da informação;

- 14.7.1.1.4.4. A CONTRATADA deverá apresentar soluções de proteção inexistentes, bem como propor otimização de custos, desempenho e performance;
- 14.7.1.1.5. Estrutura de segurança da informação:
- 14.7.1.1.5.1. A CONTRATADA deverá avaliar a estrutura do departamento de Segurança da Informação da CONTRATANTE, considerando o quantitativo de pessoas por processos gerenciados;
- 14.7.1.1.5.2. A CONTRATADA deverá apresentar alternativas de estrutura tanto interna quanto terceirizada, caso a estrutura da CONTRATANTE não atenda suficientemente às necessidades dos processos de segurança;
- 14.7.1.1.5.3. A CONTRATADA deverá considerar as especialidades mínimas de gestão de riscos e conformidades de segurança da informação, setores de defesa (Blue Team), setores de ataque (Red Team), desenvolvimento seguro e arquitetura de segurança;
- 14.7.1.1.6. Indicadores de performance (KPIs) de segurança da informação:
- 14.7.1.1.6.1. A CONTRATADA deverá avaliar os indicadores atuais de segurança da informação da CONTRATANTE;
- 14.7.1.1.6.2. A CONTRATADA deverá elaborar uma lista de indicadores de segurança necessários para acompanhar os processos do negócio;
- 14.7.1.1.6.3. A CONTRATADA deverá dividir os indicadores em agrupamentos estratégicos, táticos e operacionais;
- 14.7.1.1.6.4. A CONTRATADA deverá incluir os indicadores de Maturidade e Risco nos indicadores estratégicos e realizar reuniões trimestrais de resultados nas instalações da CONTRATANTE, apresentando se o cenário mudou, permanece o mesmo ou regrediu;
- 14.7.1.1.7. Plano estratégico e tático de segurança da informação:
- 14.7.1.1.7.1. A CONTRATADA deverá elaborar, em conjunto com a CONTRATANTE, um plano estratégico de segurança da informação, contemplando projeções de crescimento da maturidade, redução dos riscos e os investimentos financeiros e de pessoal necessários para atingir as metas do plano;
- 14.7.1.1.7.2. A CONTRATADA deverá elaborar também um Plano Tático de Segurança da Informação, que contemple os grupos de ações a serem executadas, desdobrados em um cronograma detalhado;
- 14.7.1.1.8. Controles NIST considerados:
- 14.7.1.1.8.1. GV.OC-01: A missão organizacional é entendida e informa a gestão de riscos de cibersegurança.
- 14.7.1.1.8.2. GV.OC-02: Stakeholders internos e externos são entendidos, e suas necessidades e expectativas são consideradas.
- 14.7.1.1.8.3. GV.OC-03: Requisitos legais, regulatórios e contratuais são compreendidos e gerenciados.
- 14.7.1.1.8.4. GV.OC-04: Objetivos críticos, capacidades e serviços são compreendidos e comunicados.
- 14.7.1.1.8.5. GV.RM-01: A estratégia de gestão de riscos de cibersegurança é definida, comunicada e gerenciada.
- 14.7.1.1.8.6. GV.RM-02: A estratégia é integrada nos processos de tomada de decisão organizacional.
- 14.7.1.1.8.7. GV.RR-01: Papéis e responsabilidades de cibersegurança são definidos, comunicados e atualizados regularmente.
- 14.7.1.1.8.8. GV.PO-01: Políticas de cibersegurança são estabelecidas, comunicadas e mantidas
- 14.7.1.1.8.9. GV.OV-01: Atividades de supervisão são conduzidas para assegurar a conformidade e a eficácia da estratégia de cibersegurança.
- 14.7.1.1.8.10. GV.SC-01: Riscos de cibersegurança na cadeia de suprimentos são identificados, avaliados e gerenciados.
- 14.7.1.1.8.11. ID.AM-01: Inventários de ativos físicos e virtuais são mantidos.
- 14.7.1.1.8.12. ID.AM-02: Inventários de software e hardware são mantidos.
- 14.7.1.1.8.13. ID.AM-03: Inventários de dados e metadados são mantidos.
- 14.7.1.1.8.14. ID.AM-04: Inventários de serviços fornecidos por fornecedores são mantidos.
- 14.7.1.1.8.15. ID.AM-05: Ativos são priorizados com base na classificação, criticidade e impacto na missão.
- 14.7.1.1.8.16. ID.AM-07: Inventários de dados e metadados para tipos de dados designados são mantidos.
- 14.7.1.1.8.17. ID.AM-08: Sistemas, hardware, software, serviços e dados são gerenciados ao longo de seus ciclos de vida.
- 14.7.1.1.8.18. ID.RA-01: Vulnerabilidades em ativos são identificadas, validadas e registradas.
- 14.7.1.1.8.19. ID.RA-02: Inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações.
- 14.7.1.1.8.20. ID.RA-03: Ameaças internas e externas são identificadas e registradas.
- 14.7.1.1.8.21. ID.RA-04: Impactos e probabilidades de ameaças explorarem vulnerabilidades são identificados e

registrados.

14.7.1.1.8.22. ID.RA-05: Ameaças, vulnerabilidades, probabilidades e impactos são usados para entender o risco inerente e informar a priorização da resposta ao risco.

14.7.1.1.8.23. ID.RA-06: Respostas ao risco são escolhidas, priorizadas, planejadas, rastreadas e comunicadas.

14.7.1.1.8.24. ID.RA-07: Mudanças e exceções são gerenciadas, avaliadas quanto ao impacto de risco, registradas e rastreadas.

14.7.1.1.8.25. ID.RA-08: Processos para receber, analisar e responder a divulgações de vulnerabilidades são estabelecidos.

14.7.1.1.8.26. ID.RA-09: A autenticidade e integridade do hardware e software são avaliadas antes da aquisição e uso.

14.7.1.1.8.27. ID.RA-10: Fornecedores críticos são avaliados antes da aquisição

14.7.1.1.8.28. ID.IM-01: Melhorias são identificadas a partir de avaliações.

14.7.1.1.8.29. ID.IM-02: Melhorias são identificadas a partir de testes e exercícios de segurança.

14.7.1.1.8.30. ID.IM-03: Melhorias são identificadas a partir da execução de processos, procedimentos e atividades operacionais.

14.7.1.1.8.31. ID.IM-04: Planos de resposta a incidentes e outros planos de cibersegurança que afetam operações são estabelecidos, comunicados, mantidos e melhorados.

14.7.1.1.8.32. PR.AA-01: Identidades e credenciais para usuários, serviços e hardware autorizados são gerenciadas.

14.7.1.1.8.33. PR.AA-02: Identidades são verificadas e vinculadas a credenciais com base no contexto das interações.

14.7.1.1.8.34. PR.AA-03: Usuários, serviços e hardware são autenticados.

14.7.1.1.8.35. PR.AA-04: A integridade das asserções de identidade é protegida, transmitida e verificada.

14.7.1.1.8.36. PR.AA-05: Permissões de acesso, direitos e autorizações são definidas em uma política, gerenciadas, aplicadas e revisadas, incorporando os princípios de menor privilégio e separação de funções.

14.7.1.1.8.37. PR.AA-06: O acesso físico aos ativos é gerenciado, monitorado e aplicado conforme o risco.

14.7.1.1.8.38. DE.CM-01: Redes são monitoradas para detectar eventos de cibersegurança.

14.7.1.1.8.39. DE.CM-02: Monitoramento físico é realizado para detectar eventos de cibersegurança.

14.7.1.1.8.40. DE.CM-03: Pessoal é monitorado para detectar eventos de cibersegurança.

14.7.1.1.8.41. DE.CM-04: Ações de usuários com privilégios são monitoradas para anomalias e eventos de cibersegurança.

14.7.1.1.8.42. DE.CM-05: Processos de serviço são monitorados para anomalias e eventos de cibersegurança.

14.7.1.1.8.43. DE.CM-06: Monitoramento externo é conduzido para detectar eventos de cibersegurança.

14.7.1.1.8.44. DE.AE-01: Eventos são analisados para entender a cadeia de eventos de cibersegurança.

14.7.1.1.8.45. DE.AE-02: Causas raiz de incidentes são identificadas.

14.7.1.1.8.46. DE.AE-03: Análise é realizada para determinar o impacto potencial de incidentes.

14.7.1.1.8.47. DE.AE-04: O escopo dos incidentes é determinado e o impacto validado.

14.7.1.1.8.48. DE.AE-05: A integridade dos dados de incidentes é garantida.

14.7.1.1.8.49. DE.AE-06: Indicadores de compromisso são identificados e validados.

14.7.1.1.8.50. DE.AE-07: Lições aprendidas de eventos e incidentes são documentadas e comunicadas.

14.7.1.1.8.51. DE.AE-08: Incidentes são declarados quando eventos adversos atendem aos critérios definidos.

14.7.1.1.8.52. RS.MA-01: O plano de resposta a incidentes é executado em coordenação com terceiros relevantes.

14.7.1.1.8.53. RS.MA-02: Relatórios de incidentes são triados e validados.

14.7.1.1.8.54. RS.MA-03: Incidentes são categorizados e priorizados.

14.7.1.1.8.55. RS.MA-04: Incidentes são escalados ou elevados conforme necessário.

14.7.1.1.8.56. RS.MA-05: Critérios para iniciar a recuperação de incidentes são aplicados.

14.7.1.1.8.57. RS.AN-03: Análise é realizada para estabelecer o que ocorreu durante um incidente e a causa raiz.

14.7.1.1.8.58. RS.AN-06: Ações realizadas durante uma investigação são registradas, e a integridade e procedência dos registros são preservadas.

14.7.1.1.8.59. RS.AN-07: Dados e metadados de incidentes são coletados, e sua integridade e procedência são preservadas.

14.7.1.1.8.60. RS.AN-08: A magnitude de um incidente é estimada e validada.

14.7.1.1.8.61. Relatório e Comunicação de Resposta a Incidentes (RS.CO):

14.7.1.1.8.62. RS.CO-02: Stakeholders internos e externos são notificados de incidentes.

- 14.7.1.1.8.63. RS.CO-03: Informações são compartilhadas com stakeholders internos e externos designados.
- 14.7.1.1.8.64. RS.MI-01: Incidentes são contidos.
- 14.7.1.1.8.65. RS.MI-02: Incidentes são erradicados.
- 14.7.1.1.8.66. RC.RP-01: A parte de recuperação do plano de resposta a incidentes é executada após ser iniciada pelo processo de resposta a incidentes.
- 14.7.1.1.8.67. RC.RP-02: Ações de recuperação são selecionadas, delimitadas, priorizadas e realizadas.
- 14.7.1.1.8.68. RC.RP-03: A integridade de backups e outros ativos de restauração é verificada antes de usá-los para a restauração.
- 14.7.1.1.8.69. RC.RP-04: Funções críticas de missão e gestão de risco de cibersegurança são consideradas para estabelecer normas operacionais pós-incidente.
- 14.7.1.1.8.70. RC.RP-05: A integridade dos ativos restaurados é verificada, sistemas e serviços são restaurados, e o status normal de operação é confirmado.
- 14.7.1.1.8.71. RC.RP-06: O fim da recuperação do incidente é declarado com base em critérios, e a documentação relacionada ao incidente é completada.
- 14.7.1.1.8.72. RC.CO-03: Atividades de recuperação e progresso na restauração de capacidades operacionais são comunicadas aos stakeholders internos e externos designados.
- 14.7.1.1.8.73. RC.CO-04: Atualizações públicas sobre a recuperação do incidente são compartilhadas usando métodos e mensagens aprovados.
- 14.7.1.1.9. Controles ISO/IEC 27001:2022
- 14.7.1.1.9.1. Políticas de segurança da informação
- 14.7.1.1.9.2. Organização da segurança da informação
- 14.7.1.1.9.3. Papéis e responsabilidades
- 14.7.1.1.9.4. Contato com autoridades
- 14.7.1.1.9.5. Segurança na gestão de projetos
- 14.7.1.1.9.6. Inventário de ativos
- 14.7.1.1.9.7. Uso aceitável de ativos
- 14.7.1.1.9.8. Gestão de riscos de segurança da informação
- 14.7.1.1.9.9. Conformidade com requisitos legais e contratuais
- 14.7.1.1.9.10. Auditoria interna de segurança da informação
- 14.7.1.1.9.11. Gestão de mudanças
- 14.7.1.1.9.12. Termos e condições de emprego
- 14.7.1.1.9.13. Treinamento e conscientização em segurança da informação
- 14.7.1.1.9.14. Disciplinas de segurança
- 14.7.1.1.9.15. Processo de saída
- 14.7.1.1.9.16. Segurança em áreas físicas
- 14.7.1.1.9.17. Controles de acesso físico
- 14.7.1.1.9.18. Proteção contra ameaças externas e ambientais
- 14.7.1.1.9.19. Localização e proteção de equipamentos
- 14.7.1.1.9.20. Gestão de acesso
- 14.7.1.1.9.21. Criptografia
- 14.7.1.1.9.22. Segurança nas comunicações
- 14.7.1.1.9.23. Segurança nos sistemas de informação
- 14.7.1.1.9.24. Aquisição, desenvolvimento e manutenção de sistemas de informação
- 14.7.1.1.9.25. Segurança de operações
- 14.7.1.1.9.26. Monitoramento e análise de logs
- 14.7.2. As reuniões deverão garantir que ambas as partes estejam alinhadas quanto aos objetivos, metas e métodos de avaliação dos serviços prestados;
- 14.7.3. O cronograma de evolução da maturidade deverá ser definido em comum acordo entre a CONTRATANTE técnica ATI e a CONTRATADA após a assinatura do contrato;
- 14.7.4. O cronograma acordado será utilizado como base para a avaliação mensal e subsequente pagamento dos serviços;

14.8. A CONTRATADA deverá apresentar relatórios mensais detalhados, que incluam todas as atividades realizadas, os resultados obtidos e a comprovação do cumprimento dos indicadores de desempenho (KPIs) e parâmetros estabelecidos;

14.9. A avaliação dos relatórios será conduzida pela CONTRATANTE técnica ATI para verificar a conformidade com o cronograma e os objetivos de evolução da maturidade;

14.10. A CONTRATANTE técnica ATI apenas realizará o pagamento do item de serviço Evolução da maturidade em segurança da informação, se a CONTRATADA comprovar o cumprimento da evolução da maturidade em segurança da informação, conforme for estabelecido no cronograma;

14.10.1. O pagamento pelos serviços será condicionado à validação dos resultados apresentados pela CONTRATADA;

14.10.2. Caso sejam identificadas não conformidades ou falhas no cumprimento dos objetivos acordados, o pagamento poderá ser retido parcial ou totalmente até que as questões sejam resolvidas e os objetivos atingidos.

## 15. Qualificação técnica

15.1. Os níveis mínimos de conhecimento a serem requeridos à CONTRATADA para comprovar a existência de pessoal qualificado estão listados nos termos do presente tópico;

15.2. Dada a complexidade do ambiente da CONTRATANTE e dos serviços prestados, e em conformidade com a Portaria SGD/MGI nº 6.680/2024, os profissionais alocados no Serviço de análise de segurança especializada deverão possuir nível Sênior;

15.2.1. A experiência descrita no Anexo I, item 2.2, alínea:

ad) Profissional Sênior: adequado para exercer atividades com grau elevado de complexidade e criticidade, e que requer experiência e qualificação.

15.3. A CONTRATADA deve manter todo o corpo técnico do time do Serviço de análise de segurança especializada, líderes, coordenadores e gerentes de projetos com as certificações listadas de acordo com a sua respectiva especialidade;

15.3.1. Em caso de substituição de um membro do corpo técnico, o novo profissional deverá possuir qualificação técnica compatível com os requisitos estabelecidos na qualificação técnica;

15.3.2. A CONTRATANTE deverá ser formalmente informada sobre qualquer alteração na composição do corpo técnico do CIISC.

15.4. Todas as certificações deverão estar válidas e ativas durante o período do contrato;

15.5. Certificações equivalentes reconhecidas internacionalmente poderão ser aceitas mediante análise e validação pela CONTRATANTE.

15.6. Analistas de primeiro nível e analistas do núcleo de redes e segurança setorial:

15.6.1. A CONTRATADA deve manter 50% do corpo técnico do time com as certificações listadas abaixo:

15.6.1.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;

15.6.1.2. Certificações dos fabricantes que compõem a rede de nível intermediário ou superiores relativo à administração de firewalls;

15.7. Especialista em segurança de endpoint:

15.7.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;

15.7.2. Certificação avançada em solução de EPP/EDR/XDR do fabricante do equipamento a ser ofertado na proposta;

15.8. Especialista em segurança de rede sem fio:

15.8.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;

15.8.2. Certificação avançada em Solução de Rede Sem Fio do fabricante do equipamento a ser ofertado na proposta;

15.9. Especialista em firewall:

15.9.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;

15.9.2. Certificação avançada em solução de Firewall do fabricante do equipamento a ser ofertado na proposta;

15.10. Especialista em SIEM:

15.10.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;

15.10.2. Certificação avançada em solução de SIEM do fornecedor indicado na proposta;

- 15.10.3. Certificação avançada em relatoria do fabricante indicado na proposta;
- 15.11. Especialista em conformidade:
- 15.11.1. Certificação Profissional em Privacidade e Proteção de Dados;
- 15.11.2. Certificação em Auditor Interno e/ou Auditor Líder;
- 15.11.3. Certificação Profissional em ISO/IEC 27001 Profissional;
- 15.12. Consultor de redes sem fio:
- 15.12.1. Certificação CWSP (Certified Wireless Security Professional);
- 15.13. Analista de qualidade e especialistas de atenção:
- 15.13.1. Certificação ITIL v4 Foundation ou superior;
- 15.13.2. Certificação CBPA (Certified Business Process Associate) e/ou OMG BPM 2 Fundamental ou superior;
- 15.14. Gerente de projetos:
- 15.14.1. Certificação PMP - Project Management Professional;
- 15.14.2. Certificação ITIL v4 Foundation ou superior;
- 15.14.3. Certificações em Metodologia Ágil (PSM, PSPO, CSM, CSPO ou PMI-ACP);
- 15.15. Líderes:
- 15.15.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;
- 15.15.2. Certificação ITIL v4 Foundation ou superior;
- 15.15.3. Certificações dos fabricantes que compõem a rede de nível intermediário ou superiores relativo à administração de firewalls;
- 15.16. Coordenação:
- 15.16.1. Certificações de segurança como CompTIA Security+ e/ou ISFS based on ISO/IEC 27001;
- 15.16.2. Certificação ITIL v4 Foundation ou superior;
- 15.16.3. Certificações dos fabricantes que compõem a rede de nível intermediário ou superiores relativo à administração de firewalls;
- 15.16.4. Certificações ISMP (Information Security Management Professional) ou equivalente;
- 15.17. CISO:
- 15.17.1. Certificação CISSP, CISM, CISA ou equivalentes;
- 15.18. Validação das Certificações Profissionais
- 15.18.1. A CONTRATADA deverá apresentar, obrigatoriamente, no momento da entrega do serviço CIISC – Centro Integrado de Inteligência e Segurança Cibernética da Nova Rede Corporativa, prazo máximo de 90 (noventa) dias corridos a partir da emissão da ordem de serviço, a documentação comprobatória de todas as certificações exigidas nos subitens do item 15 deste Adendo, conforme o perfil profissional e a função técnica correspondente.
- 15.18.2. A aceitação e homologação formal do serviço CIISC estará condicionada à validação, pela CONTRATANTE, da documentação apresentada, que deverá comprovar que os profissionais alocados atendem integralmente aos requisitos de qualificação técnica exigidos, com certificações válidas, ativas e compatíveis com as atribuições desempenhadas, conforme estabelecido neste Adendo.
- 15.18.3. O não cumprimento do prazo ou a apresentação de documentação em desconformidade implicará a não validação do serviço, bloqueio do pagamento do item, e a continuidade da contagem do prazo contratual. A situação ensejará na abertura de processo administrativo para apuração de responsabilidade e eventual aplicação das sanções previstas no Termo de Referência e na legislação vigente.
- 15.18.4. As certificações deverão estar individualmente vinculadas aos profissionais indicados pela CONTRATADA e poderão ser, a qualquer tempo, auditadas ou verificadas tecnicamente pela CONTRATANTE, durante toda a vigência contratual.
- 15.18.5. Em caso de substituição de qualquer profissional certificado após a homologação, a CONTRATADA deverá informar formalmente à CONTRATANTE e apresentar, no prazo máximo de 15 (quinze) dias corridos, a documentação comprobatória de certificações equivalentes do novo profissional, sob pena de aplicação das penalidades cabíveis.

#### ADENDO X - AVALIAÇÃO E MITIGAÇÃO DE RISCOS CIBERNÉTICOS

## 1. Requisitos gerais

1.1. Os integrantes da(s) equipe(s) alocadas para prestação do serviço de Avaliação e Mitigação de Riscos Cibernéticos serão disponibilizados de forma remota;

1.1.1. O serviço será composto por:

1.1.1.1. Serviço de gestão de vulnerabilidades;

1.1.1.2. Serviço de testes de intrusão (Pentest);

1.1.1.3. Serviço de analistas de segurança ofensiva (Red Team);

1.1.1.4. Serviço de análise forense.

1.2. A CONTRATADA deverá prover soluções de hardware e software que permitam suportar todas as atividades especificadas no serviço de Avaliação e Mitigação de Riscos Cibernéticos;

1.3. Todos os softwares utilizados pela equipe da CONTRATADA deverão ser licenciados, durante todo o período do contrato, evitando violação dos direitos autorais e vulnerabilidade na segurança com softwares não legalizados;

## 2. Serviço de gestão de vulnerabilidades

2.1. A CONTRATADA deve realizar varreduras automatizadas para identificar vulnerabilidades, utilizando ferramentas aprovadas pela CONTRATANTE técnica ATI. A frequência das varreduras e a seleção dos ativos a serem examinados serão definidos pela CONTRATANTE;

2.2. A CONTRATADA deve eliminar os falsos positivos e as vulnerabilidades não aplicáveis ao ambiente da CONTRATANTE para a geração dos relatórios e das recomendações;

2.3. A CONTRATADA deverá tomar as providências necessárias para evitar que as análises causem indisponibilidades ou alterações no ambiente da CONTRATANTE;

2.4. A CONTRATADA deve realizar uma análise detalhada dos relatórios gerados pelas ferramentas de varredura para identificar as vulnerabilidades encontradas, classificando-as segundo sua gravidade (crítica, alta, média e baixa) e seu potencial impacto para a segurança dos ativos;

2.5. A CONTRATADA deve auxiliar a CONTRATANTE na identificação e priorização dos ativos críticos, determinando o impacto potencial de vulnerabilidades em função da criticidade desses ativos para o órgão;

2.6. A CONTRATANTE será responsável por designar um "Dono do Ativo" para cada ativo crítico identificado, o qual deverá atuar como ponto de apoio na definição das prioridades e nas aprovações necessárias para o desenvolvimento e execução do plano de ação, assim como no acompanhamento da implementação das medidas corretivas. O Dono do Ativo deve participar das revisões periódicas e das discussões relacionadas aos ajustes de políticas, assegurando a efetiva integração das soluções com os processos do órgão;

2.7. A CONTRATADA, em conjunto com a CONTRATANTE, deve elaborar um plano de ação detalhado para tratamento das vulnerabilidades identificadas, contemplando medidas corretivas e preventivas, a designação dos responsáveis, os prazos e o plano de acompanhamento das atividades a serem realizadas;

2.8. A CONTRATADA deve auxiliar a CONTRATANTE a executar as ações corretivas e preventivas aprovadas no plano de ação, tais como aplicação de patches, atualização de softwares, reconfiguração de sistemas e outras medidas necessárias, sempre em consonância com as diretrizes da CONTRATANTE;

2.9. Após a implementação das medidas, a CONTRATADA deve conduzir testes de eficácia em conjunto com a CONTRATANTE para verificar se as vulnerabilidades foram efetivamente corrigidas ou mitigadas, garantindo que as soluções aplicadas não introduzam novas falhas no ambiente;

2.10. A CONTRATADA deve realizar o monitoramento contínuo do ambiente com o objetivo de identificar novas vulnerabilidades. A equipe designada deve utilizar ferramentas de varredura e monitoramento em tempo real e deve se manter atualizada quanto a novas ameaças e tendências de segurança, compartilhando os achados com a CONTRATANTE;

2.11. A CONTRATADA deve conduzir revisões periódicas dos processos de gestão de vulnerabilidades, avaliando a eficácia das ações adotadas e identificando oportunidades de melhoria. Relatórios de revisão devem ser elaborados e apresentados à CONTRATANTE técnica ATI, com recomendações para ajustes no plano de ação;

2.12. A CONTRATADA deve colaborar com a CONTRATANTE na revisão e atualização das políticas e procedimentos de segurança, considerando as lições aprendidas e novas ameaças identificadas. A CONTRATADA deve assegurar que as práticas adotadas estejam em conformidade com as melhores práticas e normas do setor, propondo ajustes que promovam uma gestão de vulnerabilidades mais eficiente e robusta;

2.13. Funcionalidades mínimas da solução de varredura de vulnerabilidades, de responsabilidade da CONTRATADA:

2.13.1. A solução deve ser disponibilizada em nuvem, ou no ambiente físico da CONTRATADA;

2.13.2. A Detecção e Resposta de Gestão de Vulnerabilidades (VMDR) deve permitir que o analista descubra, avalie, priorize e identifique correções para vulnerabilidades críticas e configurações incorretas em tempo real ambientes de TI híbridos em uma única solução;

2.13.3. A solução deve ser integrada e abrangente para gerenciamento de vulnerabilidades, desde a descoberta de ativos até a priorização e remediação de vulnerabilidades, fornecendo visibilidade em tempo real e fluxos de trabalho de patching eficientes, ajudando a melhorar os tempos de resposta;

2.13.4. A solução deve conter avaliação de vulnerabilidades e configurações, risco de ameaças e tecnologia de priorização de vulnerabilidades integrada com fluxos de trabalho de gerenciamento de patches, visando reduzir o Tempo Médio para Remediar (MTTR) de vulnerabilidades;

2.13.5. A solução deve atender necessidades de escaneamento interno e externo;

2.13.6. A solução deve garantir o registro preciso dos dispositivos do ambiente;

2.13.7. Realizar avaliações contínuas de vulnerabilidades com agentes e uma variedade de sensores, utilizando inteligência artificial para avaliar e priorizar ameaças instantaneamente com base em contexto e relevância;

2.13.8. Inventário de ativos em ambientes com Certificados, Nuvem, Contêineres e Dispositivos Móveis;

2.13.9. Deve possuir diversos tipos de sensores: Sensores Virtuais, Sensores Passivos, Agentes na Nuvem, Agentes Móveis, Sensores de Contêiner;

2.13.10. Deve permitir pesquisar qualquer ativo em segundos usando mais de 200 atributos pesquisáveis;

2.13.11. A solução deve possuir Dashboards e Widgets personalizáveis;

2.13.12. Deve apresentar informação de tendências e avaliação de configuração de segurança com base em benchmarks CIS (Center for Internet Security);

2.13.13. A solução deve fazer a priorização baseada em indicadores de ameaça em tempo real continuamente atualizados;

2.13.14. Deve alertar em tempo real por e-mail as vulnerabilidades críticas e alterações no seu perímetro externo;

2.13.15. A solução deve detectar patches ausentes em contexto com as vulnerabilidades detectadas;

2.13.16. Deve permitir a implantação de patches diretamente do relatório de priorização de vulnerabilidades e patches (Windows e Linux) nos ativos que possuem a Solução de proteção, detecção e resposta para servidores – EDR do ADENDO VI - SEGURANÇA DE DATACENTER;

2.13.17. Descobrir em Tempo Real as Informações de Vulnerabilidades;

2.13.18. Priorizar ou listar vulnerabilidades com base na inteligência de ameaças;

2.13.19. Detecção e implantação de patches corretivos na interface da solução e de forma simplificada;

2.13.20. Deve permitir realizar a Gestão e Organização de Ativos atribuindo tags para categorizar e organizar os ativos;

2.13.21. Identificação de ativos por diversos métodos como Scanners, Sensores Passivos, Inventário de Nuvem, Inventário de Contêiner e Inventário de Dispositivos Móveis;

2.13.22. Visualização da postura de dispositivo do ponto de vista de vulnerabilidade;

2.13.23. Relatório de priorização para priorizar as vulnerabilidades mais arriscadas dos ativos mais críticos;

2.13.24. Deve possuir visão detalhada do dispositivo com no mínimo informações de criticidade baseada em score, tipos de escaneamentos usados e tags;

2.13.25. Na visão detalhada deve trazer também os principais fatores de risco das vulnerabilidades detectadas no ativo conforme CISA Known Exploitable, Associated Threat Actors, Associated Malware, e Weaponized Vulnerability;

2.13.26. Deve pontuar os riscos utilizando método próprio de classificação;

2.13.27. Deve possuir visão detalhada das vulnerabilidades como no mínimo informações de severidade, CVE que tem maior contribuição, os malwares e atores associados, o quão explorável é a vulnerabilidade, informações adicionais acerca da vulnerabilidade e formas de remediação disponíveis;

2.13.28. Deve possuir relatórios e Dashboards;

2.13.29. Os Dashboards devem permitir visualizar ativos, exposição a ameaças, aproveitar pesquisas salvas e rapidamente entender a prioridade de vulnerabilidades;

2.13.30. Deve possuir relatório de priorização com foco nos recursos e as vulnerabilidades de maior risco;

2.13.31. Permitir os analistas de segurança escolherem os indicadores de ameaça mais relevantes;

- 2.13.32. Ajudar a identificar o patch específico que corrige uma vulnerabilidade;
- 2.13.33. Reduzir o tempo de remediação ao detectar o patch a ser implantado com fluxo de trabalho integrado com a gestão de patches. Esse recurso deve estar disponível dentro da solução;
- 2.13.34. Deve possuir integração com o Framework MITRE ATT&CK®;
- 2.13.35. Deve exibir visão detalhada de Táticas, Técnicas e Sub-Técnicas;
- 2.13.36. Deve facilitar a visibilidade sobre patches disponíveis para os ativos monitorados;
- 2.13.37. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
- 2.13.38. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
- 2.13.39. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
- 2.13.40. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
- 2.13.41. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
- 2.13.42. A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação:
  - 2.13.42.1. Contas administrativas vulneráveis a Kerberoasting attack;
  - 2.13.42.2. Utilização de criptografia vulnerável com autenticação Kerberos;
  - 2.13.42.3. Contas com pré-autenticação do Kerberos desabilitada;
  - 2.13.42.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
  - 2.13.42.5. Verificar validação de fragilidades do tipo "Unconstrained Delegation";
  - 2.13.42.6. Verificação de "Pre-Windows 2000 Compatible Access";
  - 2.13.42.7. Verificação de validade de chaves mestras "Kerberos KRBTGT";
  - 2.13.42.8. Verificação de "SID History Injection";
  - 2.13.42.9. Verificação de "Printer Bug Exploit";
  - 2.13.42.10. Verificação de "Primary Group ID";
  - 2.13.42.11. Verificação de usuários com Passwords em branco;
- 2.13.43. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 2.13.44. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 2.13.45. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 2.13.46. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 2.13.47. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 2.13.48. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
- 2.13.49. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 2.13.50. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee etc.;
- 2.13.51. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
- 2.13.52. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
- 2.13.53. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
- 2.13.54. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
  - 2.13.54.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
  - 2.13.54.2. Validação de contas desativadas em grupos privilegiados;

- 2.13.54.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;
- 2.13.54.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI- DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
- 2.13.54.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
- 2.13.54.6. Validação de contas com senhas que nunca expiram;
- 2.13.54.7. Validação de senhas reversíveis em GPOs;
- 2.13.54.8. Validação de uso de senhas reversíveis em contas de usuário;
- 2.13.54.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
- 2.13.54.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
- 2.13.54.11. Validação se o domínio possui um nível funcional desatualizado;
- 2.13.54.12. Validação de contas de usuário utilizando senha antiga;
- 2.13.54.13. Validação se o atributo AdminCount está definido em usuários padrão;
- 2.13.54.14. Validação do uso recente da conta de administrador padrão;
- 2.13.54.15. Validação de usuários com permissão para ingressar computadores no domínio;
- 2.13.54.16. Validação de contas dormentes;
- 2.13.54.17. Validação de computadores executando um sistema operacional obsoleto;
- 2.13.54.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
- 2.13.54.19. Validação de direitos perigosos configurados no Schema do AD;
- 2.13.54.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;
- 2.13.54.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
- 2.13.54.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 2.13.54.23. Validação da última alteração de senha do KDC;
- 2.13.54.24. Validação da última alteração da senha da conta SSO do Azure AD;
- 2.13.54.25. Validação de contas que podem ter senha em branco/vazia;
- 2.13.54.26. Validação de utilização do grupo nativo Protected Users;
- 2.13.54.27. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token etc.) perigosos atribuídos aos usuários;
- 2.13.54.28. Validação de possível senha em clear-text;
- 2.13.54.29. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
- 2.13.54.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
- 2.13.54.31. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
- 2.13.54.32. Validação de contas anormais nos grupos administrativos padrão do AD;
- 2.13.54.33. Validação de consistência no container adminSDHolder;
- 2.13.54.34. Validação de delegação Kerberos perigosa;
- 2.13.54.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 2.13.54.36. Validação de políticas de senha fracas aplicadas aos usuários;
- 2.13.54.37. Validação das permissões relacionadas às contas do Azure AD Connect;
- 2.13.54.38. Validação do ID do grupo primário do usuário (Primary Group ID);
- 2.13.54.39. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
- 2.13.54.40. Controladores de domínio gerenciados por usuários ilegítimos;
- 2.13.54.41. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
- 2.13.54.42. Validação de uso de protocolo Netlogon inseguro (ZeroLogon/CVE-2020-1472);
- 2.13.55. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
- 2.13.55.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;

- 2.13.55.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
- 2.13.55.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
- 2.13.55.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 2.13.55.5. Detecção e resposta a ataques;
- 2.13.55.6. Monitorar continuamente os indicadores de possíveis ataques como DCSync, DCShadow,
- 2.13.55.7. Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
- 2.13.55.8. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
- 2.13.55.9. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
- 2.13.55.10. Apresentação de ataques em uma linha do tempo;
- 2.13.55.11. Investigar ameaças, reproduzir ataques e procurar por backdoors;
- 2.13.55.12. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 2.13.56. A solução deve ser capaz de enviar alertas por e-mail;
- 2.13.57. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
- 2.13.58. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 2.13.59. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
- 2.13.60. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;
- 2.13.61. Deve ser capaz de calcular a criticidade dos ativos da organização;
- 2.13.62. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;
- 2.13.63. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;
- 2.13.64. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
- 2.13.65. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;
- 2.13.66. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
- 2.13.67. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
- 2.13.68. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
- 2.13.69. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
- 2.13.70. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade.

### 3. Serviço de testes de intrusão (Pentest)

- 3.1. Antes de iniciar o serviço de teste de intrusão, a CONTRATADA deverá elaborar e formalizar os Termos de Responsabilidade e Confidencialidade, os quais devem ser assinados por ambas as partes, CONTRATADA e CONTRATANTE;
- 3.2. Os testes de intrusão ocorrerão sob demanda, de acordo com a adesão do item de serviço pelas CONTRATANTES aderentes;
- 3.3. A CONTRATADA deverá, na fase de planejamento, identificar os dispositivos e sistemas a serem testados, bem como o tipo de testes a serem realizados. O escopo previamente definido deverá ser formalmente autorizado pela CONTRATANTE técnica ATI;

- 3.4. A CONTRATADA realizará o levantamento de informações dos alvos, incluindo IP, serviços associados, sistemas e outras características, além de identificar vulnerabilidades expostas para exploração subsequente;
- 3.5. A CONTRATADA utilizará exploits e técnicas de hacking para simular ataques, com o objetivo de identificar o grau de exploração das vulnerabilidades encontradas;
- 3.6. Caso o analista obtenha sucesso na exploração, ele deverá simular o que um atacante real faria, explorando informações sensíveis e realizando ações maliciosas controladas, sem causar danos permanentes ao ambiente;
- 3.7. Ao final dos testes, a CONTRATADA deverá documentar todas as informações do processo, desde o planejamento até os resultados, com recomendações de correção detalhadas. O relatório completo deve ser entregue às autoridades responsáveis para iniciar o plano de correção;
- 3.8. Após o recebimento das recomendações, a CONTRATANTE deverá iniciar as correções necessárias para eliminar ou mitigar as vulnerabilidades ao nível mais seguro possível;
- 3.9. A CONTRATANTE terá um prazo de até 6 (seis) meses a contar da entrega do relatório para executar as correções necessárias. Ao final desse período, a CONTRATADA deverá executar um reteste, sem custos adicionais, para verificar a efetividade das medidas adotadas;
- 3.10. Caso as correções recomendadas não sejam implementadas dentro do prazo estabelecido, a CONTRATADA poderá encerrar a Ordem de Serviço, registrando formalmente a situação para fins de conformidade e auditoria;
- 3.11. Para a adequada prestação deste serviço a CONTRATADA deverá:
- 3.11.1. Seguir orientações e padrões internacionais, além dos especificados pela ATI;
- 3.11.2. Realizar testes de vulnerabilidades e invasão nos ativos designados no ambiente computacional, incluindo servidores, bancos de dados, ativos de rede e segurança;
- 3.11.3. Realizar os testes conforme definido na Ordem de Serviço (OS);
- 3.11.4. Realizar testes do tipo Gray Box conforme solicitado na OS;
- 3.11.5. Realizar testes a partir da rede interna da ATI ou da Internet, conforme determinação;
- 3.11.6. Respeitar as condições estabelecidas na OS para cada alvo;
- 3.11.7. Comunicar imediatamente qualquer atividade que possa comprometer o ambiente antes de sua execução;
- 3.11.8. Suspender imediatamente os testes caso causem indisponibilidade.
- 3.12. O teste de invasão deverá obedecer às seguintes fases:
- 3.12.1. Planejamento;
- 3.12.2. Descoberta;
- 3.12.3. Ataque;
- 3.12.4. Relatório do teste de invasão;
- 3.12.5. Reunião de apresentação do relatório e recomendações;
- 3.12.6. Reavaliação (caso necessário) sem custo adicional, conforme OS;
- 3.12.7. Relatório final do teste de invasão.
- 3.13. Planejamento:
- 3.13.1. Durante o planejamento, todas as premissas, atividades, processos e cronogramas devem ser detalhados e apresentados;
- 3.14. Descoberta:
- 3.14.1. A CONTRATADA deverá utilizar ferramentas licenciadas para análise e gestão de vulnerabilidades, bem como técnicas manuais, com aprovação prévia da CONTRATANTE. As fases de descoberta devem incluir:
- 3.14.1.1. Coleta passiva: Utilização de técnicas como whois, nslookup, buscas online, listas de discussão, dumpster diving e packet sniffing;
- 3.14.1.2. Coleta ativa: Utilização de técnicas como port scanning e varredura de vulnerabilidades;
- 3.14.1.3. A varredura de vulnerabilidade deverá verificar/identificar, entre outros:
- 3.14.1.3.1. Hosts ativos na rede;
- 3.14.1.3.2. Portas e serviços em execução;
- 3.14.1.3.3. Serviços ativos e vulneráveis nos hosts;
- 3.14.1.3.4. Sistemas operacionais;
- 3.14.1.3.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;
- 3.14.1.3.6. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- 3.14.1.3.7. Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;

- 3.14.1.3.8. Identificação de vetores de ataque e cenários para exploração;
- 3.14.1.3.9. Vulnerabilidades Detectadas (CVE);
- 3.14.1.3.10. Vulnerabilidades de Alto, Médio e Baixo Risco. Conforme o padrão Common Vulnerability Scoring System (CVSS) - <https://www.first.org/cvss/v3.1/specification-document>, item "Qualitative Severity Rating Scale";
- 3.14.1.3.11. Informações a serem aplicadas na fase de ataques;
- 3.14.1.4. Os serviços e aplicações web deverão verificar/identificar, entre outros:
  - 3.14.1.4.1. Uso indevido de sistema de arquivos e arquivos temporários;
  - 3.14.1.4.2. Evasão de informação por configurações default de tratamento de erros;
  - 3.14.1.4.3. Tratamento indevido de entrada;
  - 3.14.1.4.4. Problemas relacionados à má configuração dos serviços;
  - 3.14.1.4.5. Gerenciamento inseguro de sessões web.
- 3.15. Ataque (exploração):
  - 3.15.1. A CONTRATADA deverá executar ataques simulados, incluindo, mas não se limitando a:
    - 3.15.1.1. Violações do protocolo HTTP;
    - 3.15.1.2. SQL Injection;
    - 3.15.1.3. LDAP Injection;
    - 3.15.1.4. Cookie Tampering;
    - 3.15.1.5. CrossSite
    - 3.15.1.6. Scripting (XSS);
    - 3.15.1.7. Directory Transversal;
    - 3.15.1.8. Buffer Overflow;
    - 3.15.1.9. OS Command Execution;
    - 3.15.1.10. Command Injection;
    - 3.15.1.11. Remote Code Inclusion;
    - 3.15.1.12. Server Side Includes (SSI) Injection;
    - 3.15.1.13. File disclosure;
    - 3.15.1.14. Information Leak;
    - 3.15.1.15. Zero day attacks;
    - 3.15.1.16. Negação de serviço;
    - 3.15.1.17. Contra protocolo TCP;
    - 3.15.1.18. Ataques contra a aplicação.
  - 3.15.2. Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas, entre outras:
    - 3.15.2.1. Bugs em serviços, aplicativos e sistemas operacionais;
    - 3.15.2.2. SYN flooding;
    - 3.15.2.3. Fragmentação de pacotes de IP;
    - 3.15.2.4. Smurf e fraggle;
    - 3.15.2.5. Teardrop, nuke e land.
  - 3.15.3. Para ataques contra o protocolo TCP:
    - 3.15.3.1. Sequestro de conexões;
    - 3.15.3.2. Prognóstico de número de sequência do protocolo TCP:
      - 3.15.3.2.1. Ataque de Mitnick;
      - 3.15.3.2.2. Source routing.
  - 3.15.4. Para ataques em nível da aplicação:
    - 3.15.4.1. Buffer Overflow;
    - 3.15.4.2. Problemas com o SNMP;
    - 3.15.4.3. Vírus, worms e cavalos de Tróia.
  - 3.15.5. Injeção de Código:
    - 3.15.5.1. Ataques XSS (Cross site Script);
    - 3.15.5.2. Comprometimento do acesso remoto;
    - 3.15.5.3. Manutenção de acesso;

3.15.5.4. Encobrimento de rastros da invasão.

3.15.6. Phishing:

3.15.6.1. Phishing por e-mail;

3.15.6.2. Phishing nos sites;

3.15.6.3. Vishing;

3.15.6.4. Smishing;

3.15.6.5. Phishing nas redes sociais;

3.15.6.6. Spear phishing;

3.15.6.7. Dropbox phishing;

3.15.6.8. Google Docs phishing;

3.15.6.9. Whaling;

3.15.6.10. Spear phishing;

3.15.6.11. Whaling;

3.15.6.12. Fraude de CEO;

3.15.6.13. Pharming;

3.15.6.14. Clone phishing;

3.15.6.15. Manipulação de links;

3.15.6.16. Scripting entre sites.

3.16. Relatório final do teste de invasão:

3.16.1. Após a entrega do relatório preliminar, a CONTRATANTE analisará as recomendações e aplicará as medidas corretivas. Após a remediação, poderá solicitar à CONTRATADA, num período de até 6 (seis) meses, uma nova avaliação dos resultados, com a emissão de um novo relatório, sem custo adicional.

#### **4. Serviço de analistas de segurança ofensiva (Red Team)**

4.1. A CONTRATADA deverá dispor de uma equipe composta por especialistas em segurança da informação, com foco em simulações de ataques cibernéticos, visando à identificação e correção de vulnerabilidades antes que estas possam ser exploradas;

4.2. O analista de segurança ofensiva é responsável por:

4.2.1. Planejar e executar simulações de testes de intrusão em ambiente controlado, para validação e aprimoramento das defesas;

4.2.2. O analista deverá atuar como um potencial atacante, utilizando variadas táticas e técnicas de ataque (conforme a estrutura MITRE ATT&CK) para explorar vulnerabilidades em redes, sistemas e usuários definidos pela CONTRATANTE técnica ATI, com o objetivo de identificar brechas de segurança;

4.2.3. O analista será responsável por simular incidentes de segurança para avaliar a eficiência e eficácia do plano de resposta a incidentes, bem como a postura e preparação dos envolvidos;

4.2.4. O analista deverá realizar a identificação e análise das vulnerabilidades presentes nos sistemas, ativos, políticas e controles, avaliando os riscos associados, de modo a recomendar ações corretivas ou mitigadoras para minimizar possíveis impactos aos órgãos;

4.2.5. Deverá ministrar treinamentos em segurança ofensiva aos colaboradores do CIISC, em parceria com a equipe responsável pelas campanhas de conscientização no ADENDO IX – CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA DA NOVA REDE CORPORATIVA, a fim de sensibilizar os usuários sobre ameaças, boas práticas e respostas adequadas a incidentes;

4.2.6. O analista deverá emitir relatórios detalhados sobre os testes realizados, incluindo o status da segurança da rede, vulnerabilidades detectadas, recomendações de correção e os impactos potenciais em caso de não implementação das correções sugeridas;

4.3. Os testes de invasão devem ser coordenados com as campanhas de conscientização e alinhados ao plano de evolução da maturidade em segurança da informação do ADENDO IX – CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA DA NOVA REDE CORPORATIVA, a serem submetidos à aprovação da área técnica da CONTRATANTE técnica ATI.

## 5. Serviço de análise forense

5.1. A consultoria forense em respostas a incidentes cibernéticos tem como objetivo identificar, coletar, analisar e preservar evidências digitais de forma rigorosa e legalmente aceitável. Esse processo é essencial para a investigação de incidentes de segurança, permitindo que a organização compreenda a origem, o impacto e os métodos utilizados pelos atacantes, além de fornecer suporte em ações legais, se necessário;

5.2. Escopo mínimo dos serviços de Consultoria Forense:

5.2.1. Identificação de Evidências:

5.2.1.1. Levantamento Inicial: Realizar uma análise inicial para identificar sistemas e dispositivos afetados;

5.2.1.2. Inventário de Evidências: Catalogar todos os possíveis locais de armazenamento de evidências digitais, incluindo servidores, estações de trabalho, dispositivos móveis, logs de rede e sistemas de armazenamento;

5.2.2. Coleta de Evidências:

5.2.2.1. Preservação da Cena: Garantir que o ambiente digital seja preservado para evitar a adulteração de dados;

5.2.2.2. Ferramentas Forenses: Utilizar ferramentas forenses reconhecidas para a coleta de dados, garantindo a integridade das evidências;

5.2.2.3. Documentação: Manter um registro detalhado de todas as etapas de coleta, incluindo data, hora, responsável e método utilizado;

5.2.3. Análise Forense:

5.2.3.1. Exame de Dados: Analisar as evidências coletadas para identificar a origem e o método do ataque, bem como as possíveis vulnerabilidades exploradas;

5.2.3.2. Reconstituição do Incidente: Reconstituir a sequência de eventos que levaram ao incidente de segurança;

5.2.3.3. Análise de Malware: Realizar a análise de qualquer software malicioso encontrado para entender seu comportamento e impacto;

5.2.4. Relatório Forense:

5.2.4.1. Relatório Técnico: Elaboração de um relatório técnico detalhado que documenta todas as descobertas, incluindo timelines, dados de logs, análise de tráfego de rede e resultados da análise de malware;

5.2.4.2. Recomendações: Fornecimento de recomendações para mitigar vulnerabilidades descobertas e prevenir futuros incidentes;

5.2.4.3. Documentação para Ações Legais: Preparação de documentação que pode ser utilizada em ações legais, se necessário, assegurando que todas as evidências foram coletadas e armazenadas de acordo com os padrões legais;

5.3. Metodologia Forense:

5.3.1. Planejamento:

5.3.1.1. Definição do Escopo: Estabelecer os objetivos e o alcance da investigação forense;

5.3.1.2. Equipe Forense: Designar profissionais certificados e experientes em análise forense;

5.3.2. Execução:

5.3.2.1. Coleta e Preservação: Seguir procedimentos rigorosos para coleta e preservação de evidências;

5.3.2.2. Análise Detalhada: Utilizar técnicas avançadas para análise de dados, reconstituição de eventos e identificação de vulnerabilidades;

5.3.3. Relatório e Apresentação:

5.3.3.1. Documentação Completa: Garantir que todas as etapas da investigação sejam documentadas de forma detalhada e clara;

5.3.3.2. Apresentação aos Stakeholders: Apresentar os resultados da análise forense aos stakeholders relevantes, incluindo a equipe de TI, departamento jurídico e alta administração;

5.4. Entregáveis

5.4.1. Relatórios de Coleta de Evidências: Documentação detalhada das evidências coletadas e métodos utilizados;

5.4.2. Análise Forense Completa: Relatórios detalhados das análises realizadas, incluindo timelines e identificação de vulnerabilidades;

5.4.3. Recomendações de Mitigação: Sugestões práticas para melhorar a segurança e prevenir futuros incidentes;

5.4.4. Documentação Legal: Relatórios e evidências formatados para suporte em possíveis ações legais.

## 6. Certificações

- 6.1. Os níveis mínimos de conhecimento a serem requeridos à CONTRATADA para comprovar a existência de pessoal qualificado estão presentes nos termos do presente tópico;
- 6.2. Os analistas de segurança ofensiva (Red Team) e os executores dos testes de intrusão (Pentest) devem portar, no mínimo, uma das certificações:
  - 6.2.1. CEH (Certified Ethical Hacker)
  - 6.2.2. OSCP (Offensive Security Certified Professional)
  - 6.2.3. GPEN (Certified Penetration Tester)
  - 6.2.4. CPENT (Certified Penetration Testing Professional)
  - 6.2.5. GXPEN (Exploit Researcher and Advanced Penetration Tester)
- 6.3. Os analistas forenses devem portar, no mínimo, uma das certificações:
  - 6.3.1. GCFA (GIAC Certified Forensic Analyst)
  - 6.3.2. CHFI (Computer Hacking Forensic Investigator)
  - 6.3.3. CCFP (Certified Cyber Forensics Professional)
- 6.4. Todas as certificações deverão estar válidas e ativas durante o período do contrato;
- 6.5. Certificações equivalentes reconhecidas internacionalmente poderão ser aceitas mediante análise e validação pela CONTRATANTE.

## ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM

1. A LICITANTE, quando fizer uso de soluções em nuvem Infraestrutura como Serviço (IaaS - Infrastructure as a Service), deverá atender aos requisitos mínimos abaixo para sustentar todos os serviços e aplicações obedecendo, obrigatoriamente, aos requisitos definidos neste Termo de Referência, além de normas e padrões de qualidade e segurança aplicáveis.
  - 1.1. A solução deverá ser implantada em datacenters redundantes, localizados em, no mínimo, duas cidades distintas, preferencialmente em estados diferentes, com o objetivo de assegurar alta disponibilidade dos serviços;
    - 1.1.1. Os servidores dos serviços de voz e de contact center deverão estar hospedados em datacenters localizados no território nacional, em conformidade com as regulamentações brasileiras relativas à proteção de dados;
    - 1.1.2. A infraestrutura deverá ser compatível com soluções VoIP/SIP, de acordo com o padrão RFC 3261, estabelecido pelo IETF (Internet Engineering Task Force).
  - 1.2. A solução deve possuir alta disponibilidade (High Availability – HA) no modo ativo-ativo, de forma que quando um dos datacenters for perdido, o outro datacenter mantém a comunicação sem interrupção do serviço de comunicação dos usuários (não deverá ocorrer perda de ligações ou indisponibilidade do sistema, devendo o processamento ser transparente e sem impacto para o usuário).
    - 1.2.1. A solução deverá permitir conexão por meio de links SIP Trunk com ambos os datacenters, garantindo a continuidade do serviço mesmo em caso de falha de um dos centros de dados;
    - 1.2.2. As manutenções e substituições de hardware deverão ser realizadas sem necessidade de paralisação dos serviços, garantindo assim a operação ininterrupta da solução.
  - 1.3. A solução deve permitir a detecção de degradação em um datacenter e migração dos serviços para o segundo datacenter, garantindo a continuidade dos serviços enquanto o datacenter degradado é recuperado.
  - 1.4. A CONTRATADA deverá utilizar datacenters e/ou soluções em nuvem envolvidos na prestação dos serviços que atendam, no mínimo, aos seguintes requisitos técnicos e operacionais, assegurando qualidade, segurança da informação, proteção de dados e continuidade de negócios, em conformidade com as melhores práticas do setor, demonstrando:
    - 1.4.1. conformidade com os parâmetros físicos, de disponibilidade e redundância compatíveis com a classificação TIA-942 Rated 3, ou Tier III da Uptime Institute.

- 1.4.2. proteção física das instalações do datacenter, com controles de acesso físico, climatização, redundância energética e sistemas de prevenção e combate a incêndio.
- 1.4.3. processos de gestão da qualidade padronizados e documentados, com mecanismos de auditoria e melhoria contínua implementados.
- 1.4.4. controles específicos para segurança da informação em ambientes de nuvem, com segregação de funções, criptografia de dados em trânsito e em repouso, controle de acesso baseado em funções, e rastreabilidade de logs.
- 1.4.5. proteção de dados pessoais em ambientes de nuvem, com políticas e controles voltados à privacidade e consentimento do titular dos dados, aderentes à LGPD.
- 1.4.6. adoção de políticas e mecanismos de continuidade de negócios e recuperação de desastres, com planos de contingência testados, documentados e integrados ao monitoramento.
- 1.4.7. conformidade com controles de segurança reconhecidos pela Cloud Security Alliance (CSA), contemplando aspectos como transparência, controle de acesso, resiliência, gestão de vulnerabilidades, gestão de incidentes e conformidade legal.
- 1.4.8. conformidade com a legislação brasileira aplicável, incluindo a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet.
- 1.5. A homologação de qualquer serviço contratado para a Nova Rede Corporativa do Governo do Estado de Pernambuco que envolva datacenters ou soluções em nuvem estará condicionada à apresentação, pela CONTRATADA, de documentação comprobatória do atendimento a todos os requisitos estabelecidos neste Adendo.
- 1.5.1. Caso a CONTRATADA opte por subcontratar serviços de datacenter ou soluções em nuvem, dentro dos limites estabelecidos no Termo de Referência, deverá apresentar, no momento da homologação dos serviços, a comprovação formal da relação contratual com a subcontratada, acompanhada da documentação que comprove o atendimento às exigências previstas neste Adendo.
- 1.5.2. A comprovação do atendimento aos requisitos técnicos e operacionais listados nos itens 1.4.1 a 1.4.8 poderá ser feita por meio de documentação técnica, relatórios de auditoria, declarações formais, políticas internas, certificações (se houver), evidências operacionais, ou outros meios equivalentes, a serem avaliados pela CONTRATANTE.
- 1.6. A solução deve possuir redundância de rede, com múltiplos provedores de internet e roteamento inteligente, para assegurar conectividade contínua mesmo em caso de falha de um dos provedores.
- 1.7. A solução deve garantir segurança física nos datacenters, incluindo vigilância 24/7, controle de acesso rigoroso, sistemas de detecção de intrusão e monitoramento por câmeras.
- 1.8. A solução deve assegurar segurança da informação, implementando criptografia de dados em trânsito e em repouso, além de políticas de segurança alinhadas com a LGPD (Lei Geral de Proteção de Dados).
- 1.9. A solução deve possuir redundância elétrica completa, incluindo sistemas de UPS (No-Break), geradores de energia e entradas de energia redundantes, para evitar interrupções em caso de falhas na rede elétrica.
- 1.10. A solução deve contar com sistemas de refrigeração redundantes, garantindo a manutenção das condições ambientais ideais para o funcionamento dos equipamentos da solução proposta.
- 1.11. A solução deve dispor de planos de *backup* e recuperação de desastres (Disaster Recovery) definidos, com realização de *backups* regulares e testes periódicos dos procedimentos de recuperação. Estes deverão estar à disposição da CONTRATANTE sempre que solicitados.
- 1.12. A solução deve fornecer Acordos de Nível de Serviço (SLA) que garantam disponibilidade superior a 99,95%, com penalidades definidas em caso de não cumprimento, conforme previsto no item de Nível Mínimo de Serviço (NMS) deste TR.
- 1.13. A CONTRATADA deve garantir que a solução fornecida seja totalmente integrada e gerenciável pela equipe de operação e gerenciamento do Centro Integrado de Inteligência e Segurança Cibernética (CIISC) da Nova Rede Corporativa. Todos os componentes da solução devem permitir monitoramento centralizado e gerenciamento

unificado pelas equipes do CIISC, possibilitando o controle de todas as funções de segurança e conectividade de forma integrada.

1.14. A solução deve ser plenamente compatível com o protocolo TCP/IPv6, garantindo a interoperabilidade com todos os sistemas existentes e planejados para a Nova Rede Corporativa. Essa compatibilidade deve assegurar a conformidade tecnológica com os padrões de rede adotados e permitir o funcionamento contínuo e adaptável às mudanças e expansões da infraestrutura.

1.15. A solução deve incluir todos os recursos necessários para o suporte ao serviço de voz da nova rede corporativa, assegurando que as comunicações de voz ocorram com continuidade, qualidade e integridade. A CONTRATADA deve garantir que o serviço de voz esteja integrado à solução e operando com os padrões de qualidade exigidos, evitando interrupções e mantendo a clareza nas comunicações entre usuários da rede.

1.16. A equipe do serviço CIISC será responsável pela segurança cibernética da rede, e, portanto, a solução fornecida pela CONTRATADA deve incluir todos os mecanismos de segurança necessários para a proteção da rede contra ameaças cibernéticas. Esses mecanismos devem contemplar prevenção, detecção e resposta a incidentes de segurança, com recursos para monitoramento contínuo e bloqueio de ataques, reduzindo a exposição a riscos cibernéticos.

1.17. A solução deve assegurar a integridade dos dados e prover mecanismos robustos de controle de acesso, prevenindo acessos não autorizados e protegendo informações sensíveis da rede. Todos os componentes da solução devem atender aos padrões de segurança estabelecidos no Termo de Referência e no CIISC, permitindo uma gestão segura de permissões e credenciais na Nova Rede Corporativa.

1.18. A CONTRATADA deve garantir que todos os elementos da solução estejam alinhados com as melhores práticas de segurança cibernética, facilitando a atuação eficaz da equipe do Centro Integrado de Inteligência e Segurança Cibernética (CIISC) na identificação e mitigação de riscos. Os componentes fornecidos devem possibilitar a gestão proativa de vulnerabilidades, habilitando a equipe do CIISC a monitorar e responder rapidamente a potenciais ameaças e vulnerabilidades.

1.19. A solução deve incluir sistemas avançados de monitoramento e alerta em tempo real, permitindo a detecção proativa de falhas e a rápida resolução de incidentes.

1.20. A solução deve estar em conformidade com requisitos regulatórios específicos do setor de atuação da empresa, caso aplicável.

1.21. A solução deve oferecer suporte técnico e serviços de manutenção 24/7, com equipes especializadas para atendimento e resolução de problemas.

1.22. O datacenter deve implementar medidas robustas de segurança cibernética, incluindo proteção contra ataques DDoS, firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS).

1.23. Os datacenters deverão seguir práticas sustentáveis e eficientes em termos energéticos, alinhadas a padrões ambientais reconhecidos, promovendo responsabilidade ambiental.

2. A CONTRATADA será responsável pela configuração e integração de todos os equipamentos fornecidos, garantindo o pleno funcionamento da solução e a interoperabilidade dos componentes necessários para a prestação dos serviços.

3. A CONTRATADA deverá conduzir uma fase de validação da infraestrutura, garantindo que todos os componentes da solução estejam configurados e integrados corretamente. Deverão ser realizados, apresentados e documentados os seguintes testes mínimos no relatório final de entrega:

3.1. Testes de conectividade e desempenho entre a infraestrutura local e a nuvem dedicada;

3.2. Testes de qualidade de serviço (QoS), como latência, jitter e disponibilidade, para assegurar uma comunicação estável e de alta qualidade;

3.3. Testes de escalabilidade, para garantir que a solução seja capaz de atender ao aumento da demanda sem perda de qualidade.

4. Os equipamentos instalados deverão estar configurados de modo a garantir total operabilidade e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade.

## **ADENDO XII – SERVIÇO DE COMUNICAÇÃO UNIFICADA (UNIFIED COMMUNICATION - UC)**

### **1. Requisitos gerais**

1.1. A Licitante deverá apresentar a descrição de todos os produtos/soluções a serem utilizados, obedecendo, obrigatoriamente, a todos os requisitos definidos neste Termo de Referência.

1.2. A solução deve ser instalada em NUVEM DEDICADA, compreendida como um recurso virtual com dedicação exclusiva à rede corporativa.

1.3. A operação da administração dos usuários deste serviço será realizada pelo Serviço CIISC - Centro Integrado de Inteligência e Segurança Cibernética;

1.4. A Gerência Técnica da Rede (ATI) deverá ter acesso de leitura a todas as configurações do serviço.

1.5. A Gerência Técnica da Rede (ATI) definirá as políticas de uso do serviço;

1.6. A CONTRATADA deverá fornecer e manter a versão mais recente de todos os componentes (hardware e software) da solução contratada.

1.7. A métrica de precificação será por conta de usuário.

1.8. Fornecer todos os componentes necessários para o pleno funcionamento do serviço e integração com as plataformas requisitas em nuvem dedicada.

1.9. Realizar todas as configurações necessárias, nos equipamentos fornecidos pela CONTRATADA, para o pleno uso do serviço aqui descrito;

1.10. Integrar-se a todos os serviços de voz descritos neste Termo de Referência;

1.11. A solução deverá operar de forma integrada ao Serviço de Voz, de modo que o usuário que possua o recurso de Comunicação Unificada (Unified Communications and Collaboration – UCC) possa ter vinculado o seu número (NIM) ao serviço de UCC, sendo possível efetuar e receber chamadas da rede pública de telefonia (STPC), garantindo compatibilidade com o protocolo SIP padrão (RFC 3261);

1.12. Implementar o número único de chamadas, fazendo o roteamento das chamadas de acordo com as preferências do usuário:

1.12.1. As preferências dos usuários devem ser configuradas diretamente no aplicativo, podendo ser direcionado para seus dispositivos preferenciais ou qualquer NIM da Nova Rede Corporativa;

1.13. Oferecer, no mínimo, os seguintes perfis:

1.13.1. Administrador - Permissão para criar, excluir e alterar dados e contas dos clientes, além de acessar o portal de operações;

1.13.2. Cliente – Usuário comum.

1.14. Oferecer suporte técnico, em idioma português, através de formulário da Web e contato telefônico através do *service desk* do serviço CIISC - Centro Integrado de Inteligência e Segurança Cibernética;

1.15. Oferecer página web de administração do serviço para que administradores gerenciem todo o conjunto de serviços disponíveis. Após entrar no site de administração, os administradores de serviço poderão realizar diversas tarefas comuns, tais como adicionar e excluir usuários, modificar classe de um usuário, entre outras;

- 1.16. Permitir aos usuários finais da solução fazer login uma vez e acessar de forma conveniente todos os serviços sem ter que digitar a senha repetidas vezes;
- 1.17. Possuir integração com sistemas que usem LDAP, LDAP/AD, mantendo as mesmas senhas definidas na base de usuários da CONTRATANTE, sendo necessária a aprovação da ATI para uso de qualquer outra solução de base de autenticação;
- 1.18. Oferecer as interfaces e telas dos softwares para o usuário cliente no idioma Português do Brasil;
- 1.19. Disponibilizar conteúdo de ajuda, de forma online, para usuários clientes em português brasileiro;
- 1.20. Disponibilizar conteúdo de ajuda, de forma online, para usuários administradores;
- 1.21. Oferecer recurso de busca, onde seja possível pesquisar pela informação desejada em todas as conversas que já foram realizadas, incluindo pessoas, arquivos e palavras específicas, no caso de acesso Web Browser, este recurso deverá estar compatível com os recursos de busca do Browser;
- 1.22. Permitir estabelecer sessões de mensagens instantâneas com pessoas da organização ou por meio de conexão com os serviços na nuvem de outras entidades que usam o mesmo serviço;
- 1.23. Permitir estabelecer sessões de áudio e vídeo entre dois ou mais terminais (computador ou dispositivo móvel);
- 1.24. Encriptar de forma segura todo o conteúdo das mensagens instantâneas, utilizar no mínimo os protocolos HTTPS, SSL ou SIGNAL, ou outro protocolo de criptografia de mensagens equivalente;
- 1.25. Permitir incluir imagens, vídeos e urls na mensagem;
- 1.26. Incluir uma marca com a hora nas mensagens instantâneas;
- 1.27. Permitir adicionar participantes a um grupo ou a uma conversa já existente no sistema de mensagens instantâneas;
- 1.28. Possuir estado de presença, permitindo aos demais usuários visualizar os status na lista de contatos da ferramenta de mensagens instantâneas;
- 1.29. Fornecer pelo menos os seguintes estados de presença: “Disponível”, “Ocupado”, “Ausente” e “Desconectado”;
- 1.30. Permitir modificar manualmente ou automaticamente, em caso de inatividade, o estado de presença;
- 1.31. Permitir que o usuário realize uma conferência de áudio (voz), vídeo, web e compartilhamento de conteúdo sob o mesmo serviço;
- 1.32. Permitir que o usuário compartilhe a sua tela, como conferência de vídeo;
- 1.33. Possuir a capacidade de enviar um convite de conferência web, via e-mail, a todos os convidados com o link de acesso para a conferência. O convite deve conter no mínimo a data, hora, assunto, Número de Identificação Multidigital (NIM) para acesso à conferência utilizando apenas telefone e nome do demandante da conferência web;
- 1.34. Possuir capacidade de adaptação às condições de tráfego da rede, na realização de chamadas de vídeo e/ou áudio, utilizando codecs adaptativos à largura de banda disponível entre os usuários da chamada;
- 1.35. Implementar recursos de conversa em grupo, onde:
  - 1.35.1. Possua todos os recursos multimídia de uma conversa ponto-a-ponto: voz, vídeo, chat, compartilhamento de tela, envio/recebimento de arquivos, independentemente de ser usuário ou convidado;
  - 1.35.2. Seja permitida, no mínimo, a participação de 100 (cem) pessoas;
  - 1.35.3. Possa iniciar a conferência, com todos os participantes, ao acionamento de apenas um clique;
  - 1.35.4. Seja possível determinar um “Moderador” para a conferência, ou deixá-la sem moderação;

1.35.5. Deve permitir o envio de convites (invites) com os dados de acesso à conferência. No horário agendado, o sistema deverá iniciar a conferência automaticamente ou aguardar que o moderador/organizador a inicie manualmente;

1.35.6. A solução deve garantir que qualquer aparelho telefônico na rede pública possa participar de uma conferência, via voz, ao ligar para um NIM (Número de Identificação Multidigital) da Nova Rede Corporativa.

1.36. A solução deverá suportar, no mínimo, 30% (trinta por cento) de sessões simultâneas em relação ao total de contas de usuários, devendo permitir expansão modular e escalável conforme o aumento da base de usuários, sem necessidade de substituição de infraestrutura ou alteração contratual da arquitetura existente.

1.36.1. A CONTRATADA será responsável por dimensionar e ajustar a capacidade da solução, de forma a assegurar desempenho, estabilidade, qualidade de comunicação e continuidade do serviço durante picos de uso, observando os Níveis Mínimos de Serviço (NMS) estabelecidos no ADENDO II.

1.37. Realizar conversas de áudio, sem interrupções, quando conectado com largura de banda mínima de 64 Kbps;

1.38. Realizar conversas de vídeo, sem interrupções, quando conectado com largura de banda mínima de 512 Kbps;

1.39. A solução de Comunicação Unificada (UC) deverá atender aos seguintes requisitos de gravação:

1.39.1. A solução deve permitir a gravação de todas as sessões de comunicação, incluindo áudio, vídeo e compartilhamento de tela, garantindo que a qualidade da gravação seja equivalente à da transmissão ao vivo, sem degradações.

1.39.2. As gravações devem ser armazenadas em um ambiente seguro na nuvem, acessível aos usuários autorizados. A CONTRATADA deverá fornecer um repositório centralizado, com acesso através de interface web, que permita a busca, download e reprodução das gravações de maneira eficiente, incluindo mecanismos de busca por data, participante ou título da sessão, e reprodução direta na interface web, sem necessidade de softwares adicionais.

1.39.3. O armazenamento deve respeitar os requisitos de segurança e privacidade, com a criptografia dos dados em repouso e em trânsito, garantindo a conformidade com as normas vigentes de proteção de dados.

1.39.4. Para as videochamadas gravadas, as gravações deverão ser armazenadas por um período mínimo de 30 dias, ou tempo menor se especificado pela política de retenção do Governo. Deverá ser possível configurar políticas de retenção, garantindo a eliminação segura das gravações ao término do período.

1.39.5. Para as demais mensagens o tempo de retenção deverá ser de todo período contratado.

1.39.6. O sistema deve implementar controle de acesso baseado em papéis, conforme conceito de "Role-Based Access Control (RBAC), permitindo que apenas usuários devidamente autorizados possam acessar, visualizar, editar ou excluir gravações;

1.39.7. Deve haver registro de logs de auditoria para todas as ações de acesso e manipulação das gravações, garantindo rastreabilidade e transparência das operações;

1.39.8. As gravações devem ser disponibilizadas em formatos compatíveis com os principais players de mídia, como MP4 para vídeo e MP3 para áudio, garantindo ampla compatibilidade e facilidade de uso.

1.39.9. A solução deve permitir a exportação das gravações em massa, mediante solicitação, e possibilitar a integração com sistemas externos para arquivamento ou análise posterior, utilizando APIs padronizadas.

1.39.10. A solução deve realizar a gravação programada das conferências colaborativas, com início automático para reuniões específicas, ou a gravação sob demanda, para que o responsável pela reunião possa iniciar ou parar a gravação conforme necessário.

1.39.11. A solução deve incluir funcionalidades que permitam a notificação dos participantes sobre a gravação da sessão, de modo a garantir o conhecimento conforme regulamentações de privacidade e proteção de dados.

- 1.40. Realizar conferências de vídeo, sem interrupções, com 'N' participantes, quando conectado com largura de banda mínima de 512 Kbps \* N + 64 Kbps. Em outras palavras, para 3 usuários, o serviço deverá executar a conferência sem interrupções se os usuários tiverem largura de banda mínima de 512 \* 3 + 64 Kbps, que resultará em 1.540 Kbps;
- 1.41. Permitir, prioritariamente, a vinculação a qualquer tipo de Ponto de Voz Fixo (PVF), possibilitando que o serviço também possa ser vinculado a um Ponto de Voz Móvel (PVM) ou a qualquer outro dispositivo móvel do usuário compatível com o serviço;
- 1.42. Suportar codecs baseados em padrões abertos para chamadas de vídeo e/ou áudio;
- 1.43. Suportar câmeras de vídeo tipo USB conectadas ao PCs ou Notebooks, quando realizar sessões ou conferências de vídeo;
- 1.44. Suportar câmeras de vídeo integradas a Computadores (All in one), Notebooks e dispositivos móveis, quando realizar sessões ou conferências de vídeo;
- 1.45. Permitir ser acessado pelos usuários através do navegador via web (Microsoft Edge, Mozilla Firefox, Google Chrome ou Safari, versão mais atual) ou aplicativo cliente instalado no dispositivo móvel (iOS ou Android, versão mais atual);
- 1.46. Permitir que usuários possam criar uma nova conversa com qualquer usuário do sistema, sem necessitar que o destinatário da mensagem seja um contato salvo no dispositivo;
- 1.47. Permitir que os usuários criem grupos de contatos;
- 1.48. Permitir que usuários enviem mensagens instantâneas a grupos de contatos;
- 1.49. Permitir que usuários se conectem de qualquer lugar através da Internet utilizando computadores ou dispositivos móveis, podendo estabelecer áudio conferências, videoconferências e web conferências, como reuniões programadas e reuniões de colaboração não programadas no sistema (ad-hoc);
- 1.50. Permitir que usuários não cadastrados na solução participem de conferências de vídeo ou áudio, através de mecanismo de acesso como "convidado". O mesmo mecanismo deve exigir uma forma de identificar o convidado;
- 1.51. Permitir que os usuários e convidados possam transferir uma conferência de vídeo ou áudio do computador para um dispositivo móvel e vice-versa, sem interrupções.
- 1.52. Permitir que o administrador, através do portal de administração, possa realizar ações tais como:
- 1.52.1. Ativar ou desativar a solução de comunicação unificada;
- 1.52.2. Criar usuários e atribuir recursos e licenças que habilitem o uso da solução de comunicação unificada;
- 1.52.3. Acessar a ajuda online;
- 1.53. Permitir, quando as conferências de voz ou áudio agendadas tiverem moderador, que os participantes se comuniquem apenas após o moderador estar conectado à sala.

## 2. Segurança e privacidade

- 2.1. A CONTRATADA não recolherá qualquer informação sobre o uso da Internet ou a localização por parte dos usuários;
- 2.2. A solução deverá prover mecanismos seguros de recuperação de senhas;
- 2.3. A solução deverá identificar tentativas de acesso inválidas;
- 2.4. A solução deverá prover mecanismos para mitigar ataques de força bruta;
- 2.5. A solução não deverá possuir credenciais de acesso em texto claro em arquivos de configuração.

### 3. Criptografia

- 3.1. Não será permitida a utilização de criptografia com padrões de segurança inferiores aos especificados neste documento, sendo responsabilidade da CONTRATADA adotar todas as medidas técnicas e administrativas necessárias para garantir essa conformidade;
- 3.2. A CONTRATADA deverá implementar medidas técnicas que impeçam a utilização dos serviços de forma insegura, bloqueando conexões com padrões criptográficos abaixo dos exigidos. Desta forma, a CONTRATADA deve proteger os usuários da redução inadvertida do grau de proteção devido ao uso de dispositivos ou softwares inadequados ou obsoletos, bem como de várias classes de ataques MITM (*man-in-the-middle*);
- 3.3. A solução deverá permitir o acesso apenas através de protocolos de criptografia TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) com chave de, no mínimo, 128 bits;
- 3.4. O protocolo TLS 1.2 (ou superior) deverá ser suportado em todos os servidores da solução;
- 3.5. É proibida a utilização dos protocolos SSLv2 e SSLv3, pois são considerados inseguros;
- 3.6. É proibido o acesso ao serviço através de dispositivos que não suportem o protocolo TLS;
- 3.7. É recomendável evitar os algoritmos que são especialmente suscetíveis a falhas no gerador de números aleatórios, como DSA, ECDSA e DH.

### 4. Implantação dos serviços

- 4.1. A CONTRATADA deverá fornecer documentação técnica completa original de todos os componentes fornecidos, em língua portuguesa ou inglesa. A documentação poderá ser fornecida em meio impresso e/ou meio eletrônico. Quaisquer atualizações da documentação deverão ser fornecidas, sem ônus, durante o período de garantia dos produtos fornecidos;
- 4.2. A CONTRATADA deverá fornecer documentação de configuração da rede contendo, no mínimo:
- 4.2.1. Diagrama de conexão física da solução;
  - 4.2.2. Configuração realizada em cada equipamento;
  - 4.2.3. Documentação de toda a estrutura configurada;
  - 4.2.4. Descrição de todos os produtos a serem instalados;
  - 4.2.5. Diagrama de interconexão dos equipamentos;
  - 4.2.6. Projeto lógico de configuração.
- 4.3. A CONTRATADA deverá realizar a configuração e integração de todos os equipamentos, objeto de fornecimento, que garantam o correto funcionamento da solução;
- 4.4. Os equipamentos instalados deverão estar configurados de modo a garantir total operabilidade e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade.

### 5. Capacitação dos Usuários Finais

- 5.1. A CONTRATADA deverá disponibilizar instruções de uso e capacitação funcional sobre todos os recursos da solução, no formato EAD (Ensino a Distância) e em versão gravada, permitindo que os usuários possam acessar e revisar o conteúdo sempre que necessário;
- 5.2. As instruções deverão contemplar o uso dos principais recursos da Comunicação Unificada (UC), incluindo softphones, funcionalidades colaborativas, integração com contact center e demais recursos aplicáveis;

5.3. A CONTRATADA deverá fornecer materiais de apoio digital e assegurar que os conteúdos permaneçam acessíveis aos usuários durante todo o período contratual.

## 6. Gestão de mudanças

6.1. Todas as atividades de implantação que envolvam a alteração da infraestrutura existente deverão ser geridas por um processo formal de gestão de mudanças, contemplando:

6.1.1. Análise de impacto para o ambiente atual.

6.1.2. Aprovação da CONTRATANTE antes da execução de mudanças significativas.

## 7. Fase de suporte pós-implantação (Go-Live)

7.1. Após a implantação, a CONTRATADA deverá fornecer suporte pós-implantação por um período mínimo de 90 dias, que deverá incluir:

7.1.1. Acompanhamento contínuo da operação para ajuste fino da solução.

7.1.2. Atendimento para suporte e resolução de incidentes, com tempo de resposta de até 24 horas corridas, exceto finais de semana e feriado.

## ADENDO XIII – SERVIÇO DE PONTOS DE VOZ FIXOS (PVF) e TRÁFEGO TELEFÔNICO EXTRARREDE

### 1. Requisitos gerais

1.1. A Licitante deve apresentar na Proposta de preços a descrição de como será a prestação dos serviços de Ponto de Voz Fixo para NOVA REDE CORPORATIVA, atendendo aos princípios gerais e requisitos contidos neste Termo de Referência, e respeitando os requisitos obrigatórios, abaixo elencados:

1.2. Prover o Serviço de Ponto de Voz Fixo (PVFs) para os PCs da Nova Rede Corporativa, os quais serão formalizados pelos CONTRATANTES Aderentes através de Termos Aditivos de Adesão conforme previsto no Edital e seus anexos.

1.3. Prover, instalar, configurar e manter aparelhos telefônicos para uso da telefonia fixa, denominado de Pontos de Voz Fixos (PVFs) em diversas modalidades, tais como:

1.3.1. Telefone Wi-Fi IP: Equipamentos compatíveis com as redes sem fio especificadas neste TR, oferecendo criptografia de dados para garantir segurança e proporcionando mobilidade. A modalidade inclui tanto modelos de mesa quanto dispositivos portáteis.

1.3.2. Telefone DECT IP: Aparelhos DECT com suporte a comunicação por IP, oferecendo criptografia segura para chamadas e proporcionando mobilidade, sendo disponíveis em modelos portáteis.

1.3.3. Softphone (Telefone por Software): Solução que permita utilização em computadores ou dispositivos móveis, garantindo a funcionalidade de voz por meio de software compatível com os sistemas operacionais mais utilizados no mercado (Windows, macOS, Android e iOS).

1.3.4. Virtualização de PVFs: A CONTRATADA deverá possibilitar a virtualização dos números de identificação dos PVFs, permitindo a flexibilidade na alocação e no uso dos recursos.

1.4. A contratada deverá prover um servidor de voz em nuvem e com segurança, atendendo a todos os requisitos/especificações do **ADENDO XI - INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM**, no entanto, não será exigida a exclusividade do hardware físico utilizado pela solução, desde que haja isolamento lógico e segurança garantida.

1.4.1. A CONTRATADA deverá apresentar o certificado de conformidade técnica para telecomunicações, emitido pela Agência Nacional de Telecomunicações (ANATEL) ou órgão credenciado pela ANATEL para homologação do serviço.

1.4.2. Ser baseado em software utilizando comunicação VoIP baseado no protocolo SIP, conforme RFC 3261 da IETF.

1.4.3. Ser baseada em tecnologia de telefonia IP (SIP - RFC 3261 da IETF), e deverá permitir, através de recursos próprios de hardware e software adequados, utilizando a rede de dados corporativa da CONTRATANTE, interligação a outros servidores de voz ou gateways de voz do mesmo ou de outros fornecedores para equipamentos não integrantes do escopo de fornecimento da Solução de Voz, Comunicação Unificada e Contact Center por meio da tecnologia de voz sobre IP (VoIP).

1.4.4. A solução deverá suportar todos os recursos exigidos de forma integrada, podendo ser composta por múltiplos componentes, desde que operem de maneira transparente para os usuários e para a administração, como um sistema lógico único.

1.4.5. Suportar todo o tráfego extrarrede (origem ou destino) da Rede Pública de Telefonia Comutada (RPTC) devendo seguir as seguintes regras:

1.4.5.1. A CONTRATADA deverá garantir que não haverá tarifação para chamadas intragrupo e extrarrede, com exceção das chamadas do tipo Discagem Direta Internacional (DDI). Para chamadas realizadas dentro do território nacional (fixa ou móvel, independente da operadora), a CONTRATADA deverá prover ligações ilimitadas, sem qualquer custo adicional para o Governo.

1.4.5.2. A CONTRATADA deverá incluir, obrigatoriamente, na solução proposta, uma franquia anual de 1000 (mil) minutos para chamadas DDI, compartilhada entre todos os ramais contratados pelo Estado e utilizável por qualquer ramal que tenha categoria habilitada para realizar chamadas DDI, sem custo adicional.

1.4.5.2.1. Essa franquia será compartilhada entre todos os ramais contratados pelo Estado e poderá ser utilizada por qualquer ramal que tenha categoria habilitada para realizar chamadas DDI.

1.4.5.3. A CONTRATADA deverá prover serviço de tráfego telefônico extrarrede com ligações ilimitadas para os Pontos de Voz Fixo (PVF), abrangendo todos os tipos de ligação (local, longa distância, móvel ou fixo), para qualquer operadora, dentro do território nacional, sem custos adicionais por ligação ou tarifação individualizada. O custo deste serviço deverá ser integrado ao valor do respectivo serviço de PVF associado, sem discriminação financeira por uso.

1.4.5.4. A solução deverá permitir e realizar, quando solicitado, a categorização de ramais, viabilizando a configuração de perfis de uso que determinem as permissões para realização de chamadas, incluindo chamadas locais, interurbanas, móveis, internacionais (DDI) ou somente intragrupo.

1.4.5.5. Possuir a quantidade de canais necessários para o escoamento de todo o tráfego extrarrede, devendo ampliar esta quantidade quando sua capacidade atingir no máximo 70% em sua média mensal nos Horários de Maior Movimento (HMM);

1.4.5.6. Para complementar informações que possam contribuir no dimensionamento da solução por parte da CONTRATADA, foi disponibilizado informações adicionais no **ANEXO D (QUANTITATIVO DE TRAFÉGO EXTRARREDE E ESPECIFICAÇÕES TÉCNICAS PARA DIMENSIONAMENTO DE SOLUÇÃO DE VOZ EM CLOUD)**.

1.4.6. A solução deverá ser plenamente integrada às redes de dados corporativas da CONTRATANTE, viabilizando o transporte de tráfego de voz sobre IP (VoIP) com qualidade e eficiência. A integração deverá ser compatível com os padrões técnicos e operacionais da infraestrutura de rede da CONTRATANTE, assegurando o funcionamento adequado dos serviços de voz contratados.

1.4.7. O serviço de Ponto de voz Fixo (PVFs) deverá ser instalado associado a um PCS da nova rede corporativa da rede Wi-Fi do projeto e exceções devem ser submetidas a prévia autorização da Agência Estadual de Tecnologia da Informação – ATI.

1.4.8. Os endereços IPs a serem utilizados para identificar os Pontos de Voz Fixos, associados a cada LBL e LME, deverão ser definidos pela ATI.

1.4.8.1. Caso solicitado pela ATI a CONTRATADA deverá fornecer contribuições para elaborar um Plano de Numeração para os Pontos de Voz Fixo.

1.4.8.2. A CONTRATADA deverá prover, implementar e garantir suporte integral ao serviço de gerenciamento de voz convergente, incluindo a operação e administração dos Pontos de Voz Wi-Fi, DECT IP, softphone e voz virtual, bem como o tráfego extrarrede e extrarrede reverso, assegurando plena integração e funcionamento dentro do **ADENDO IX - CENTRO INTEGRADO DE INTELIGÊNCIA E SEGURANÇA CIBERNÉTICA**.

1.4.8.2.1. O serviço deverá contemplar ferramentas de gestão, monitoramento, configuração remota e controle de desempenho, garantindo alta disponibilidade, segurança e conformidade com as exigências operacionais do Centro Integrado.

1.4.9. Permitir a utilização de equipamentos dos Pontos de Voz Wi-Fi, DECT IP, *softphone* e virtual, conforme modelos apresentados e especificado neste Termo de Referência;

1.4.10. A CONTRATADA deverá manter o registro de todas as ligações realizadas, contendo, no mínimo, as seguintes informações: terminal que originou a chamada, data, hora, duração das chamadas e número de destino.

1.4.10.1. Os registros deverão ser mantidos por toda a vigência contratual, incluindo eventuais prorrogações, e por um período adicional de 6 (seis) meses após o encerramento do contrato.

1.4.10.2. A retenção dos registros deverá atender, no mínimo, às exigências do Marco Civil da Internet (Lei nº 12.965/2014), garantindo a integridade e a segurança das informações armazenadas durante o período de guarda.

1.4.11. Disponibilizar um sistema de gerenciamento de falhas para informar ao Serviço CIISC - Centro Integrado de Segurança Cibernética da nova rede corporativa de todos os eventos de ocorrência de falhas, via rede TCP/IP, priorizando os tipos de falhas;

1.4.12. Permitir que todos os terminais de voz (PVFs), previstos neste serviço, possam ser utilizados em conferências providas pelo serviço de Comunicação Unificada da Nova Rede Corporativa;

1.4.13. A taxa de congestionamento interno devido à falha não poderá exceder a 1%;

1.4.14. Tempo máximo para recebimento do canal de voz deverá ser de 3 (três) segundos, contados a partir da discagem do número de destino;

1.4.15. A solução deverá permitir e realizar a configuração de, no mínimo, 10 (dez) classes de serviço distintas para os pontos de voz fixos contratados (PVFs), quando solicitada, viabilizando a atribuição de diferentes níveis de permissões, acessos e funcionalidades de voz.

1.4.15.1. As classes de serviço deverão, no mínimo, permitir o controle de:

- Tipos de chamadas autorizadas (internas, locais, interurbanas, móveis, internacionais).
- Acesso a funcionalidades de voz, como rediscagem, chamada em espera, transferência, conferência e bloqueio de chamadas específicas.
- Priorizações ou restrições baseadas no perfil de uso de cada ramal.

1.4.15.2. A configuração ou alteração das classes de serviço deverá ser realizada pela CONTRATADA, quando solicitado pela CONTRATANTE, sem custos adicionais e com registro detalhado das alterações efetuadas.

1.4.16. A solução deverá permitir a configuração de categorias de uso diferenciadas por período (diurno e noturno) para os PVFs, com opções de habilitação e restrição de facilidades e funcionalidades de voz específicas para cada categoria.

1.4.16.1. As categorias diurna e noturna deverão possibilitar, no mínimo:

- A definição de permissões distintas para tipos de chamadas (ex.: habilitação de chamadas locais durante o período diurno e bloqueio de chamadas interurbanas durante o período noturno);
- A ativação ou restrição de funcionalidades de voz, como conferência e transferência, com base no período;
- A programação de horários específicos para ativação automática de cada categoria.

1.4.16.2. A configuração das categorias deverá ser flexível e customizável para atender às necessidades específicas da CONTRATANTE, sendo realizada pela CONTRATADA, sem custos adicionais.

1.4.17. A solução proposta pela CONTRATADA, assim como todos os aparelhos fornecidos, deverá identificar e exibir, de forma clara e precisa, o número de origem (telefone que realiza a chamada) e o número de destino (telefone que recebe a chamada), utilizando a funcionalidade conhecida como BINA. Essa funcionalidade deverá estar disponível para todas as chamadas externas e internas realizadas entre os ramais do Governo.

1.4.18. Possuir a facilidade de captura de chamadas para ramais de um mesmo grupo ou não, através de comandos via teclas ou outros recursos do próprio PVP;

1.4.19. Permitir a transferência de chamadas entre PVFs;

1.4.20. Fornecer serviço de aguardo, de modo que as chamadas externas encaminhadas para pontos de telefone cujo atendente esteja ausente sejam automaticamente dirigidas aos pontos de voz fixos pré-determinados (pelo próprio usuário);

1.4.21. Fornecer facilidade de siga-me (*follow-me*) para um número interno ou desvio de chamadas para um número externo, sendo programável a partir do Ponto de Voz Fixo de origem ou a partir de qualquer Ponto de Voz Fixo da Rede, controlável através de classe de restrição do usuário e senha;

- 1.4.22. Fornecer a facilidade de conferências por telefone, no mínimo entre 03 (Três) participantes, onde os participantes realizam a conferência a partir dos recursos oferecidos por cada tipo de PVF;
- 1.4.23. Fornecer facilidade de Função chefe-secretária. As chamadas encaminhadas ao chefe são direcionadas para o aparelho telefônico da secretária que controla as ligações;
- 1.4.24. Fornecer o serviço especial com a possibilidade de configuração de determinados PVFs como confidencial, isto é, o número de identificação do PVF não deve aparecer no receptor que está sendo chamado (aparelho-destino);
- 1.4.25. Suportar protocolo de interconexão Q.Sig, SIP Trunking ou outro protocolo que permita a interoperabilidade entre quaisquer fabricantes de servidores de voz, permitindo também a identificação do chamador;
- 1.4.26. Permitir o cadastramento dos nomes dos usuários internos para que possa ser exibido o nome do usuário que está chamando no display dos PVFs com recurso de display ou software;
- 1.4.27. Oferecer ferramentas para monitorar qualidade de serviço das chamadas de VoIP, a qual deverá ser baseada em SNMP/MIB para fácil acesso pelas aplicações de gerenciamento de rede;
- 1.4.28. Prover a facilidade em que os telefones IPs devem poder obter endereços IP e VLAN através de implementações padrões de DHCP;
- 1.4.29. Permitir reinicialização dos telefones IP a partir da interface de administração;
- 1.4.30. Implementar encriptação entre usuários de telefones IP para todas as ligações. O mecanismo de criptografia a ser utilizado, deverá seguir o padrão *Advanced Encryption Standard (AES)* ou tecnologia superior;
- 1.4.31. Cada Ponto de Voz Fixo terá um Número Identificador Multidigital – NIM, compreendidos numa faixa de numeração da Rede de Telefônica Pública Comutada (RTPC) regulamentada pela ANATEL, para fins de registros dos serviços originados a partir do PCS, além de sua identificação interna e externa à NOVA REDE CORPORATIVA;
- 1.4.32. Utilizar o atual plano de numeração dos Pontos de Voz Fixo;
- 1.4.33. Prover as facilidades de discagem direta nos Pontos de Voz conhecida como Discagem Direta a Ramal-DDR, utilizando os NIMs da RTPC;
- 1.4.34. Utilizar os respectivos NIMs de cada PVF para identificar os tráfegos de voz encaminhados para o serviço de Tráfego Extrarrede, permitindo que este tráfego seja tarifado por PVF, para ligações do tipo DDI.
- 1.5. Instalar, operacionalizar e manter todos os Pontos de Voz Fixos (PVFs) nos PCSs, sendo os tipos de Recursos Tecnológicos para prover os serviços de voz (aparelhos ou softwares), listados abaixo:
- 1.5.1. Aparelho de Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL);
- 1.5.2. Aparelho de Voz IP de Mesa WI-FI Tipo I (PVF WI-FI IP MESA TIPO I);
- 1.5.3. Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP MESA TIPO II);
- 1.5.4. Aparelho de Voz DECT IP (PVF-DECT IP);
- 1.5.5. Software de Voz (PVF-Software);
- 1.5.6. Ponto de Voz Virtual (PVF-Virtual);
- 1.5.7. Headset sem fio (PVF-sem fio Fone de Cabeça);
- 1.5.8. Headset (PVF-Fone de Cabeça).
- 1.6. Prover os aparelhos de voz IPs e recursos de software (Software de Voz) de forma garantir a compatibilidade e gerência dos serviços de forma integrada. Será permitido que estes aparelhos e recursos sejam fornecidos por fabricante distinto dos servidores de voz, desde que atendam as seguintes exigências:
- 1.6.1. Que permita o acesso a todas as funcionalidades previstas, e o atendimento dos Níveis Mínimos de Serviço, para o serviço de Pontos de Voz Fixos, definidos neste Termo de Referência;
- 1.6.2. Que o fabricante e modelo seja o mesmo, para toda nova rede corporativa, por tipo de PVF, garantindo a padronização dos serviços oferecidos. Exceções devem ser tratadas para atendimento específico a solicitações de cada Órgão aderente à Rede e aprovação da ATI.
- 1.7. Prover todos os recursos tecnológicos, sejam aparelhos telefônicos ou soluções de softwares, para fornecer o serviço de voz com no mínimo as características e funcionalidades conforme requerido a seguir:
- 1.7.1. Serviço de Ponto de Voz Fixo com aparelho Voz WI-FI IP Móvel (PVF WI-FI IP MÓVEL):**
- 1.7.1.1. O Terminal Telefônico Móvel SIP deve ser compatível e interoperável com a plataforma de voz SIP ofertada;
- 1.7.1.2. Possuir Display gráfico iluminado TFT, colorido, com resolução mínima de 240 × 320 pixels (QVGA) ou superior;

- 1.7.1.3. Possuir indicativo de eventos;
- 1.7.1.4. Ser compatível com os padrões IEEE 802.11 a/b/g/n/ac WLAN
- 1.7.1.5. Permitir uso do Protocolo de Iniciação de Sessão (SIP) sobre a WLAN para manter a comunicação de voz;
- 1.7.1.6. Suportar os protocolos:
  - 1.7.1.6.1. TCP/IP;
  - 1.7.1.6.2. IP addressing: DHCP, fixed;
  - 1.7.1.6.3. Configurable DSCP;
  - 1.7.1.6.4. DNS support (primary/secondary);
  - 1.7.1.6.5. SIP/RTP;
  - 1.7.1.6.6. UDP;
  - 1.7.1.6.7. SRTP/TLS;
  - 1.7.1.6.8. SNMP.
- 1.7.1.7. Suportar os codecs:
  - 1.7.1.7.1. G.711 A-law e G.711  $\mu$ -law;
  - 1.7.1.7.2. G.729, G729A e G729B;
  - 1.7.1.7.3. G.722.
- 1.7.1.8. Suporte de recursos adicionais de VoWLAN:
  - 1.7.1.8.1. Quality of Service (QoS);
  - 1.7.1.8.2. Wireless: Suportar mecanismos de priorização de tráfego e controle de admissão para aplicações de voz sobre Wi-Fi (VoWLAN), tais como WMM (Wi-Fi Multimedia) e mecanismos de Call Admission Control (CAC), incluindo TSPEC-based CAC ou soluções tecnicamente equivalentes.
- 1.7.1.9. Suportar os seguintes métodos de segurança:
  - 1.7.1.9.1. Security standard: 802.11i, 802.11w;
  - 1.7.1.9.2. Suportar o Método de Criptografia AES-CCMP;
  - 1.7.1.9.3. Suportar os seguintes Métodos de Autenticação:
    - 1.7.1.9.3.1. 802.1XWPA-PSK;
    - 1.7.1.9.3.2. WPA3-PSK;
    - 1.7.1.9.3.3. PEAP-MSCHAPv2;
    - 1.7.1.9.3.4. EAP-TLS.
- 1.7.1.10. Suportar Roaming WLAN Avançado:
  - 1.7.1.10.1. 802.11r, 802.11k;
  - 1.7.1.10.2. Opportunistic key caching;
  - 1.7.1.10.3. PMKSA caching;
  - 1.7.1.10.4. Mecanismos de gerenciamento e reaproveitamento de chaves de segurança durante o roaming, que permitam transições rápidas entre pontos de acesso, com manutenção da sessão de voz ativa, tais como IEEE 802.11k/r/v, CCKM ou soluções tecnicamente equivalentes, compatíveis com ambientes corporativos de VoWLAN.
- 1.7.1.11. Possuir tipos de toques, ajustáveis em steps (no mínimo 8) e diferenciáveis em Internos, Externos e Emergência, conforme o SIP Server;
- 1.7.1.12. Possuir idiomas: No mínimo, Português.
- 1.7.1.13. Possuir facilidade "Hands-free" (viva-voz ou alto falante) Full Duplex;
- 1.7.1.14. Possuir bloqueio contra a pressão involuntária de teclas automático e manual;
- 1.7.1.15. Possuir histórico de chamadas (Call history) para as últimas 10 chamadas recebidas, perdidas e realizadas;
- 1.7.1.16. Possuir lista telefônica para 100 (cem) registros;
- 1.7.1.17. Possuir indicador de status da bateria do aparelho;
- 1.7.1.18. Possuir tempo de conversação médio de, no mínimo, 4 (quatro) horas com uma única carga de bateria;
- 1.7.1.19. Possuir tempo em Stand-by médio: 100 horas;
- 1.7.1.20. Possuir alerta com vibração integrado;
- 1.7.1.21. Possuir programação e gerenciamento local ou remoto, podendo ser realizados por:
  - 1.7.1.21.1. Conexão com PC via USB; ou
  - 1.7.1.21.2. Interface web por endereço IP; ou
  - 1.7.1.21.3. Solução de gerenciamento central compatível com a plataforma de comunicação unificada em uso.

- 1.7.1.22. O equipamento deverá atender às especificações de RF compatíveis com os padrões IEEE 802.11 a/b/g/n/ac, conforme especificação técnica do fabricante;
- 1.7.1.23. Banda de frequência: O equipamento deverá operar nas faixas de frequência de 2,4 GHz e 5 GHz, em conformidade com a regulamentação vigente da ANATEL;
- 1.7.1.24. Potência Máxima de Saída: 100 mW / 20 dBm;
- 1.7.1.25. Proteção - IP44, IEC EN 60529;
- 1.7.1.26. Deverão acompanhar todos os cabos, acessórios e fonte de alimentação para a instalação e operação do aparelho;
- 1.7.1.27. Possuir homologação da ANATEL.

**1.7.2. Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI IP Tipo I (PVF WI-FI IP MESA TIPO I):**

- 1.7.2.1. Possuir display de cristal líquido monocromático ou colorido, com resolução mínima de 128 × 64 e 3 linhas para texto, ambos com iluminação de fundo;
- 1.7.2.2. Possuir Led de alerta de chamada;
- 1.7.2.3. Possuir, no mínimo, 4 (quatro) teclas de função programáveis, destinadas à configuração de linhas SIP e/ou funcionalidades do sistema, com indicação visual no display do equipamento;
- 1.7.2.4. Possuir teclas de facilidades fixas, descritas abaixo:
  - 1.7.2.4.1. Hold;
  - 1.7.2.4.2. Transferência;
  - 1.7.2.4.3. Conferência;
  - 1.7.2.4.4. Menu/Configuração;
  - 1.7.2.4.5. Mensagens.
- 1.7.2.5. Possuir teclas de Navegação de 4 direções mais tecla OK;
- 1.7.2.6. Possuir Teclas de função de áudio (mudo/alto-falante/fone de ouvido);
- 1.7.2.7. Possuir tecla de Volume +/-;
- 1.7.2.8. Possuir Tecla de mãos livres (full duplex);
- 1.7.2.9. Possuir Conexão:
  - 1.7.2.9.1. Interface de fone de ouvido (DHSG ou EHS);
  - 1.7.2.9.2. Interface USB;
- 1.7.2.10. Possuir Ergonomia:
  - 1.7.2.10.1. Possibilidade de montagem em parede.
- 1.7.2.11. CODEC de Audio:
  - 1.7.2.11.1. G.711 a e µ-law;
  - 1.7.2.11.2. G.722;
  - 1.7.2.11.3. G.729AB;
  - 1.7.2.11.4. OPUS;
  - 1.7.2.11.5. Cancelamento de eco.
- 1.7.2.12. Possuir recursos de rede, segurança e Qualidade de Serviço (QoS), conforme especificado a seguir:
  - 1.7.2.12.1. Possuir, no mínimo, 2 (duas) interfaces LAN Ethernet 10/100/1000 Mbps, com switch integrado;
  - 1.7.2.12.2. Possuir interface de conectividade sem fio (Wi-Fi) nativa ou por intermédio de dongle USB, compatível com os padrões IEEE 802.11 a/b/g/n/ac WLAN;
  - 1.7.2.12.3. Suportar LLDP-MED;
  - 1.7.2.12.4. Suportar VLAN IEEE 802.1Q;
  - 1.7.2.12.5. Suportar alimentação elétrica adequada ao seu funcionamento contínuo, incluindo:
    - 1.7.2.12.5.1. Alimentação via Power over Ethernet (PoE), quando conectado por interface Ethernet, conforme padrões aplicáveis; e
    - 1.7.2.12.5.2. Fonte de alimentação externa própria, quando utilizado com conectividade sem fio (Wi-Fi).
  - 1.7.2.12.6. Suportar autenticação IEEE 802.1X;
  - 1.7.2.12.7. Suportar SRTP;
  - 1.7.2.12.8. Suportar criptografia TLS (Transport Layer Security) versão 1.2 ou superior, para proteção das comunicações de sinalização;

1.7.2.12.9. Suportar certificados digitais padrão X.509 v3;

1.7.2.13. Possuir homologação da ANATEL.

**1.7.3. Serviço de Ponto de Voz Fixo com Aparelho de Voz IP de Mesa WI-FI Tipo II (PVF WI-FI IP MESA TIPO II):**

1.7.3.1. Possuir display de cristal líquido colorido, resolução mínima de 480 x 272 pixels com 5 linhas para texto e iluminação de fundo;

1.7.3.2. Possuir Led de alerta de chamada multicolorido;

1.7.3.3. Possuir, no mínimo, 6 (seis) teclas de função programáveis, destinadas à configuração de linhas SIP e/ou funcionalidades do sistema, com indicação visual no display do equipamento, bem como sinalização luminosa (LED) nas teclas, com cores, para indicação de estado;

1.7.3.4. Possuir teclas de facilidades fixas, descritas abaixo:

1.7.3.4.1. Hold;

1.7.3.4.2. Transferência;

1.7.3.4.3. Conferência;

1.7.3.4.4. Menu/Configuração;

1.7.3.4.5. Ausente;

1.7.3.4.6. Mensagens.

1.7.3.5. Possui teclas de navegação de 4 direções mais tecla OK;

1.7.3.6. Possuir teclas de função de áudio (mudo/alto-falante/fone de ouvido);

1.7.3.7. Possui tecla de Volume +/-;

1.7.3.8. Possuir tecla de mãos livres (full duplex);

1.7.3.9. Possuir Conexão:

1.7.3.9.1. Interface de fone de ouvido (DHSG ou EHS);

1.7.3.9.2. Interface USB;

1.7.3.9.3. Possibilidade de uso de Key Module.

1.7.3.10. Possuir Ergonomia:

1.7.3.10.1. Possibilidade de montagem em parede.

1.7.3.11. CODEC de Audio:

1.7.3.11.1. G.711 a e  $\mu$ -law;

1.7.3.11.2. G.722;

1.7.3.11.3. G.729AB;

1.7.3.11.4. OPUS;

1.7.3.11.5. Cancelamento de eco.

1.7.3.12. Possuir recursos de rede, segurança e QoS abaixo:

1.7.3.12.1. Possuir, no mínimo, 2 (duas) interfaces LAN 10/100/1000 Mbps, com switch integrado;

1.7.3.12.2. Possuir interface de conectividade sem fio (Wi-Fi) nativa ou por intermédio de dongle USB, compatível com os padrões IEEE 802.11 a/b/g/n/ac WLAN;

1.7.3.12.3. Suportar LLDP-MED;

1.7.3.12.4. Suportar 802.1Q;

1.7.3.12.5. Suportar alimentação elétrica adequada ao seu funcionamento contínuo, incluindo:

1.7.3.12.5.1. Alimentação via Power over Ethernet (PoE), quando conectado por interface Ethernet, conforme padrões aplicáveis; e

1.7.3.12.5.2. Fonte de alimentação externa própria, quando utilizado com conectividade sem fio (Wi-Fi).

1.7.3.12.6. Suportar IEEE 802.1x;

1.7.3.12.7. Suportar SRTP;

1.7.3.12.8. Suportar criptografia TLS (Transport Layer Security) versão 1.2 ou superior, para proteção das comunicações de sinalização;

1.7.3.12.9. Suportar Certificado Digital por X.509 V3;

1.7.3.13. Possuir homologação da ANATEL.

**1.7.4. Serviço de Ponto de Voz Fixo com aparelho de Voz DECT IP (PVF-DECT IP):**

- 1.7.4.1. Os aparelhos devem ser compatíveis com as especificações DECT detalhadas neste Termo de Referência.
- 1.7.4.2. A tecnologia de rádio usada no aparelho deverá estar em conformidade da frequência autorizada para uso em solo brasileiro e deverá possuir Certificações ANATEL;
- 1.7.4.3. O idioma requerido nas interfaces dos aparelhos deverá ser obrigatoriamente em português;
- 1.7.4.4. Deverá possuir display colorido com resolução mínima de 128 x 160 pixels;
- 1.7.4.5. Deverá permitir o usuário escolher toque de chamada para personalizar o toque. O aparelho, deverá possuir ao menos 08 toques internos para tal;
- 1.7.4.6. Deverá possuir a opção de “mute de toque”, com opção de vibração para recebimento de chamadas;
- 1.7.4.7. Possuir agenda para no mínimo 100 números;
- 1.7.4.8. Possuir rediscagem;
- 1.7.4.9. Sinalização visual e acústica;
- 1.7.4.10. Possuir interface de fone de ouvido com plug 3,5mm;
- 1.7.4.11. Suportar temperatura entre +5 °C até +45 °C;
- 1.7.4.12. Deve ser fornecido com carregador de baterias.
- 1.7.4.12.1. O carregamento do aparelho não deverá indisponibilizar o uso durante a carga;
- 1.7.5. Serviço de Ponto de Voz Fixo utilizando Software de Voz (PVF SOFTWARE):**
  - 1.7.5.1. Permitir a realização de identificação de chamadas externas e internas do tipo BINA (B identifica A);
  - 1.7.5.2. Deverá ser solução Cloud based através de suporte WebRTC;
  - 1.7.5.3. Possuir Interface simples e intuitiva;
  - 1.7.5.4. Possuir interfaces do software similares em SmartPhones e PCs (Windows ou Mac);
  - 1.7.5.5. Ser utilizável em ambos os dispositivos simultaneamente (smartphone e PC);
  - 1.7.5.6. Ser compatível, ao menos, com a solução Ofertada;
  - 1.7.5.7. A Solução Ofertada deverá ser capaz de funcionar nos dispositivos móveis baseados em:
    - 1.7.5.7.1. Dispositivos Apple IOS;
    - 1.7.5.7.2. Telefones e/ou Tablets Android;
  - 1.7.5.8. Possuir suporte aos browsers:
    - 1.7.5.8.1. Google Chrome;
    - 1.7.5.8.2. Mozilla Firefox;
    - 1.7.5.8.3. Microsoft Edge;
    - 1.7.5.8.4. Apple Safari.
  - 1.7.5.9. Possuir a funcionalidade de “Lista de Contatos comum” (capacidade de compartilhar e sincronizar listas de contatos entre diferentes dispositivos ou aplicativos) (ex. partilhar contatos do IOS);
  - 1.7.5.10. Enviar comandos DTMF em uma chamada para acesso a sistemas com URA;
  - 1.7.5.11. Possuir as seguintes facilidades:
    - 1.7.5.11.1. Efetuar chamada, atender, recusar e desligar chamadas;
    - 1.7.5.11.2. Reter e recuperar, silenciar/reactivar, transferir chamadas;
    - 1.7.5.11.3. Capturar chamadas de outros ramais pertencentes ao um mesmo grupo comum.
    - 1.7.5.11.4. Enviar chamada para número alternativo;
    - 1.7.5.11.5. Possuir recurso para atendimento de uma segunda chamada;
    - 1.7.5.11.6. Ao Atender a segunda chamada possuir recurso para pendular as chamadas atendidas;
    - 1.7.5.11.7. Participar de conferência;
    - 1.7.5.11.8. Possuir recurso para reencaminhamento de chamadas;
    - 1.7.5.11.9. Possuir recurso de número alternativo (One Number Service);
    - 1.7.5.11.10. Possuir acesso a contatos via MS Office 365, Mobile Contacts no IOS e Android;
    - 1.7.5.11.11. Possuir gerenciamento de Presença;
    - 1.7.5.11.12. Possuir Integração com fone de ouvido USB, bluetooth e P2 (Smartphone e PC);
    - 1.7.5.11.13. Possuir linguagem na língua portuguesa obrigatoriamente em suas interfaces (Smartfone e PC);
    - 1.7.5.11.14. Possuir a facilidade de lista de chamadas:
      - 1.7.5.11.14.1. Não atendidas;
      - 1.7.5.11.14.2. Realizadas com êxito;

- 1.7.5.11.14.3. Recebida e atendida;
- 1.7.5.11.14.4. Recebida e não atendida;
- 1.7.5.11.14.5. Recebida em ocupado.
- 1.7.5.12. Possuir identificação de número e nome dos ramais pertencentes a mesma Rede;
- 1.7.5.13. Possuir identificação de número e nome de linhas externas com cadastro em tabelas do PABX (ex. Lista de discagem);
- 1.7.5.14. Deverá possuir Integração com a ferramenta de comunicação unificada projetada para nova rede;
- 1.7.5.15. Facilidades requeridas quando do uso integrado com a ferramenta ofertada de comunicação unificada do projeto da nova rede corporativa:
  - 1.7.5.15.1. Chamada para ramais e Operadora;
  - 1.7.5.15.2. Envio de DTMF para URAs ou similares;
  - 1.7.5.15.3. Transferência de chamadas;
  - 1.7.5.15.4. Atendimento de segunda chamada;
  - 1.7.5.15.5. Ao Atender a segunda chamada possuir recurso para pendular as entre as chamadas;
  - 1.7.5.15.6. Transformar a chamada pendular em conferência;
  - 1.7.5.15.7. Possuir recurso para atendimento da segunda chamada em outro dispositivo;
- 1.7.5.16. Possibilidade de configuração:
- 1.7.5.17. Definição de número alternativo;
- 1.7.5.18. Definição de desvios;
- 1.7.5.19. Visualização de chamadas em curso nos dispositivos gerenciados pela aplicação (ex. telefone de mesa, número alternativo);
- 1.7.5.20. Possuir homologação da ANATEL

**1.7.6. Serviço de Ponto de Voz Fixo Virtual (PVF-Virtual):**

- 1.7.6.1. Suportar a facilidade de virtualização de NIMs;
- 1.7.6.2. Um conjunto de NIMs pode ser usado por qualquer aparelho telefônico da nova rede corporativa a partir de uma codificação e senha específica;
- 1.7.6.3. Permitir realizar ligações intra e extra-grupo da nova rede corporativa.

**1.7.7. Serviço PVF-Bluetooth Fone de Ouvido):**

- 1.7.7.1. Possuir no mínimo Bluetooth 4.2;
- 1.7.7.2. Possuir opções de uso com arco, do tipo eartip/earhook, on-ear ou over-ear;
- 1.7.7.3. Ser Plug&Play;
- 1.7.7.4. Ser compatível com a solução proposta;
- 1.7.7.5. Possuir tempo de conversação médio de, no mínimo, 6 (seis) horas com uma única carga de bateria.;
- 1.7.7.6. Possuir alcance sem fio mínimo de 20m;
- 1.7.7.7. Possuir faixa de frequência do alto-falante: 20 Hz-14 kHz.
- 1.7.7.8. Possuir homologação da ANATEL.

**1.7.8. Serviço PVF-Fone-de-Cabeça:**

- 1.7.8.1. Possuir fone de ouvido e microfone integrados (headset) com cancelador de ruídos e eco;
- 1.7.8.2. Os Fones de Cabeça deverão ter:
  - 1.7.8.2.1. Tubo de voz removível ou flexível;
  - 1.7.8.2.2. Giro do tubo de voz em 300 graus;
  - 1.7.8.2.3. Ajuste de adaptação ergonômica à cabeça;
  - 1.7.8.2.4. Tiara com tamanho ajustável e revestida em material anti-alérgico;
  - 1.7.8.2.5. Apoio lateral de material atóxico;
  - 1.7.8.2.6. Protetor auricular em material antialérgico e individual;
  - 1.7.8.2.7. Cabo quick disconnect ou solução equivalente que permita desconexão rápida sem desligar a chamada;
  - 1.7.8.2.8. Proteção contra choque acústico;
  - 1.7.8.2.9. Interface adequada ao dispositivo de uso em computadores, devendo possuir conexão USB Plug & Play.

1.8. Fornecer ou disponibilizar aos usuários da Nova Rede Corporativa, ao término da instalação dos serviços no PCS, manual ilustrativo contendo todos os recursos e facilidades disponíveis para cada PVF contratado, utilizando linguagem clara e objetiva com ilustrações e recomendações podendo ser disponibilizado impresso ou na *WEB*.

1.9. Prover ferramentas para Gerenciamento de Bilhetagem e Tarifação (Discagem Direta Internacional – DDI), conforme requisitos e funcionalidades elencadas a seguir:

1.9.1. A CONTRATADA deverá entregar uma solução de bilhetagem para registrar todas as chamadas originadas pelos Pontos de Voz Fixo (PVF), incluindo informações detalhadas, tais como:

1.9.1.1. Número de origem e destino.

1.9.1.2. Data e hora da ligação.

1.9.1.3. Duração da chamada.

1.9.1.4. Tipo de ligação (local, longa distância, móvel, fixo).

1.9.1.5. Identificação do PVF de origem.

1.9.1.6. Esses registros deverão ser disponibilizados mensalmente em formato digital através de uma plataforma *WEB* segura e de fácil acesso, com possibilidade de extração no formato de meio digital como arquivos CSV ou TXT, e deverão estar acessíveis para fins de auditoria, investigações e processos legais, quando necessário.

1.9.2. A solução tecnológica deverá disponibilizar o Gerenciamento de Bilhetagem dos tráfegos de voz fixa e móvel operacionalizados na nova rede corporativa.

1.9.3. Registrar todos os bilhetes de tráfego intrarrede e extrarrede, dos PVFs da Nova Rede Corporativa.

1.9.4. Disponibilizar acesso via *WEB* para consulta a relatórios customizados de ligações efetuadas, possibilitando a visualização dos somatórios de tráfegos por tipo de ligação realizada (local, longa distância, intrarrede, extrarrede, telefonia móvel ou fixa), mês a mês, para cada um dos clientes aderentes, possibilitando desta forma um acompanhamento do serviço contratado.

1.9.5. Disponibilizar facilidades para que os acessos ao sistema sejam hierarquizados de forma que os gestores de cada Órgão CONTRATANTE Aderente, ou outros conjuntos de hierarquias como PVF, PVM, PCS etc. associados possam determinar como visualizar suas informações e garantir que elas somente sejam visualizadas por pessoas devidamente autorizadas.

1.9.6. Possuir a capacidade de armazenamento que disponibilize a consulta dos registros com permanência mínima de 12 (doze) meses. Os dados após 30 (trinta) dias devem ser salvos em *backups* periódicos e disponibilizados à ATI, em arquivo texto (.txt), contendo o detalhamento de todas as ligações e demais serviços de conta conforme modelo elaborado pela FEBRABAN, versão V3R0 ou mais recente, e em pasta segura na *WEB*.

1.9.7. Bilhetar e tarifar (apenas DDI) as ligações realizadas e/ou recebidas por cada ponto de voz fixo, providas por diferentes sites.

1.9.8. Gerar bases de dados contendo informações e dados estatísticos e de tráfegos intra e extrarrede da nova rede corporativa originados e recebidos pelos PVFs, podendo classificar informações por grupos diversos de interesse.

1.9.9. Contabilizar os dados de bilhetagem e tarifação (DDI) para cada categoria de tráfego originada dos pontos de voz fixos.

1.9.10. Separar os custos por CONTRATANTE ADERENTE para consolidação dos relatórios com detalhamento de seus respectivos usuários;

1.9.11. Os registros de bilhetagem deverão ser tratados em conformidade com a Lei Geral de Proteção de Dados (LGPD). A CONTRATADA deverá garantir a confidencialidade, integridade e disponibilidade desses dados, permitindo o acesso apenas a pessoas autorizadas, conforme diretrizes estabelecidas pela CONTRATANTE.

1.10. Instalação de Pontos de Voz Fixa (PVF) por Rede Cabeada ou Infraestrutura Existente

1.10.1. Sob autorização expressa da Agência Estadual de Tecnologia da Informação (ATI), será permitida a instalação de Pontos de Voz Fixa (PVF) utilizando rede cabeada ou infraestrutura física existente, em substituição à rede sem fio, desde que sejam integralmente observados os seguintes requisitos:

1.10.1.1. A CONTRATADA deverá garantir os mesmos parâmetros de qualidade, disponibilidade e gerenciamento (NMS) aplicáveis aos PVFs da solução;

1.10.1.2. A infraestrutura física utilizada — nova ou preexistente — deverá atender às normas e padrões técnicos definidos nos itens 1.2.6 e 1.2.7 (Obrigações aplicáveis ao LOTE 01) do Adendo I – Obrigações da Contratada e Contratante, incluindo cabeamento estruturado, conectores e manutenção preventiva;

1.10.1.3. A responsabilidade integral pelos custos de instalação, manutenção e operação dessa infraestrutura cabeada

ou mista será da CONTRATADA, sem ônus adicional para a CONTRATANTE;  
1.10.1.4. A autorização de uso de infraestrutura cabeada ou existente será concedida caso a ATI avalie como mais adequada à realidade técnica e física do local, garantindo o desempenho e a compatibilidade com o restante da solução contratada.

## 2. Tecnologia DECT IP

- 2.1. A solução ofertada deverá ser apresentada com Antenas e aparelhos IP DECT.
- 2.2. A solução ofertada deverá ser do tipo DECT sobre IP.
- 2.3. Os terminais deverão estar conectados diretamente na Nuvem através das Antenas IP DECT.
- 2.4. A solução deverá ser baseada em SIP (RFC 3261).
- 2.5. A solução deverá permitir a integração com sistemas de telefonia VoIP.
- 2.6. O usuário DECT será um PVF conectado diretamente a NUVEM.
- 2.7. O Idioma requerido para a interface de administração e configuração da solução deverá ser em português.
- 2.8. A tecnologia de rádio usada na solução deverá estar em conformidade da frequência autorizada para uso em solo Brasileiro e deverá possuir Certificações ANATEL.
- 2.9. A solução deve permitir o roaming, fazendo que uma chamada não seja desconectada mesmo quando o usuário sai da área de cobertura de uma antena e entra na área de cobertura de outra antena.
- 2.10. A ligação à infraestrutura de Voz sobre IP deverá ser realizada por meio do protocolo SIP, não sendo exigida a utilização de componentes adicionais.
- 2.10.1. Serão admitidos componentes complementares quando tecnicamente necessários à solução, desde que não comprometam o desempenho, a integração e o atendimento aos níveis mínimos de serviço estabelecidos neste Termo de Referência.
- 2.11. A solução deverá garantir funcionamento dentro do ambiente do PCS no qual o terminal está sendo instalado.
- 2.12. A solução deverá fornecer criptografia segura na comunicação entre o telefone e a base, garantindo a privacidade das conversas. O padrão de criptografia deve utilizar AES com chave de 128 bits ou superior, permitindo futuras atualizações para algoritmos mais avançados, caso necessário.
- 2.13. A solução deverá fornecer autenticação entre a base e o telefone para evitar interferências ou acessos não autorizados.
- 2.14. A solução deverá possuir áudio de alta definição (HD Voice) para melhorar a qualidade das chamadas.
- 2.15. A solução deverá possuir redução de ruídos e eco, especialmente importante em ambientes governamentais ruidosos.
- 2.16. A solução deverá oferecer sistema de gerenciamento centralizado que permita a administração de bases e terminais de maneira remota pelo CIISC, facilitando a configuração e monitoramento de desempenho.
- 2.17. A solução deverá ter capacidade de realizar atualizações de firmware remotamente para garantir a segurança e a funcionalidade.
- 2.18. A solução deverá possuir no mínimo os seguintes elementos:
  - 2.18.1. Software de configuração e gerenciamento;
  - 2.18.2. Telefone DECT;
  - 2.18.3. Antena IP DECT.
- 2.19. A solução ofertada deverá possuir capacidade que permita no mínimo 40% de ligações simultâneas;
- 2.20. A solução deverá permitir escalabilidade;
- 2.21. Especificações mínimas da antena:
  - 2.21.1. Range de temperatura +5 °C até +45 °C;
  - 2.21.2. Suportar Virtual Local Network (VLAN)
  - 2.21.3. Suportar QoS (Quality of Services):
    - 2.21.3.1. Layer 2 (802.1p/q);
    - 2.21.3.2. Layer 3 (ToS, DiffServ).
  - 2.21.4. Suportar DHCP Options.

## 3. Protocolos e padrões que deverão ter suporte

3.1. Os seguintes protocolos e padrões devem ser atendidos pela Plataforma de Voz, de forma a garantir interoperabilidade, confiabilidade e transparência de recursos entre fabricantes diferentes.

3.1.1. RFC 3261: SIP: Session Initiation Protocol;

3.1.2. RFC 2976: SIP INFO Method;

3.1.3. RFC 3262: Reliability of Provisional Responses in SIP;

3.1.4. RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers;

3.1.5. RFC 3264: SDP Offer/Answer Model;

3.1.6. RFC 3265: SIP-specific Event Notification;

3.1.7. RFC 3311: SIP UPDATE Method;

3.1.8. RFC 3323: SIP Privacy Mechanism;

3.1.9. RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks;

3.1.10. RFC 3326: The Reason Header Field for the Session Initiation Protocol (SIP);

3.1.11. RFC 3515: SIP REFER Method;

3.1.12. RFC 3891: The Session Initiation Protocol (SIP) Replaces Header;

3.1.13. RFC 3892: The Session Initiation Protocol (SIP) Referred-By Mechanism;

3.1.14. RFC 3903: PUBLISH method;

3.1.15. RFC 3911: Join header field;

3.1.16. RFC 4028: Session Timers in the Session Initiation Protocol (SIP);

3.1.17. RFC 4092: ANAT in SIP;

3.1.18. RFC 5630: SIP-SIPS;

3.1.19. RFC 5806: Diversion header field;

3.1.20. RFC 5876: Updates to Asserted Identity;

3.1.21. RFC 5923: Connection reuse;

3.1.22. RFC 5954: Essential correction for IPv6 ABNF and URI comparison rules;

3.1.23. RFC 6086: SIP INFO packages;

3.1.24. RFC 2327: Session Description Protocol (SDP);

3.1.25. RFC 4566: Session Description Protocol (SDP) new;

3.1.26. RFC 3266: Support for IPv6;

3.1.27. RFC 3605: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP);

3.1.28. RFC 3890: Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP);

3.1.29. RFC 4091: Alternative Network Address Types (ANAT);

3.1.30. RFC 4567: Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP);

3.1.31. RFC 4568: Session Description Protocol (SDP) Security Descriptions for Media Streams;

3.1.32. RFC 3842: Message waiting indication;

3.1.33. RFC 4235: INVITE-initiated dialog event package;

3.1.34. RFC 4575: Conference event package;

3.1.35. RFC 6035: RTCP summary event package;

3.1.36. RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals;

3.1.37. ECMA CSTA: Services for Computer Supported Telecommunications Applications (CSTA) Phase III;

#### 4. SERVIÇO DE TRÁFEGO TELEFÔNICO EXTRARREDE

4.1. A LICITANTE deve apresentar na Proposta de preços a descrição de como será a prestação dos serviços de Tráfego Extrarrede para a Rede Corporativa do Estado de Pernambuco, os quais serão contratados pelos Órgãos Aderentes através de Contratos de Adesão, atendendo aos princípios gerais e requisitos contidos no Termo de Referência da Nova Rede Corporativa e seus ADENDOS, respeitando os requisitos obrigatórios elencados nos itens a seguir:

4.1.1. Entende-se por Tráfego Extrarrede o recurso que um terminal telefônico tem para acessar as redes telefônicas públicas fixa e/ou móvel de telecomunicações para realizar chamadas, tendo como destino usuários de telefonia pública fixa e móvel, que não fazem parte do conjunto de terminais telefônicos integrantes da Rede Corporativa do Estado de Pernambuco.

4.1.2. Prover os serviços de Tráfego Extrarrede. Todas as chamadas realizadas a partir dos usuários de telefonia fixa, integrantes da Rede Corporativa do Estado de Pernambuco, para outros usuários de telefonia pública fixa e/ou móvel que não sejam do grupo intrarrede da Rede Corporativa do Estado de Pernambuco, são consideradas como Serviço de Tráfego Extrarrede.

4.1.3. Prover o Serviço de Tráfego Extrarrede para Telefonia Fixa e Telefonia Móvel através dos sistemas de conexão, utilizando de interfaces SIP (RFC 3261 da IETF) com as redes telefônicas públicas, fixa e móvel de telecomunicações, nas modalidades e estimativas relacionadas na Tabela de Serviços do Termo de Referência e **ANEXO D – QUANTITATIVO DE TRAFÉGO EXTRARREDE E ESPECIFICAÇÕES TÉCNICAS PARA DIMENSIONAMENTO DE SOLUÇÃO DE VOZ EM CLOUD.**

4.1.4. A CONTRATADA deve prover link para escoamento de todo o tráfego extrarrede demandado, entrante e sainte, para a Rede Pública de Telefonia para Nova Rede Corporativa do Estado de Pernambuco.

4.1.5. Os links para escoamento do tráfego extrarrede devem ser protegidos por uma infraestrutura de alta disponibilidade (HA), de responsabilidade da CONTRATADA e instalada na interligação entre o serviço de tráfego telefônico extrarrede e o Núcleo da rede corporativa de voz do Estado. Esta infraestrutura de alta disponibilidade deve ser composta por equipamentos redundantes, configurados em HA, e rotas de acesso distintas, deverá garantir continuidade automática do serviço em caso de falha de qualquer componente ou rota, mantendo a capacidade integral de escoamento do tráfego extrarrede, conforme especificado no ADENDO XI – INFRAESTRUTURA PARA OS SERVIÇOS EM NUVEM.

4.1.6. O quantitativo de canais disponíveis para o escoamento do tráfego extrarrede deve ser suficiente para atender toda a demanda por este serviço da Rede Corporativa do Estado de Pernambuco, devendo ocorrer a ampliação do número de canais quando sua capacidade atingir no máximo 80% em sua média mensal nos Horários de Maior Movimento (HMM);

4.1.6.1. O **ANEXO D – QUANTITATIVO DE TRAFÉGO EXTRARREDE E ESPECIFICAÇÕES TÉCNICAS PARA DIMENSIONAMENTO DE SOLUÇÃO DE VOZ EM CLOUD**, fornece dados relacionados à quantidade de Pontos de Voz Fixo (PVFs) por município que necessitam ser portados, além de informações sobre o tráfego consumido durante todo o ano de 2024 pelos serviços 0800 Estadual e Solução de Tráfego Extrarrede. Essas informações estão disponibilizadas para subsidiar os LICITANTES na avaliação da capacidade de suas redes, permitindo que atendam adequadamente às especificações técnicas e aos requisitos operacionais estabelecidos no Termo de Referência.

4.1.7. Deve atender à quantidade de canais definidos pelos CONTRATANTES Aderentes para o serviço de Infraestrutura de Voz para Contact Center.

4.1.8. O Serviço de Tráfego Extrarrede deve atender aos Níveis Mínimos de Serviço (NMS), conforme especificado no Termo de Referência da Nova Rede Corporativa e seus Adendos.

4.1.9. Deve manter o atual plano de numeração dos terminais telefônicos em uso pelos Aderentes da Rede Corporativa do Estado de Pernambuco, através de portabilidade. Para os casos de aumento ou atualizações necessárias durante a vigência da prestação dos serviços, a CONTRATADA deverá fornecer uma nova faixa de numeração, onde estes números devem ser sequenciados, preferencialmente, com sequências exclusivas para os usuários da Rede Corporativa do Estado de Pernambuco, respeitando legislação vigente;

4.1.9.1. Eventuais situações em que a CONTRATADA não consiga realizar a portabilidade por motivos técnicos deverão ser formalmente reportadas à ATI-PE, acompanhadas de todas as evidências e relatórios técnicos que venham a ser solicitados. A ATI-PE analisará o caso e, a seu critério, poderá aprovar ou não a não execução da portabilidade.

4.1.10. Encaminhar para os usuários dos serviços de telefonia pública, fixa ou móvel, o número completo de identificação (BINA) do PVF originador da chamada, salvo por solicitação expressa da CONTRATANTE;

4.1.11. Realizar o bloqueio do recebimento de chamadas à cobrar, o bloqueio deve ser feito na central pública. Este bloqueio deve estar disponível independentemente do serviço de voz de origem da chamada;

4.1.12. Bilhetar todo o tráfego extrarrede.

4.1.12.1. Todos os serviços passíveis de bilhetagem e tarifação (ligações do tipo DDI) conforme descrito neste Adendo, deverão ser registrados (bilhetados) para fins de comprovação mensal.

4.1.12.2. O modelo de tarifação do tráfego extrarrede deve ser integralmente associado ao custo dos PVFs contratados, sem cobrança adicional por ligações efetuadas. Todas as métricas de consumo deverão ser registradas em sistemas de bilhetagem robustos, acessíveis à CONTRATANTE e às CONTRATANTES ADERENTES, com relatórios detalhados por PCS, gerados mensalmente e disponibilizados automaticamente.

4.1.13. Os serviços de Tráfegos Extrarrede, para atender aos PVFs, deve compreender toda a integração do acesso da rede pública com os requisitos operacionais e facilidades provenientes dos servidores de voz utilizados nas conexões de forma a garantir o acesso aos PVFs da CONTRATANTE, pela sociedade de forma direta, através da facilidade de Discagem Direta a um PVF, conhecida como DDR-Discagem Direta a Ramal.

4.1.14. Disponibilizar na web (internet) relatórios de desempenho do serviço de Tráfego Extrarrede, apresentando o resultado de indicadores de forma a permitir que sejam adotadas providências em tempo hábil para manter a qualidade do serviço.

4.1.15. Participar, quando solicitado pela CONTRATANTE Principal ou pela CONTRATANTE Aderente Técnica, de reuniões de acompanhamento dos indicadores de qualidade dos serviços a Rede Corporativa do Estado de Pernambuco.

4.1.16. Garantir que chamadas originadas pela sociedade (pessoa física ou jurídica) destinadas a um PVF, através da rede pública de telefonia, a partir de qualquer município do Estado de Pernambuco, incluindo Fernando de Noronha, sejam tarifadas com custo de ligação local quando originadas e recebidas nestas respectivas localidades.

4.1.17. O serviço de tráfego extrarrede deverá ser fornecido para os tipos de ligações previstas pela ANATEL, quais sejam:

4.1.17.1. Local fixo-fixo para todas as localidades;

4.1.17.2. Local fixo-móvel, para todas as localidades;

4.1.17.3. Longa Distância Fixo-Fixo (DDD);

4.1.17.4. Longa Distância Fixo-Móvel (DDD); e

4.1.17.5. Longa Distância Internacional – DDI para os sistemas de conexão com as redes telefônicas públicas fixa e móvel de telecomunicações.

## **4.2. Portabilidade e Migração de Números Telefônicos**

4.2.1. A CONTRATADA deverá realizar, sem custo adicional para a CONTRATANTE, a portabilidade numérica de todos os números telefônicos fixos atualmente em uso pela Rede Corporativa do Estado de Pernambuco, conforme regulamentação vigente da ANATEL, garantindo a preservação integral do plano de numeração atual.

4.2.2. A portabilidade numérica deverá ser realizada em janelas programadas e previamente acordadas com a CONTRATANTE, garantindo a continuidade dos serviços em operação e minimizando impactos para os usuários.

4.2.3. A CONTRATADA deverá fornecer à CONTRATANTE um plano detalhado de migração, incluindo:

4.2.3.1. Cronograma de execução para a portabilidade.

4.2.3.2. Procedimentos de contingência para minimizar impactos em caso de falhas.

4.2.3.3. Identificação de pontos de contato técnicos e operacionais para suporte durante a portabilidade.

4.2.4. A CONTRATADA deverá garantir que a operação dos números portados seja realizada com qualidade, sem degradação de serviços, e totalmente integrada à nova infraestrutura fornecida.

4.2.5. Todos os números portados deverão estar configurados para operação plena, incluindo funcionalidades como Discagem Direta a Ramal (DDR), identificação de chamadas (BINA), e atendimento aos requisitos de segurança e gerenciamento previstos neste Termo de Referência.

4.2.6. Em casos de necessidade de alteração ou expansão do plano de numeração durante a vigência do contrato, a CONTRATADA deverá prover números adicionais, devidamente integrados à Rede Corporativa e sequenciados preferencialmente em blocos contínuos, sendo necessário aprovação prévia da CONTRATANTE;

4.2.7. A CONTRATADA será responsável por todas as atividades técnicas, administrativas e operacionais necessárias à portabilidade, incluindo contato com os operadores de origem, a CONTRATANTE Principal e as CONTRATANTES Aderentes, sempre que necessário, e o cumprimento de prazos regulatórios, devendo garantir total conformidade com a Resolução ANATEL nº 460/2007.

4.2.8. A CONTRATADA deverá disponibilizar suporte técnico dedicado durante todo o processo de portabilidade e nos 15 (quinze) dias subsequentes à sua conclusão.

4.2.9. A CONTRATADA deverá apresentar, no momento da homologação do serviço de tráfego extrarrede, o Termo de Direito, Delegação, Autorização, Concessão ou Outorga de operação expedido pela Agência Nacional de Telecomunicações (ANATEL) para a prestação do Serviço Telefônico Fixo Comutado (STFC), com cobertura e autorização para operação no estado de Pernambuco, conforme estabelecido no Regulamento do Serviço Telefônico Fixo Comutado (Resolução Anatel nº 426, de 9 de dezembro de 2005). O referido documento poderá ser apresentado em nome da

própria CONTRATADA, de uma das empresas integrantes do consórcio ou de uma subcontratada formalmente vinculada ao consórcio para a execução do serviço.

4.2.10. Para portabilidade de Tridígitos Telefônicos a CONTRATADA deverá garantir a portabilidade dos números de telefone de três dígitos atualmente utilizados pela administração pública, conforme regulamentação vigente da Agência Nacional de Telecomunicações (ANATEL).

4.2.10.1. A solução fornecida deve permitir a continuidade do uso dos tridígitos telefônicos já estabelecidos, sem interrupção dos serviços;

4.2.10.2. Em caso de migração para outra operadora ou infraestrutura, a contratada deve garantir a manutenção dos números curtos sem impacto para os usuários;

4.2.10.3. A tecnologia adotada deve assegurar a plena funcionalidade dos números portados em todas as redes de telefonia fixa e móvel;

4.2.10.4. A CONTRATADA deve oferecer suporte técnico contínuo para a manutenção da portabilidade, garantindo atendimento a eventuais falhas ou inconsistências;

4.2.10.5. A portabilidade dos tridígitos deve atender às normas da ANATEL e demais órgãos reguladores pertinentes.

## **5. SERVIÇO TRÁFEGO TELEFÔNICO EXTRARREDE REVERSO, DO TIPO DISCAGEM DIRETA GRATUITA (DDG)**

5.1. Serviço de telefonia, adquirido opcionalmente por parte da Contratante Aderente, utilizando o prefixo 0800, no sistema de tarifação reversa, para possibilitar receber ligações telefônicas locais e de todas as cidades e municípios da República Federativa do Brasil, destinadas aos órgãos do Governo do Estado de Pernambuco e Aderentes do Contrato. Esta modalidade de tráfego deverá apresentar as facilidades aos Órgãos Contratantes Aderentes abaixo descritas:

5.1.1. Permitir restringir as áreas das quais não deseja receber chamadas, devendo os usuários originadores dessas ligações receberem mensagens gravadas com as informações pertinentes.

5.1.2. Delimitar as Áreas, permitindo restringir o acesso de chamadas originadas em áreas geográficas que não são de seu interesse;

5.1.3. Permitir o bloqueio dos acessos por chamadas originadas em terminais móveis (celular).

5.1.4. Permitir a restrição de chamadas originadas por telefone público.

5.1.5. Permitir o agendamento por horários, data, dia da semana ou origem, neste caso possibilitando definir o local de atendimento das chamadas em função da hora, data, dia da semana ou origem da ligação.

5.1.6. Possibilitar a distribuição de chamadas (cíclica, sequencial ou percentual) das chamadas entre os diversos pontos de atendimento do órgão aderente, de acordo com sua especificação.

5.1.7. Permitir o reencaminhamento/direcionamento de chamadas nos casos de congestionamento, linha ocupada e na situação de não responde, para outro ponto de atendimento.

5.1.8. Disponibilizar na web (internet) relatórios de desempenho do serviço de 0800, apresentando o resultado de indicadores de forma a permitir que sejam adotadas providências em tempo hábil para manter a qualidade do serviço;

5.1.9. Manter os números 0800 atualmente utilizados pelos Contratantes Aderentes segundo a resolução ANATEL 460 de 19/03/2007 (Regulamento Geral de Portabilidade). A migração do número (portabilidade) não deverá acarretar ônus para a CONTRATANTE.

5.1.10. Notificar formalmente via os diversos meios de comunicação, mediante acordo prévio com o Contratante Aderente, sobre a necessidade de ampliação da capacidade de atendimento do 0800, caso os Níveis Mínimos de Serviço contidos no ADENDO II deste Termo de Referência não estejam dentro dos padrões especificados para a central de atendimento.

5.2. Serviço de tráfego extrarrede: O serviço de tráfego extrarrede deverá ser fornecido de acordo com os tipos de ligações previstas pela ANATEL, quais sejam:

5.2.1. Serviço Fixo Inter Estadual;

5.2.2. Serviço Fixo Intra Estadual;

5.2.3. Serviço Fixo Local;

5.2.4. Serviço Móvel Intra Estadual;

5.2.5. Serviço Móvel Local;

5.2.6. Serviço Móvel VC2;

5.2.7. Serviço Móvel VC3; e

5.2.8. Serviço Longa Inter Regional Fixo.

## 6. SERVIÇO ADICIONAL DE ACESSO SIP (SIP TRUNK)

6.1. A CONTRATADA deverá instalar, quando contratado pelas CONTRATANTES ADERENTES, links individuais de acesso SIP, conforme as especificações definidas neste Termo de Referência, com preços específicos definidos na tabela de preços.

6.1.1. A solução deverá ser baseada no protocolo SIP (RFC 3261 da IETF), e cada link individual de acesso SIP fornecido deverá suportar, no mínimo, 30 (trinta) conexões simultâneas para tráfego extrarrede.

6.1.2. A solução deverá permitir a interligação/ integração com equipamentos do CONTRATANTE ADERENTE por meio de entroncamento SIP TRUNK Padrão, com troca de sinalização SIP.

6.1.3. Os links individuais de acesso SIP devem possuir capacidade de expansão modular, permitindo que o número de conexões simultâneas seja ampliado em múltiplos de 30 (trinta), com limite de banda contratada ajustável máximo de até 10 Mbps, sem custos adicionais para a CONTRATANTE.

6.1.3.1. A ampliação da capacidade, seja em número de conexões ou largura de banda, deverá ser realizada em até 15 (quinze) dias corridos após solicitação formal pela CONTRATANTE, sem interrupção dos serviços já contratados.

6.1.4. CONTRATADA deverá garantir que cada link de acesso SIP possua largura de banda suficiente para suportar o volume de tráfego contratado, mantendo a qualidade do serviço (QoS) exigida e o desempenho, mesmo em condições de alta demanda.

6.1.5. Cada link de acesso SIP deverá ser configurado para atender aos padrões de segurança especificados neste Termo de Referência, incluindo suporte a criptografia (TLS e SRTP) e proteção contra ataques cibernéticos, como DoS e fraude de chamadas.

6.1.6. A CONTRATADA deverá realizar testes de ativação para cada link instalado, garantindo conformidade com as especificações técnicas e o desempenho exigido. Os relatórios dos testes deverão ser apresentados à CONTRATANTE para validação.

6.1.7. Cada link individual deverá ser integrado ao sistema de monitoramento e gerenciamento da Nova Rede Corporativa, conforme definido pela CONTRATANTE.

6.1.8. A CONTRATADA será responsável pela manutenção preventiva e corretiva dos links de acesso SIP, garantindo a continuidade operacional e atendendo a chamados técnicos em conformidade com os prazos estabelecidos nos Níveis Mínimos de Serviço (NMS).

6.1.9. Os links devem suportar chamadas simultâneas utilizando codecs padrão G.711 a-law e u-law, G.729 e Opus, garantindo interoperabilidade com sistemas existentes e qualidade de áudio. A CONTRATANTE priorizará, sempre que viável tecnicamente, o uso dos codecs G.729 e Opus, devido à maior eficiência no uso da banda, permitindo maior número de chamadas simultâneas em comparação ao codec G.711.

6.1.10. A CONTRATADA deverá fornecer relatórios mensais contendo dados de utilização, disponibilidade e desempenho dos links individuais instalados, detalhando eventuais falhas ou interrupções.

### 6.1.11. Configuração e Operação do Tronco SIP com Faixa de Numeração

#### 6.1.11.1. Suporte à Faixa de Numeração:

6.1.11.1.1. O tronco SIP deverá suportar a alocação e configuração de faixas de numeração fornecidas pela CONTRATANTE, de acordo com os padrões regulamentados pela ANATEL e pela UIT-T.

6.1.11.1.2. A CONTRATADA deverá garantir que a faixa de numeração alocada seja configurada de forma a permitir chamadas originadas e recebidas sem restrições técnicas ou administrativas, salvo restrições regulamentares impostas pela ANATEL.

#### 6.1.11.2. Requisitos de Configuração Técnica:

6.1.11.2.1. Suporte à autenticação por credenciais SIP para segurança do tronco.

6.1.11.2.2. Configuração para permitir redundância e alta disponibilidade, com fallback para rotas alternativas em caso de falha de conexão primária.

6.1.11.2.3. Capacidade de registrar múltiplos números ou faixas de numeração em um único tronco.

6.1.11.2.4. Permitir a programação de modo de operação de entrada, saída ou bidirecional, por software.

6.1.11.2.5. Suporte a codecs padrão (G.711, G.729 e Opus), priorizando codecs mais eficientes conforme definido no item 6.1.9.

#### 6.1.11.3. Compatibilidade com Requisitos de Rede:

6.1.11.3.1. O tronco SIP deverá ser configurado para funcionar em redes protegidas por NAT (Network Address Translation) e firewalls, com suporte aos protocolos STUN/TURN e ICE, quando necessário.

6.1.11.3.2. Deverá ter garantia de interoperabilidade com dispositivos e sistemas VoIP que utilizem os protocolos padrão SIP RFC 3261.

6.1.11.3.3. Deverá priorizar pacotes de voz (ToS/DSCP) na rede de transporte, a fim de garantir baixa latência e jitter, além de evitar perda de pacotes atendendo aos Níveis Mínimos de Serviço e Requisitos de Qualidade de Serviço (QoS) estabelecidos neste Termo de Referência.

#### 6.1.11.4. Formato de Números no Tronco SIP

6.1.11.4.1. Todos os números de telefone configurados e utilizados no tronco SIP, tanto para chamadas originadas quanto recebidas, deverão obedecer ao padrão internacional E.164, conforme definido pela UIT-T.

6.1.11.4.2. O formato de números deverá incluir o código do país (por exemplo, +55 para o Brasil), seguido pelo código de área e o número local, sem caracteres adicionais como parênteses, traços ou espaços.

6.1.11.4.3. A CONTRATADA deverá garantir que seu sistema seja capaz de realizar conversões de formato de numeração (Dial Plan) automaticamente, para adequar-se às exigências de sistemas legados ou das operadoras envolvidas.

6.1.11.4.4. O tronco SIP deverá validar números de entrada e rejeitar aqueles que não estejam em conformidade com o padrão E.164, retornando a mensagem de erro SIP adequada ao emissor.

6.1.11.4.5. A CONTRATADA deve configurar o tronco SIP para tratar corretamente números portados, garantindo interoperabilidade com bases de dados de consulta (consulta prévia ou dip-charging).

### 7. Da Segurança

7.1. A CONTRATADA será responsável por implementar políticas de segurança robustas para proteger a comunicação SIP contra acessos não autorizados, interceptações e ataques cibernéticos, incluindo:

7.1.1. Criptografia de sinalização e mídia utilizando TLS (Transport Layer Security) versão 1.2 ou superior e SRTP (Secure Real-time Transport Protocol);

7.1.2. Autenticação segura para todos os terminais SIP conectados à solução.

7.2. A infraestrutura deverá ser protegida contra ataques de negação de serviço (DoS/DDoS), spoofing, manipulação de headers SIP e outras vulnerabilidades conhecidas.

7.3. Atender todos os requisitos de segurança para conexões do tipo SIP Padrão (RFC 3261).

7.4. A CONTRATADA deverá implementar políticas de segurança robustas, incluindo a configuração de firewalls SIP em sua infraestrutura interna. Esses firewalls devem proteger o tráfego SIP contra ataques como negação de serviço (DoS/DDoS), spoofing e manipulação de headers SIP.

7.4.1. A gestão e manutenção e atualização desses firewalls serão de total responsabilidade da CONTRATADA, devendo garantir proteção eficaz sem acesso direto aos dispositivos pela CONTRATANTE;

7.4.2. As políticas de segurança aplicadas deverão ser documentadas e submetidas à CONTRATANTE, incluindo descrição das medidas de mitigação e os procedimentos de resposta a incidentes.

7.5. A CONTRATADA deverá realizar auditorias regulares de segurança e corrigir eventuais vulnerabilidades identificadas.

7.6. Todas as configurações e logs deverão ser armazenados em sistemas seguros, garantindo rastreabilidade e conformidade com as políticas de segurança da informação do projeto durante todo o período do contrato.

7.7. A CONTRATADA deverá se submeter às políticas de segurança vigente pelo Poder Executivo Estadual.

### 8. Do Gerenciamento e Monitoramento

8.1. A CONTRATADA deverá assegurar que os equipamentos fornecidos estejam configurados, habilitados e plenamente operacionais para atender às solicitações da CONTRATANTE. Os equipamentos deverão realizar o monitoramento e gerenciamento por meio de comunidades SNMP v3 configuradas especificamente para a CONTRATANTE, quando solicitado.

8.1.1. Toda solução fornecida para prestação do serviço deverá ser integrada ao sistema de monitoramento central da Nova Rede Corporativa, conforme estabelecido no **ADENDO IX – CENTRO INTEGRADO DE INTELIGÊNCIA E**

**SEGURANÇA CIBERNÉTICA.** Além disso, a CONTRATADA deverá disponibilizar relatórios regulares de desempenho e falhas, acessíveis à CONTRATANTE, para garantir transparência e acompanhamento contínuo da operação.

8.1.2. As configurações SNMP deverão incluir autenticação e criptografia, seguindo as melhores práticas de segurança do protocolo SNMP v3, protegendo os dados gerados durante o monitoramento.

8.2. A CONTRATADA deverá fornecer à CONTRATANTE, quando solicitada, as seguintes configurações e acessos:

8.2.1. Senha de leitura (read-only) para todos os equipamentos fornecidos;

8.2.2. Informações detalhadas para configuração de traps SNMP v3, incluindo endereços IP, portas de comunicação e detalhes técnicos específicos;

8.3. Logs de eventos, alertas e estatísticas relevantes para a operação, sempre que solicitado pela CONTRATANTE, com retenção para todo o período contratual.

8.4. Fornecer Documentação técnica detalhada contendo as informações necessárias para integração e monitoramento dos equipamentos, incluindo descrições de MIBs (Management Information Base) e configurações de traps, quando solicitado.

## 9. Da Proteção de Dados e Privacidade

9.1. A CONTRATADA deverá assegurar que todas as chamadas e registros de tráfego sejam tratados em conformidade com a Lei Geral de Proteção de Dados (LGPD).

9.2. Os dados de chamadas devem ser armazenados em ambiente seguro e acessíveis apenas por pessoal autorizado, conforme normas de segurança da informação.

## ADENDO XIV – SERVIÇO DE INFRAESTRUTURA DE TECNOLOGIA PARA CONTACT CENTER

### 1. REQUISITOS GERAIS

#### 1.1. Características Gerais

1.1.1. A Solução deverá ser totalmente integrada e permitir implementar o atendimento, através de quaisquer meios: voz, vídeo, chat, e-mail, mensagens instantâneas, WhatsApp, SMS, redes sociais, atendimento automatizado (chatbots, atendimento na URA e inclusive Inteligência Artificial (IA) Generativa) e atendentes humanos, conforme todas as características descritas nestas especificações.

1.1.2. A Solução deverá buscar, de acordo com regras parametrizadas, o melhor atendente para realizar o melhor atendimento para o cliente de acordo com o contexto, categoria e o momento da chamada, seguindo as regras de negócios.

1.1.3. A Solução deverá possuir desempenho de produtos, componentes e demais tecnologias suficientes para atendimento inicial ou futuro de todas as necessidades descritas neste documento. A solução deverá ser desenvolvida e concebida para funcionamento em nuvem não sendo aceita soluções ditas como “on-premise”, cuja implementação é dedicada ao cliente, porém em um ambiente virtualizado apenas hospedado em nuvem pública ou acessível via internet.

1.1.4. A Solução deverá ter o tempo sincronizado com a Hora Legal Brasileira de acordo com os diferentes fusos-horários presentes no Brasil.

1.1.5. Todos os usuários da solução tais como: atendentes, supervisores, suporte, BackOffice, administradores, gestores etc., deverão ter associados a solução perfis específicos de acordo com cada atribuição, sendo possível parametrizar acessos e funcionalidades conforme função.

1.1.6. A Solução deverá possuir base unificada de todas as interações dos clientes, deverá ser possível exportá-las, utilizando bancos de dados de mercado, seja por acesso via ferramenta da solução ou mesmo acesso direto disponibilizado por API para consumo.

1.1.7. A Solução CONTRATADA deverá suportar todos os entroncamentos de voz advindos de empresas de telecomunicações ou outras centrais de atendimento (Contact Center) diretamente em pontos de Voz no Brasil, geograficamente separados e em datacenters Tier 3 ou superior.

1.1.8. A CONTRATADA deverá prover toda a estrutura de segurança necessária ao tráfego de voz e vídeo (SBC - Session Border Controller e afins) com essas entidades, conforme especificações descritas neste documento.

1.1.9. A CONTRATADA deverá manter a compatibilidade da SOLUÇÃO com as versões das soluções dos serviços de troca de mensagens deste Adendo, bem como com as respectivas plataformas.

1.1.10. A funcionalidade para integração com soluções de troca de mensagens deverá estar disponível dentre os produtos licenciados para ativação quando necessário.

1.1.11. A CONTRATADA deverá suportar prover a infraestrutura para fornecer os seguintes serviços de voz: Ligações/Chamadas Ativas Manualmente e por meio de Discador Automático; Atendimento Eletrônico e Roteamento inteligente para Chamadas Receptivas e prover as gravações de todas as chamadas de forma integrada ao orquestrador Omnichannel.

1.1.12. A solução deverá prover comunicação e interação com usuários por meio de Softphone WebRTC (Web Real-Time Communications) integrado na solução.

1.1.13. A solução deverá possibilitar administração e gerenciamento de forma centralizada, bem como a geração de relatórios personalizados.

1.1.14. A solução deverá garantir a escalabilidade, permitindo futuras expansões, preservando-a, inclusive, para o caso de criação de novas unidades/sites de atendimento.

1.1.15. A solução deverá ter funcionalidades de ASR (Automatic Speech Recognition) e TTS (Text to Speech) e prover capacidades cognitivas de reconhecimento de contexto de conversa (Inteligência Artificial (IA) Generativa).

1.1.16. A solução deverá comportar a criação de multitenancy 100% apartados.

1.1.17. A CONTRATADA deverá prestar diretamente os serviços ou atuar como integrador (Cloud Broker) entre a CONTRATANTE e o Provedor de serviços de computação em nuvem (Cloud Provider), em conformidade com as características básicas e definições dispostas neste Termo de Referência.

1.1.17.1. A CONTRATADA deverá ficar responsável por qualquer ônus que seja necessário para operacionalizar a solução;

1.1.18. A CONTRATADA deverá oferecer console de gestão amigável de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Cloud Computing. Esse console deve englobar as exigências listadas abaixo:

1.1.18.1. Permitir o agendamento e a realização de backups de dados (incluindo as gravações das interações);

1.1.18.2. Permitir o gerenciamento dos recursos contratados;

1.1.18.3. Prover o monitoramento do ambiente de Cloud (serviços e recursos), de forma automatizada dando cobertura as aplicações, em tempo real (24x7x365), visando detectar problemas.

1.1.19. A CONTRATADA deve assegurar a proibição do uso dos dados que não seja para o propósito para o qual foi contratado.

1.1.20. A CONTRATADA deve assegurar a proteção dos dados, independente se o provedor esteja local no próprio país ou fora do país de origem do CONTRATANTE, devendo informar a localização das informações.

1.1.20.1. Segurança e Criptografia: será aplicado aos dados do CONTRATANTE sob custódia pelo provedor do serviço em nuvem;

1.1.20.2. Protocolos de Segurança: Os protocolos de segurança implementados pelo provedor devem impedir invasões e tentativas de acesso aos dados do CONTRATANTE e do próprio provedor, por pessoas não autorizadas;

1.1.20.3. Descarte de mídias ou equipamentos ou informações: O provedor de serviços deve garantir um processo de reutilização e alienação segura de equipamentos (conforme ISO 27001:2022);

1.1.20.4. Compartilhamento dos dados: o provedor deve garantir que os dados estão seguros e que o acesso à rede dos dados está conforme os controles do item A.11.4 da norma ISO 27001:2022.

1.1.21. Notificação de incidentes de segurança: O CONTRATANTE deve ter acesso aos relatórios e ser informado de eventuais incidentes de segurança, seguindo os padrões da norma ISO 27001:2022.

1.1.22. A CONTRATADA deverá implementar e disponibilizar em sua plataforma, de forma comprovada e auditável, os seguintes recursos e funcionalidades:

1.1.22.1. Mecanismos de prevenção e detecção de intrusão;

1.1.22.2. Medidas de prevenção de vazamento de informações;

1.1.22.3. Realização periódica de testes e varreduras para detecção de vulnerabilidades, com geração de relatórios acessíveis ao CONTRATANTE;

1.1.22.4. Proteção contra softwares maliciosos;

1.1.22.5. Ferramentas de rastreabilidade para eventos de segurança;

1.1.22.6. Controles robustos de acesso e segmentação da rede de computadores;

1.1.22.7. Mecanismos de manutenção de cópias de segurança de dados, informações e metadados;

1.1.22.8. Sistema de aviso imediato para incidentes de segurança da informação.

1.1.23. Repasse de Conhecimento

1.1.23.1. A CONTRATADA deverá realizar a operação assistida para os serviços de Contact Center, para cada CONTRATANTE Aderente que fizer a sua primeira contratação.

1.1.23.2. A operação assistida deve contemplar:

1.1.23.2.1 O repasse de conhecimento de todas as funcionalidades, configurações e operação dos sistemas, tanto para o perfil de atendente quanto para o de supervisor;

1.1.23.2.2 A customização de relatórios que atendam as demandas da CONTRATANTE Aderente;

1.1.23.2.3 A criação de mensagens gravadas em áudio ou texto para os recursos contratados que possuam funcionalidades associadas a tais mensagens;

1.1.23.3 A CONTRATADA deve disponibilizar profissional(ais) capacitado(s) para atender a todos requisitos da operação assistida durante um período mínimo de 10 (dez) dias úteis, salvo se expressamente registrado pelo CONTRATANTE Aderente, de que todos os requisitos foram atendidos antes do prazo mínimo.

1.1.23.4 Tais profissionais devem realizar o repasse de conhecimento no ambiente da CONTRATANTE Aderente;

1.1.23.4 A CONTRATANTE deverá fornecer guias rápidos para orientação na utilização dos recursos do serviço de Contact Center, podendo tais guias serem fornecidos de forma impressa ou digital, inclusive em vídeo.

1.1.23.5 Toda a operação assistida como os materiais fornecidos devem ser ofertados em língua portuguesa do Brasil.

1.1.23.6 Ao final da operação assistida a CONTRATANTE Aderente deve emitir um parecer reconhecendo que o repasse de conhecimento foi concluído e atendeu às exigências definidas.

1.1.24. Todos os requisitos necessários para a prestação de serviços deste Adendo XIV, que envolvam o uso de soluções em nuvem ou datacenters, estão descritas no **Adendo XI – Infraestrutura para os Serviços em Nuvem**. A CONTRATADA é obrigada a atender integralmente às exigências estabelecidas naquele documento, garantindo a conformidade com as melhores práticas de qualidade, segurança da informação, proteção de dados e continuidade de negócios.

## 1.2. Alta disponibilidade

1.2.1. A solução deverá estar disponível para funcionamento ininterrupto (24x7x365);

1.2.2. A solução deve prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos estabelecidos em função do orçamento disponível;

1.2.3. A Solução deverá garantir disponibilidade mensal de, no mínimo, 99.99%, incluindo as paralizações programadas e janelas operacionais.

1.2.4. O BOT da solução contratada deverá ter capacidade para atender no mínimo 100 usuários por segundo.

1.2.5. A Solução deverá funcionar em alta disponibilidade, com elementos redundantes em diferentes zonas de disponibilidade e infraestrutura de rede em contingência sem a necessidade de contratação de serviços e/ou custos adicionais para CONTRATANTE.

### 1.3. Protocolos

1.3.1. Solução deverá suportar, no mínimo, os seguintes protocolos:

1.3.1.1. Sessão e mídia: SIP Padrão (RFC 3261), SIP TRUNK Padrão, RTP, RTCP, SDP e WebRTC.

1.3.2. Acesso seguro via Internet para as integrações entre os componentes da SOLUÇÃO na nuvem e os serviços expostos pela CONTRATANTE na internet/intranet.

1.3.3. Deve suportar comunicação com storage e aplicações por: HTTPs, SFTP ou SOAP.

1.3.4. Transações com sistemas via: SOAP, REST (gerenciado ou não por solução de API Manager), MQ ou Stream.

1.3.5. As APIs devem possuir compatibilidade com formatos padrão de dados, como JSON e XML, e suporte à compressão de dados para melhorar a eficiência das comunicações, devendo ser documentadas e compatíveis com padrões abertos de integração (como REST ou SOAP), de modo a assegurar interoperabilidade e plena validação pela CONTRATANTE.

1.3.6. Gestão de grupos e usuários: LDAP, MS-Active directory.

1.3.7. Autenticação via protocolo OpenID Connect para integração com soluções de SSO padronizadas.

1.3.8. Todos os protocolos e integrações utilizados na solução deverão adotar mecanismos de autenticação segura, encriptação de dados em trânsito e geração de logs de auditoria, de modo a garantir a rastreabilidade e a integridade das comunicações.

1.3.8.1. Esses mecanismos deverão ser passíveis de verificação técnica pela CONTRATANTE durante a fase de homologação e operação dos serviços.

1.3.8.2. Durante a fase de homologação técnica, deverá ser verificado o desempenho das integrações e o tempo médio de resposta das APIs, de modo a comprovar a estabilidade da solução e a integridade das transações durante o processamento simultâneo de requisições.

### 1.4. Facilidades Básicas

1.4.1. Todas as interfaces de usuários deverão ser do tipo GUI (Graphical User Interface), interativas, simples de usar, de maneira que o usuário não necessite de conhecimentos técnicos de TI para sua operação;

1.4.2. As interfaces da solução deverão ser unificadas, ou seja, todas as funcionalidades solicitadas deverão ser apresentadas em interface única da solução, para cada tipo de usuário: Operador, Supervisor, Administrador e Técnico de suporte. Será permitido apenas que interfaces de desenvolvimento, criação de scripts, criação de roteamento e desenvolvimento/gestão avançadas esteja em interface apartada, porém que utilize os mesmos usuários e níveis de acesso da administração principal para login dos usuários;

1.4.3. O acesso do cliente poderá ser realizado por quaisquer meios indicados neste edital e a resolução de suas demandas poderá ser realizada de maneira imediata, ao longo do atendimento, ou posteriormente, quando a resolução depender de outras equipes ou Unidades internas e entidades externas;

1.4.4. Todas as respostas e interações com os clientes deverão ficar registradas no seu histórico, criando uma visão 360º do cliente atendido na solução;

1.4.5. Deverão ser gravadas todas as interações entre o Cliente e o Atendente, Assistente Virtual ou atendimentos eletrônicos, independente do meio de acesso, com objetivo de manter o histórico do atendimento e gerar informações para a realização do mapeamento da jornada do cliente;

1.4.6. A Solução deve disponibilizar APIs para que os acessos por chat, bots e vídeo possam ser disponibilizados em qualquer sistema, de maneira a prover ao cliente a possibilidade de acesso independente do meio em que estiver se comunicando;

1.4.7. A SOLUÇÃO deve identificar a origem do atendimento (web, redes sociais, app etc.), possibilitando tratar de forma diferente as mesmas perguntas dependendo das peculiaridades do canal ou plataforma;

1.4.8. A ferramenta deverá contemplar procedimento para envio direto do histórico do atendimento e/ou conteúdo do chat ao cliente, meio eletrônico, com a devida identificação do atendente emissor para fins de auditoria.

## 1.5. Idioma

1.5.1. A solução ofertada deverá fornecer todas as interfaces de acesso dos usuários ao sistema, no idioma português do Brasil.

1.5.2. Todos os Relatórios disponibilizados pela solução ofertada deverão estar no idioma português do Brasil.

## 1.6. Desempenho

1.6.1. Todas as interações entre os atendentes e clientes, via meios textuais síncronos (chat, instant messengers etc.) e assíncronos (como WhatsApp, SMS, E-mail etc.) deverão ter latência e desempenho adequado para uma boa comunicação, excluindo a parte que diz respeito a rede da CONTRATANTE e de terceiros como mídias sociais etc.

1.6.2. No caso da digitação, a solução deverá apresentar visualização na tela de quem escreve, das próprias informações digitadas de maneira instantânea, não sendo aceitos delays que prejudiquem a fluidez da digitação. Tal característica é aplicável tanto ao atendente quanto ao cliente.

1.6.3. As interações dos Bots com os clientes não poderão ter latência que prejudiquem a fluidez da conversação.

1.6.4. No caso das chamadas de voz e vídeo, estas deverão ser fluidas e sem delays ou variações, com qualidade superior ao índice SNR (Signal to Noise Ratio).

1.6.4.1. Conforme a ITU-T, a CONTRATADA deverá manter o SNR acima de 20 dB para garantir inteligibilidade adequada e qualidade de serviço satisfatória.

1.6.5. A solução deverá possuir mecanismos de monitoramento da qualidade das comunicações de voz em tempo real ou quase real, permitindo a identificação de degradações de áudio, tais como latência elevada, jitter, perda de pacotes e falhas de transmissão.

1.6.6. A solução deverá, ainda, permitir a identificação de anomalias em chamadas, tais como ausência de áudio (chamadas mudas), disponibilizando tais informações para fins de monitoramento operacional e geração de relatórios.

## 1.7. Gerenciamento

1.7.1. A Solução deverá implementar funcionalidades de monitoração e gerenciamento de todos os seus componentes, das operações dos atendentes e dos atendimentos sob o ponto de vista de falhas, desempenho, capacidade e troubleshooting.

1.7.1.1. Deverá dispor de registro de todas as ações: operacionais, de atendimento, de gestão, de acesso, de configuração, de transações e de autenticações realizadas na Solução.

1.7.1.1.1. Todos estes registros deverão estar identificados com usuários, data e horário do evento.

1.7.2. Deverá implementar interface de gestão de toda a solução, unificada, de maneira a prover todas as informações analíticas, sintéticas, quantitativas e qualitativas, em tempo real ou histórica.

1.7.2.1. Implementar, conforme solicitação, a geração de relatórios, visões, dashboards, painéis, utilizando os indicadores de desempenho definidos neste edital, de forma descritiva e gráfica, totalmente customizáveis e online;

1.7.2.2. Os relatórios e dashboards deverão ser disponibilizados em modelos dos tipos: line charts, area charts, column and bar charts, pie charts e 3D charts;

1.7.2.3. Todos esses relatórios, dashboards e painéis, deverão ser acessíveis via Browser de mercado.

1.7.3. Todas as informações (campos, dados calculados, parâmetros, ou qualquer outro tipo de informação nativo ou criado na ferramenta) que constem na solução e os dados oriundos das integrações com os outros sistemas devem ser disponibilizadas, por meio de B.I., API ou arquivo, a fim de permitir a geração de relatórios diversos.

1.7.4. Permitir exportar os relatórios para arquivos em formato de planilha eletrônica e de forma gráfica que permitam análise de desempenho.

1.7.5. Todos os usuários definidos na solução deverão ter suporte ao uso do SSO (Single Sign-On) para login na solução por meio de comunicação padrão Security Assertion Markup Language 2.0 (SAML 2.0) ou OpenID Connect (OIDC).

1.7.6. Implementar níveis de serviço para os indicadores de desempenho e configurar alarme para esse nível de serviço.

1.7.7. A Solução deverá permitir o agrupamento/vinculação dos atendentes e apuração de resultados por site de atendimento grupo e/ou localidade.

1.7.8. Os relatórios gerados deverão permitir a extração para no mínimo os seguintes formatos .pdf e .csv e permitir agendamento para geração automática dos relatórios em um destes formatos em diretório na máquina do usuário e/ou rede, devendo este agendamento permitir diferentes formas de periodicidade (ex: diário, semanal, mensal, dias específicos, horários definidos, a cada X minutos etc.).

1.7.9. Sistemas de Gerência de uso dos recursos.

1.7.9.1. Fornecer todas as informações de uso dos serviços contratados;

1.7.9.2. Deverá implementar relatórios de picos de uso dos recursos contratados, que permita medir utilização/consumo dos recursos.

1.7.10. Sistemas de gerência de log da solução

1.7.10.1. Deverá dispor de registro de todas as ações: operacionais, de atendimento, de gestão, de acesso, de configuração, de transações, de autenticações realizadas na solução.

1.7.11. Relatórios e outros recursos

1.7.11.1. A solução deverá possuir a capacidade de geração de relatórios, online e impressos, sem afetar diretamente o desempenho da solução;

1.7.11.2. Deverá implementar relatórios padronizados com as informações comuns relativas aos atendimentos assim como poder gerar relatórios customizados de acordo com as necessidades;

1.7.11.3. A geração desses relatórios deverá ser via interface unificada de gestão simples, com entrada em produção sem afetar a produção dos demais relatórios ativos;

1.7.11.4. Deverá possibilitar a geração e gestão de diferentes relatórios em ambiente Web como: Relatórios de Agentes, de Fila, de Campanhas e de Interações;

1.7.11.5. Deverá alinhar na fase de implantação a definição de relatórios básicos de acordo com a necessidade da CONTRATANTE.

## **1.8. Interoperabilidade da Solução**

1.8.1. Todos os componentes da solução deverão ser completamente integrados e interoperáveis entre si.

1.8.2. A solução deverá possuir módulo de Inteligência Artificial (IA) Generativa integrado.

## **1.9. Segurança de Mídia e Sinalização**

1.9.1. Deverá suportar SIP sobre TLS.

1.9.2. Deverá suportar a sinalização no SDP para o estabelecimento de sessão de transporte seguro de mídia orientada à conexão sobre o protocolo TLS.

1.9.3. A solução deverá suportar o transporte seguro da sinalização SIP sobre o protocolo TLS conforme estabelecido na RFC 3261.

1.9.4. Suportar o transporte seguro da mídia RTP, chamado de SRTP, em conformidade com as normas estabelecidas na RFC 3711 ou RFC 5506 e atualizações ou via algoritmo sem a degradação do sistema.

1.9.5. Suportar as funcionalidades stateful inspection, sendo capaz de analisar a sessão e manter o estado dela em uma tabela de conexões.

1.9.6. A Solução deverá ser capaz de rejeitar ou bloquear todos os protocolos e aplicações que não se encontram envolvidos na comunicação SIP.

1.9.7. Implementar proteções, tais como: contra IP Spoofing, contra SYN Flood e UDP Flood e contra ataques de negação de serviço, DoS (Denial Of Service), DDoS (Distributed Denial of Service) e contra ataques de fragmentação em TCP/IP.

1.9.8. Realizar bloqueio de ataques com base na análise de pacotes de rede.

1.9.9. Proteger contra-ataques de anomalias de protocolos.

1.9.10. Identificar e proteger contra anomalias de tráfego.

1.9.11. Proteger contra-ataques em nível 2 da camada OSI (timeouts de conexão, tabela de endereços MAC, tamanho de pacotes).

1.9.12. Proteger contra tentativas de varredura de portas e rede (ataques de reconhecimento).

1.9.13. Controle de tráfego de sinalização por usuário e por interconexão, para proteção contra-ataques DoS e DDoS (Distributed Deny of Service).

1.9.14. Capacidade de analisar, de forma configurável, tanto o cabeçalho (header) como a área de dados (payload) de cada pacote que trafega pela rede monitorada.

1.9.15. Possuir capacidade de realização de todas as suas atividades de inspeção, análise e bloqueio compatível com o volume de chamadas especificado neste documento, de maneira a não inserir quaisquer atrasos ou problemas nas comunicações de tempo real e sem nenhum prejuízo às capacidades exigidas nestas especificações.

1.9.16. Proteger contra avalanche de registros, mesmo quando for usado autenticação para os Registros de usuários SIP. A solução deve permitir que todos os usuários se registrem aos poucos durante uma avalanche, sem comprometer o SBC e nem os Application Servers envolvidos.

## 1.10. Operação

1.10.1. A CONTRATADA deverá implementar a gestão operacional do Contact Center, assegurando o controle e a administração eficientes dos processos e equipes. Para tal, a CONTRATADA deve atender aos seguintes requisitos mínimos:

1.10.1.1. Ferramentas de Monitoramento e Controle de Performance: Fornecer e configurar ferramentas para monitorar, em tempo real, indicadores de desempenho, incluindo volume de chamadas, tempo de espera, taxa de resolução no primeiro contato, entre outros;

1.10.1.2. Gestão de Pessoas: Disponibilizar ferramentas para o controle de escalas de trabalho, desempenho individual dos atendentes, bem como relatórios detalhados sobre produtividade e qualidade de atendimento;

1.10.1.3. Automação e Gestão de Processos: Implementar soluções que permitam automatizar e gerenciar os fluxos de trabalho do Contact Center, garantindo a aderência aos processos e a otimização das operações para melhorar a eficiência geral;

1.10.1.4. Geração de Relatórios e Informações Operacionais: Disponibilizar relatórios customizáveis que incluam métricas operacionais essenciais, como desempenho, qualidade de atendimento e indicadores de satisfação do cliente, conforme necessidades do contratante;

1.10.1.5. Interface para Supervisores: Implementar uma interface dedicada para supervisores, que permita o acompanhamento em tempo real das operações, acesso a relatórios detalhados e a possibilidade de realizar intervenções e ajustes.

1.10.1.6. Integração com Copiloto de Inteligência Artificial Generativa

1.10.1.6.1 A solução deverá possibilitar integração com serviços de Inteligência Artificial Generativa de mercado, por meio de APIs ou SDKs abertos, permitindo futura adoção de recursos de copiloto para suporte a agentes, supervisores e administradores.

1.10.1.6.2 A funcionalidade de copiloto, quando disponível, deverá operar de forma contextual, segura e integrada à plataforma, contemplando:

1.10.1.6.2.1. Agentes: apoio em tempo real durante interações, com sugestões de respostas, resumos de conversas e orientações baseadas na base de conhecimento da organização;

1.10.1.6.2.2. Supervisores: disponibilização de insights e recomendações sobre desempenho de filas, agentes e interações, além de geração de resumos automáticos de atendimentos;

1.10.1.6.2.3. Administradores: suporte à configuração e gestão da plataforma, com possibilidade de execução de tarefas administrativas via comandos em linguagem natural (ex.: criação de usuários, filas e políticas de roteamento).

1.10.1.6.3 Será permitido que a solução contemple copiloto integrado nativamente à plataforma CCaaS (Contact Center as a Service), não obrigatório, desde que não implique custo adicional para CONTRATANTE.

1.10.2. As chamadas deverão chegar aos atendentes logados na solução de maneira automática, de acordo com as configurações realizadas na solução e com as decisões tomadas na própria solução de acordo com as regras de negócio estabelecidas;

1.10.3. A solução deverá permitir aos atendentes:

1.10.3.1. Tratar mais de uma chamada por atendimento, conforme regras estabelecidas pela CONTRATANTE na Solução.

1.10.3.2. As chamadas poderão ser redirecionadas para outra fila de atendimento sem perder as informações já prestadas ao cliente nem o que já foi conversado, permitindo que o novo atendente, ou “Bot”, tenha acesso a todas as informações anteriores e possa utilizá-las como parâmetros para um atendimento personalizado.

1.10.3.3. Permitir que todos os atendentes cadastrados na solução possam utilizar todos os meios de acesso no atendimento ao cliente, de maneira flutuante, de acordo com a necessidade estabelecida pela CONTRATANTE e configurada na solução.

1.10.3.4. Permitir a montagem de consultas personalizadas dentro da estrutura da Solução.

1.10.3.5. Implementar rastreamento da chamada do início ao fim, inclusive se houver transferências internas ou externas, com mudança de meio de acesso ou forma de atendimento (humano ou eletrônico).

1.10.3.6. No caso de queda da comunicação da solução, os atendimentos em curso deverão ser salvos permitindo que sejam retomados após a normalização da comunicação.

1.10.3.7. Permitir que o atendente, em uma chamada em curso com o cliente por um meio de acesso, possa interagir com o cliente através de outro meio simultaneamente.

1.10.3.8. Também deverá ser possível realizar chamadas paralelas à chamada com o cliente, para outros supervisores ou atendentes, visando realizar conferência com o cliente.

1.10.3.9. A Solução deve permitir o monitoramento do atendimento pelo Supervisor ou outro perfil definido pela CONTRATANTE. Tal monitoração deve ser realizada em tempo real para áudio e tela do atendente.

1.10.3.10. A solução proposta deve prover ferramentas para monitoramento do desempenho dos atendentes e acompanhamento online dos resultados da operação.

1.10.3.11. A Solução deverá implementar filas de atendimento, para atendentes individuais, assim como para grupos de atendimento, permitindo transferências entre grupos ou atendentes específicos, de acordo com configuração solicitada pela CONTRATANTE, independentemente da localização física dos atendentes.

1.10.3.11.1. Para cada recepção de chamadas, seja por grupos ou atendentes, poderá ser implementada uma fila de espera específica, com mensagem(s) específica(s), dando opções para o cliente aguardar o atendimento ou programar um retorno para cada uma delas;

1.10.3.11.2. A Solução deve possibilitar a inclusão, exclusão e consulta de mensagens de fila de espera, com log de auditoria destas ações, por grupo ou perfil de acesso específico.

## 1.11. Frontend

1.11.1. Frontend é a interface apresentada aos usuários do sistema para suas interações.

1.11.2. Tal interface deverá ser única e configurável para cada perfil de usuário, grupo de atendimento ou mesmo tipo de atendimento (produto ou meio, canal, fila ou assunto).

1.11.3. A solução deverá apresentar no frontend de atendimento as informações pessoais do cliente, caso identificado previamente por bot ou atendente, o canal, fila e/ou assunto escolhido e um histórico dos últimos contatos com a CONTRATANTE.

1.11.4. A interface do atendente deverá permitir rodar aplicação e web site em um painel para permitir ao atendente não precisar trocar de tela durante interação com o cliente, a aplicação ou site web devem ser configurados previamente e não podem ser alterado pelo atendente.

## 1.12. Scripts e Telas

1.12.1. Implementar a funcionalidade de respostas automáticas baseadas em scripts visuais, adaptados pela solução para: o meio de acesso da chamada, para o cliente identificado, para o assunto abordado além de parâmetros como:

fila de espera, interações anteriores do cliente e outros parâmetros que serão implementados com o uso de Inteligência Artificial (IA) Generativa, como o humor do cliente.

1.12.1.1. Tais scripts poderão ser apresentados plenamente (script completo) ou por passos, a exemplo de um “Wizard”, onde os passos seguintes aparecem somente depois de recebidas as respostas relativas aos passos anteriores, e de acordo com o teor dessas respostas.

1.12.2. A solução deve dispor de módulo para montagem e ajustes nos scripts do sistema, permitindo a criação de novos scripts, com suas árvores de escolhas, na própria ferramenta bem como alteração nos scripts já existentes.

1.12.3. Um mesmo Script ou seus passos intermediários poderá ter visões distintas para diferentes perfis de usuários (atendente, supervisor, empregado da CONTRATANTE, gestor ou quando o próprio cliente estiver se auto atendendo - chatbot).

1.12.4. Permitir seleção dos estados dos atendentes, tais como: logado; não logado; disponível; pausa; treinamento; lanche; banheiro; feedback; pausa pós-atendimento (automática ou manual); não disponível e outros motivos a serem incluídos pela CONTRATANTE.

1.12.5. Permitir o gerenciamento de dados de configuração, bem como o gerenciamento através da supervisão em tempo real de grupos de gestão e dos atendentes.

1.12.6. Deverá permitir aos supervisores se colocarem à disposição para receber chamadas durante os períodos de maior movimento.

1.12.7. Permitir configurar o nível de serviço para cada fila, de forma a proporcionar que o Supervisor as monitore em tempo real.

1.12.8. Permitir ao supervisor a monitoração, em seu frontend, das chamadas em curso pelos atendentes com escuta ativa e passiva.

1.12.9. Permitir a configuração centralizada, a partir dos frontends dos supervisores, de parâmetros de configuração de atendentes e de grupos de atendimento, dentre outros.

1.12.9.1. Permitir a emissão de relatórios estatísticos, de ocorrências e gráficos, de forma remota e centralizada, conforme descritos nestas especificações;

1.12.9.2. Permitir ao supervisor e a outros usuários localizados na rede da CONTRATANTE logados na Solução, através de configuração, a monitoração em tempo real dos dados de atendentes e grupos.

1.12.10. A solução deve permitir discar para um número telefônico assim como permitir a transferência de chamada.

1.12.11. Deverá ser permitido comandos para as funções na tela da estação de trabalho, nas posições de atendimento, tais como: login/logout para recebimento de chamadas.

1.12.12. Deverá permitir desconectar ou não desconectar uma ligação, conforme parametrização da CONTRATANTE.

1.12.13. Participar ou iniciar uma conferência com capacidade para, no mínimo, 3 participantes;

1.12.14. Permitir transferência de chamada;

1.12.15. Configuração viva-voz (handsfree), sem cortes ou interrupções durante a conversação e estabelecimento de ligações;

1.12.16. Deverá permitir comandos para funções do softphone como: login/logout para recebimento de chamadas; discagem para um número interno ou externo; consulta; pausa nas ligações, com inclusão do motivo.

### 1.13. Workforce Management

1.13.1. A solução deve possuir interface gráfica amigável e navegação simples que permita a manutenção dos estados dos atendentes (inclusão, alteração, exclusão e desabilitação).

1.13.2. Implementar as funções de coleta de dados históricos, Previsão de Demanda (Forecasting), Dimensionamento, Programação de Escalas (Scheduling), Flexibilidade da Força de Trabalho (Workforce), Tecnologia Diferenciada (cálculos e finalizações imediatas) e Aderência (adherence) as quais proporcionam as seguintes funcionalidades:

1.13.2.1. Permitir a alteração de turnos entre atendentes baseado em tarefas e skills adequados, com propostas e aceitação das alterações;

1.13.2.2. Gerenciamento de operação (intradiário), de forma a reagir aos imprevistos do dia a dia;

1.13.2.3. Alocação adequada dos atendentes, evitando excesso de pessoas ou queda do nível de serviço;

1.13.2.4. Acompanhamento da aderência dos funcionários ao planejamento, para que não ocorra perda de tempo;

1.13.2.5. Planejamento de atividades, permitindo que ações fora do atendimento sejam realizadas sem afetar a qualidade da operação e sem necessidade de alocação de mais profissionais;

1.13.2.6. Simulação a capacidade de atendimento do site permitindo a validação das configurações das escalas de trabalho dos atendentes e supervisores;

1.13.2.7. Deverá realizar geração automática das escalas de trabalhos, suportando múltiplos tipos (meio período, período integral e quaisquer outros definidos pelo CONTRATANTE);

1.13.2.8. Implementar estudos estatísticos comparativos, permitindo visualizar a situação de desempenho atual da equipe de atendimento, da Unidade de atendimento (várias equipes) e de toda a Solução (todas as Unidades), possibilitando gerenciamento e adequações proativas objetivando sempre manter níveis de estabilidade e controle das demandas de atendimentos;

1.13.2.9. Permitir prever o desempenho da Unidade com base em parâmetros definidos e históricos de ligações e possibilitando a preparação dela para condições de desempenho variáveis, de maneira a manter os níveis de serviço;

1.13.2.10. Possibilitar simular cenários com diferentes volumes de entradas de clientes.

1.13.2.11. Implementar elaboração de prognóstico (forecast) para as ações realizadas (receptivas e ativas) por todos os meios de atendimento ao cliente presentes na Solução;

1.13.2.12. Permitir o acompanhamento dos prognósticos gerados em tempo real, possibilitando ações de correção de curso imediatas com o uso de funcionalidade adherence com base nos forecast e Schedule gerados possa ser usada de forma a otimizar a utilização dos diversos recursos em tempo real;

1.13.2.13. A funcionalidade de Workforce Management deverá permitir a comparação dos resultados previstos com os “em realização” e “realizados”, conforme preconizado na funcionalidade de “Aderência em tempo real”;

1.13.2.14. Permitir a utilização dos volumes de chamadas históricos para prever o volume de chamadas a ser recebido na central de atendimento em intervalos específicos, e calcular os recursos necessários para atender uma demanda futura;

1.13.2.15. Permitir a criação de cenários alternativos e a inserção de eventos especiais que permitam avaliar os impactos dos volumes previstos de forma a visualizar o melhor e o pior cenário no dia a dia de uma central de atendimento;

1.13.2.16. Criar modelos a serem seguidos para um novo tipo de serviço que ainda não possui histórico para ser utilizado quando um determinado serviço possui um comportamento estável durante todo o decorrer do dia;

1.13.2.17. Permitir ajustes manuais nas curvas que exibem o comportamento da operação em função da previsão realizada, de maneira totalmente gráfica. Assumir os novos valores conforme a curva vai sendo redefinida, de acordo com a estratégia para o período;

1.13.2.18. Todos os componentes do Workforce Management descritos neste item devem ser do mesmo fabricante, compondo uma suíte integrada.

#### 1.14. Curadoria

1.14.1. A CONTRATADA deve fornecer um canal de atendimento para que a CONTRATANTE possa solicitar atualizações e melhorias necessárias aplicadas ao sistema;

1.14.2. O atendimento deverá ser realizado pela CONTRATADA, durante toda a vigência do contrato, por meio de telefone, e-mail ou ferramenta específica disponibilizada pela mesma;

1.14.3. O prazo para realização do serviço será contado a partir do momento que for registrada o ticket do chamado junto ao CIISC;

1.14.4. Tempo máximo para atendimento será de 24h úteis contadas a partir da solicitação;

1.14.5. Compreende solicitações de atualizações e melhorias necessárias aplicadas ao sistema, como os exemplos abaixo:

1.14.5.1. Analisar e qualificar interações recebidas pelo Assistente Virtual Cognitivo;

1.14.5.2. Identificar as mensagens recebidas e medir a evolução da ferramenta;

1.14.5.3. Melhorar o conteúdo do robô levando em conta as necessidades dos Usuários Externos e da CONTRATADA;

1.14.5.4. Criar e/ou alterar intenções e suas possibilidades de respostas;

1.14.5.5. Criar e editar fluxos de atendimento;

1.14.5.6. Gerar insights para melhorias e implementações;

1.14.5.7. Entregar relatórios sobre otimizações e funcionamento do Assistente Virtual Cognitivo;

1.14.5.8. Ou outras atividades correlatas.

1.14.6. A solução deve permitir a curadoria de informações em bases de conhecimento através de atividades de validação, mapeamento, divisão, união e remanejamento de intenções, indexação e reindexação de dados, tratamento de fluxos e representação textual de intenções.

1.14.7. A plataforma deve disponibilizar painel de gestão contendo informações sobre a utilização de protótipos, casos implementados e demais informações necessárias que permitam ações de otimização;

1.14.8. Plataforma deve permitir modelar, construir, treinar, avaliar e validar protótipos com o Inteligência Artificial (IA) Generativa para atendimento cognitivo;

1.14.9. O serviço de curadoria deverá possibilitar o treinamento dos modelos de IA de acordo com os requisitos específicos do projeto;

1.14.10. A CONTRATADA deverá realizar ajustes finos para otimizar o desempenho e a precisão do Assistente Virtual Cognitivo;

1.14.11. A CONTRATADA deverá realizar testes rigorosos para validação da precisão e confiabilidade.

1.14.12. A CONTRATANTE, mediante a necessidade do seu projeto, poderá contratar pacotes de curadoria de forma mensal recorrente, sem compromisso de continuidade ao longo do contrato, ou seja, poderá a seu critério contratar ou não o serviço de curadoria;

1.14.13. Os componentes utilizados na construção de aplicativos e soluções devem possuir capacidade de aprendizado, de maneira a permitir a evolução contínua das bases de conhecimento utilizadas pela tecnologia de IA;

1.14.14. A CONTRATANTE, a seu critério, poderá realizar a contratação de mais de um pacote de curadoria no mês;

1.14.15. A curadoria das informações utilizadas nas tecnologias para atendimento cognitivo deve ser realizada pela CONTRATADA.

#### 1.15. Motor de inteligência artificial

- 1.15.1. O Assistente Virtual Cognitivo deverá possuir um motor de inteligência artificial cognitiva.
- 1.15.2. A CONTRATADA deverá fornecer ferramentas para gestão de conteúdo por meio de perguntas e resposta;
- 1.15.3. A solução deverá fornecer uma ferramenta de criação de diálogos intuitiva e de fácil utilização por pessoas sem experiência no paradigma de linguagens de programação estruturada;
- 1.15.4. A solução deverá permitir a definição de entidades que representam termos específicos que se deseja identificar no texto e extrair para que possa realizar algum tipo de tratamento.
- 1.15.5. Deverá ser possível também agrupar entidades semelhantes em categorias e usar os sinônimos desses termos para identificar um mesmo valor;
- 1.15.6. A solução deverá oferecer recurso de jumps e slots de modo que seja possível reutilizar nós e fluxos de diálogos, criar fluxos complexos, definir nós com capacidade de coletar múltiplas informações dos usuários externos;
- 1.15.7. Suportar diálogos com contexto e memória, segundo jornadas de diálogo humanizado;
- 1.15.8. A solução deverá, baseado no diálogo, classificar o assunto referente a intenção do usuário externo;
- 1.15.9. A solução deverá possuir a capacidade de fazer perguntas em linguagem natural, em português brasileiro, para que possa buscar a resposta mais adequada;
- 1.15.10. A solução deverá permitir a criação de diálogos para usuários diferentes;
- 1.15.11. A solução deverá oferecer recursos de NLG (Natural Language Generation) integrado ao motor de inteligência artificial para responder automaticamente às perguntas dos usuários externos através de conteúdo disponíveis em documentos próprios fornecidos pela CONTRATANTE;
- 1.15.12. A solução deverá permitir o versionamento dos diálogos, com a possibilidade de publicações e retorno a versões mais antigas;
- 1.15.13. A solução deverá permitir a configuração de diálogos com:
  - 1.15.13.1. Suporte a confirmações implícitas;
  - 1.15.13.2. Questões de verificação;
  - 1.15.13.3. Possibilidade de corrigir informações já dadas;
  - 1.15.13.4. Capacidade de entender quando é dado mais informações do que foi perguntado;
  - 1.15.13.5. Capacidade de suportar negações;
  - 1.15.13.6. Capacidade de entender referências pela análise do discurso e das anáforas;
  - 1.15.13.7. Capacidade de suportar sub diálogos dentro do diálogo principal.
- 1.15.14. Os fluxos de diálogo podem ser construídos com perguntas aninhadas, saltos e lógica condicional para refinar o contexto, obter informações mais refinadas do interlocutor e obter/entregar respostas mais precisas;
- 1.15.15. A solução deverá permitir o reuso e enriquecimento de diálogos em domínios já conhecidos e contidos na base de dados;
- 1.15.16. A solução deverá permitir a utilização de expressões regulares com entidades, variáveis de contexto e sobre perguntas do usuário;
- 1.15.17. A solução deverá permitir a criação de expressões lógicas com as intenções, entidades e variáveis de contexto;
- 1.15.18. A solução deverá possuir entidades de sistema referente a datas e hora de modo que sua lógica considera o termo amanhã como o dia subsequente ao que foi perguntado de maneira automática;
- 1.15.19. A solução deverá permitir a visualização e melhoria dos diálogos, assim como a identificação aquelas perguntas que tiveram baixo entendimento e aquelas que estão em conflito.

### 1.16. Módulo de Integração

1.16.1. A solução deverá possuir a capacidade de ser integrado com plataformas de desenvolvimento existentes, ambientes de DevOps e pipelines de dados. Suportar o ajuste fino e o treinamento personalizado de modelos para atender a casos de uso específicos, permitindo uma integração com serviços como CRM, ERP, automação de atendimento aos usuários externos via chatbot e 0800.

1.16.2. A solução deve permitir integração com diferentes canais, no mínimo, os seguintes: web chat, SMS, Microsoft Teams, Facebook Messenger, Telegram, WhatsApp e voz.

1.16.3. A solução deverá possuir integração com sistema de telefonia de forma nativa através dos serviços de transcrição e sintetização de voz.

1.16.4. A solução deverá possuir recurso próprio para depuração do desenvolvimento do assistente diretamente na interface, com os áudios da integração telefônica.

1.16.5. A solução deverá oferecer APIs RESTful documentadas e seguras para integração com sistemas internos e externos.

1.16.6. A solução deverá possuir integrações realizadas através do formato OpenAPI.

1.16.7. As APIs deverão implementar controles de versão (versionamento) para evitar incompatibilidades em atualizações futuras.

1.16.8. Para integrações com canais de comunicação que possuam políticas específicas de uso ou exijam utilização de interfaces oficiais, a solução deverá utilizar APIs ou mecanismos homologados pelos respectivos provedores, garantindo conformidade com suas políticas, bem como a segurança, integridade e continuidade das comunicações.

1.16.8.1. Para o canal WhatsApp, será obrigatória a utilização de APIs oficiais disponibilizadas pelo provedor da plataforma.

### 1.17. Processamento

#### 1.17.1. RIC – Roteamento Inteligente de Chamadas

1.17.1.1. O RIC deve ter a capacidade de tomada de decisões e roteamento automático de interações em todos os canais disponíveis na Solução, de acordo com os parâmetros definidos previamente pelas regras negociais configuradas, com base em parâmetros diversos de desempenho e capacidade da estrutura tecnológica, dos atendentes e das informações da CONTRATANTE.

1.17.1.1.1. O RIC deve interagir com o motor de decisão, executando todas as programações estabelecidas e regras de negócio definidas no motor;

1.17.1.2. As ações do RIC devem envolver a priorização das chamadas nas filas existentes, o envio aos atendentes de acordo com o nível de habilidades e dos contextos delineados pelas regras negociais implementadas na solução e da CONTRATANTE;

1.17.1.3. O RIC deverá realizar o roteamento da chamada para o melhor atendente disponível para o cliente de acordo com as definições negociais implementadas na solução;

1.17.1.4. Deverá distribuir chamadas entre os diferentes atendentes e grupos, independentemente de estarem em redes locais distintas ou geograficamente distantes.

1.17.1.5. Deverá permitir o roteamento de chamadas em função do número telefônico de destino DNIS - Dialed Number Identification Service e do número telefônico de origem ANI - Automatic Number Identification.

1.17.1.6. Deverá permitir a restrição de chamadas indevidas (trotes), através do ANI, para grupos específicos de atendentes, com configuração por meio de interface amigável.

1.17.1.7. Deverá permitir a definição do roteamento de chamadas a partir de um “script de eventos”, permitindo a parametrização de músicas de espera e mensagens diferentes para cada fila ou outro parâmetro do cliente que já tenha sido identificado.

1.17.1.8. Deverá possuir capacidade para a configuração para o tratamento das chamadas, roteando-as por grupo de atendimento, tomando como base, no mínimo, estes critérios: horário de atendimento; número de atendentes disponíveis; número de chamadas em fila e prioridade para atendimento; número de atendentes logados; tempo em fila de espera; chamada mais antiga em fila de espera; anúncio de desconexão; roteamento; habilidades dos atendentes; nível exigido de habilidades para o tipo de atendimento; categoria do cliente; capacidade estimada de atendimento assim como outros parâmetros definidos com uso de Inteligência Artificial (IA) Generativa.

1.17.1.9. Permitir o roteamento condicional de chamadas, baseando-se, pelo menos nos seguintes dados: número de chamadas em espera nas filas dos grupos; número de atendentes disponíveis nos grupos; tempo da chamada mais antiga na fila dos grupos; número de atendentes logados nos grupos; tempo de ocupação dos atendentes.

1.17.1.10. Possuir interface gráfica amigável para configuração de regras de roteamento.

1.17.1.11. Permitir o roteamento baseado em atributos ou facilidade similar, possibilitando o encaminhamento de chamadas baseado na habilidade ou currículo de cada agente;

1.17.1.12. Permitir que os atendentes com as mesmas habilidades possam ser diferenciados por preferência de atendimento de chamada e por pontuação atribuída às suas habilidades e resultado das avaliações do atendimento realizadas pelos clientes.

## **1.18. Executor de Campanhas**

1.18.1. A lista de contatos deverá ter sua constituição configurável, com a possibilidade de inserção e retirada de campos predefinidos ou novos.

1.18.2. A lista de contatos deverá possuir a funcionalidade de exclusão/inativação de clientes incluídos em listas restritivas, como blacklist e “Não Perturbe”, ou outras bases cadastrais a critério;

1.18.3. Deverá possuir funcionalidade de avaliação dos atendimentos em curso e da capacidade de atendimento instantâneo, de maneira a avaliar e indicar ao atendente se a(s) abordagem(ens) de venda deverá(ão) ser realizada(s) ou não.

1.18.4. Implementar a definição de critérios para geração da campanha (horário, agentes, Mailing);

1.18.5. Possuir interface para gerenciamento da campanha e da lista de clientes, permitindo que os supervisores monitorem, em tempo real, campanhas, grupos de atendentes de campanhas, informações das listas de contatos, iniciem ou parem as campanhas ou sequências de campanhas;

1.18.6. Permitir que o supervisor ou administrador ajustem parâmetros (taxa de rediscagem ou reenvio, taxa de ocupação do agente, tempo médio de geração de chamadas, mudança do modo de discagem) das campanhas ativas durante a sua execução, ou seja, em tempo real;

1.18.7. Gerenciar a lista de contatos compreendendo as seguintes características: observar a lista, adicionar/modificar/deletar registros da lista, criar cadeias de registros na lista (tipos de contato: residencial, comercial, celular etc.), visualizar/alterar o filtro utilizado para cada lista de chamadas;

1.18.8. Definir e utilizar-se de público-alvo e scripts de abordagem com roteiro de instruções para o melhor atendimento dos clientes;

1.18.9. Gerir o encadeamento de campanhas, permitindo campanhas múltiplas na mesma plataforma, simultaneamente;

1.18.10. Possuir mecanismo de acompanhamento do retorno e efetividade de toda campanha, com detalhes dos atendimentos e respectivas operações, indexado por cliente. Tais informações também podem ser enviadas aos Sistemas da CONTRATANTE por meio de arquivo ou serviços online;

1.18.11. Deverá apurar os resultados das campanhas, através da ferramenta de análise baseada nas informações oferecidas pela Solução de atendimento;

1.18.12. Permitir que o supervisor associe os atendentes de acordo com a sua especialidade nas campanhas. Um atendente poderá ser associado em mais de uma campanha.

### **1.19. Fila Universal**

1.19.1. A solução deverá implementar a recepção de chamadas por qualquer meio em fila universal, com capacidade para aplicação de política de atendimento.

1.19.1.1. A Solução deverá identificar o cliente por meio do seu número de telefone ou dado informado pelo cliente na URA.

1.19.2. Esta fila universal deverá implementar parametrizações e controle de prioridades dos meios de acesso de acordo com as definições das regras de negócio implementadas na solução.

1.19.2.1. Todos os parâmetros relacionados ao cliente, como perfil, tempo de espera, quantidade de atendimentos frustrados, meio de acesso preferencial, número de rechamadas, telefones suspeitos e outros parâmetros implementados com o uso de Inteligência Artificial (IA) Generativa (como o humor do cliente), deverão compor as regras de negócio e por conseguinte as prioridades e organizações na fila universal.

1.19.3. Também deverá ser possível gerar avisos e propagandas visuais ou auditivas, adequada ao seu meio de acesso, enquanto o cliente aguarda, podendo a mesma ser obrigatória para o passo seguinte de atendimento, ou opcional, podendo o cliente optar por não ser apresentado.

### **1.20. Geração de Números de Protocolos**

1.20.1. A solução deverá possibilitar a integração com o sistema da CONTRATANTE para geração de protocolos únicos por atendimento, devendo este ser informado para o cliente o início da interação independentemente do meio de acesso utilizado;

1.20.2. Os protocolos deverão ser informados ao cliente, ao atendente e registrados na solução como histórico do cliente, através de meios eletrônicos e de atendimento humano;

1.20.3. Permitir que o número do protocolo seja disponibilizado ao cliente pelo canal utilizado para contato;

1.20.4. A Solução deverá permitir localização das gravações através do número do protocolo.

### **1.21. Monitoria de Qualidade**

#### **1.21.1. Análise de Fala (Speech Analytics)**

1.21.1.1. A Solução deverá apresentar os termos e categorias mais citadas em todas as interações processadas, em formato de lista, nuvem ou árvore de palavras;

1.21.1.2. A Solução deverá fornecer busca por palavra-chave e/ou frases;

1.21.1.3. A Solução deve ser capaz de transcrever e analisar integralmente o teor de todas as chamadas de voz e interações textuais processadas pela ferramenta;

1.21.1.4. A Solução deve ser capaz de interpretar e consolidar dados e apresentar em dashboards parametrizáveis a análise de desempenho dos atendentes;

1.21.1.5. A Solução deve possibilitar a criação de alarmes ou alertas para gerentes e supervisores com relação ao desempenho dos atendentes, individualmente ou por site.

### 1.21.2. Avaliação de Desempenho (Quality Monitoring)

1.21.2.1. A solução deverá contemplar recursos de Quality Monitoring integrados à plataforma, permitindo a avaliação de desempenho de agentes por meio de formulários personalizáveis, aplicados por supervisores ou avaliadores, com critérios objetivos e subjetivos (ex.: empatia, aderência ao script, resolução da demanda).

1.21.2.2. A solução deverá disponibilizar mecanismos de feedback estruturado aos agentes, com notificações e relatórios acessíveis no próprio ambiente da plataforma.

1.21.2.3. A solução deverá fornecer relatórios e painéis (dashboards) em tempo real e histórico, incluindo de forma nativa indicadores de satisfação do cliente como CSAT (Customer Satisfaction Score/ Índice de Satisfação do Usuário) e, adicionalmente, indicadores de lealdade do cliente NPS (Net Promoter Score/ Escore Líquido de Promotores), que poderão ser entregues de forma nativa na plataforma ou via integração provida, configurada e mantida pela CONTRATADA, desde que não implique em custos adicionais para a CONTRATANTE.

### 1.22. Gravação Digital

1.22.1. A Solução deverá realizar a gravação das chamadas realizadas por quaisquer meios de acesso e das telas dos atendentes com os passos seguidos no momento do atendimento e permitir a reprodução com o áudio e vídeo sincronizados, em ferramenta de reprodução com facilidades padrões de dispositivos de reprodução (reproduzir, pausar, avançar, retroceder e posicionar diretamente em um ponto da gravação).

1.22.1.1. A Solução deve permitir realizar a gravação de todas as interações realizadas por meio de voz, texto, vídeo e atendimento automático, incluindo chatbots.

1.22.1.2. A Solução deve permitir realizar a monitoração da gravação de todas as interações em tempo real.

1.22.2. Todas as gravações deverão suportar exportação dos arquivos no formato em padrão aberto, de menor tamanho possível.

1.22.2.1. Todas as transcrições de atendimentos realizados deverão ser gravadas em arquivos não editáveis.

1.22.3. A solução deverá realizar as gravações exclusivamente no ambiente centralizado da solução, não sendo permitida a gravação local nas PAs (Posição de Atendimento).

1.22.4. Deverá ter a capacidade para a gravação simultânea de todas as chamadas recebidas, originadas, transferidas internamente e internas por grupo/fila de atendimento, agente ou ramal, de forma configurada, através de software.

1.22.5. As gravações deverão permitir auditoria e acompanhamento das ligações gravadas, através de software de monitoramento de avaliação da qualidade a ser fornecido pela CONTRATADA.

1.22.6. Implementar a categorização (marcação) da gravação de forma a diferenciar as chamadas de abordagem (confirmação do contato realizado e do entendimento do cliente) das chamadas de abordagens com aceite vocal (registro do seu interesse), sendo que estas últimas deverão ser sinalizadas através de análise automática do conteúdo do atendimento, ou, adicionalmente, por acionamento manual pelo operador e/ou supervisor.

1.22.7. As gravações deverão ser armazenadas no ambiente da CONTRATADA pelo período mínimo de 180 dias para voz e texto.

1.22.8. A Solução deverá implementar a indexação de todos os arquivos armazenados no ambiente da solução e manter os metadados para quando estes forem transferidos para o ambiente externo, de maneira a permitir que os gestores e usuários possam gerir os arquivos através do uso dos metadados da interação, podendo realizar buscas por quaisquer parâmetros definidos em comum acordo.

1.22.9. Deverá transcrever os áudios gravados em texto (speech to text), armazenando e permitindo pesquisa no texto gerado.

1.22.10. O tempo de armazenamento dos arquivos deve ser parametrizável, permitindo ao cliente definir o que melhor lhe atenda.

1.22.11. Todos os arquivos gravados deverão estar indexados, no mínimo com as seguintes informações (metadados): Nome do cliente; nome do operador; número do telefone do cliente, e-mail ou outra identificação de cliente; meio acessado: Chat, e-mail, voz, vídeo, SMS, Instant Messengers, Redes Sociais e campos numéricos tais como:

1.22.11.1. Campo numérico com, no mínimo 11 (onze) dígitos, representando o CPF e CNPJ;

1.22.11.2. Data: Campo numérico composto de 6 (seis) dígitos representando a data do atendimento, no formato: ddmmaa: dd - dois dígitos representando o dia e mm - dois dígitos representando o mês. aa - dois dígitos representando o ano;

1.22.11.3. Hora: Campo de quatro dígitos representando a hora do atendimento no formato 24 (vinte e quatro) horas: hhmm: hh - dois dígitos representando a hora e mm - dois dígitos representando os minutos;

1.22.11.4. Pelo número do telefone do cliente, e-mail ou identificação de cliente;

1.22.11.5. Número do protocolo do atendimento;

1.22.11.6. Outros parâmetros acordados entre CONTRATANTE e CONTRATADA.

### 1.23. Armazenamento e Backup

1.23.1. Todos os dados deverão ser gravados e armazenados de forma contínua, em banco de dados relacional e/ou NoSQL, desde que assegurem escalabilidade, baixa latência, integridade transacional, auditabilidade e rastreabilidade, em nuvem pública localizada em território brasileiro;

1.23.2. A CONTRATADA deverá manter a CONTRATANTE informada, durante toda a vigência do contrato, do endereço das instalações onde os dados serão gravados e armazenados;

1.23.3. A CONTRATADA deverá manter o ambiente de hospedagem do sistema de forma segura, tanto lógica como fisicamente, a partir de recursos tecnológicos na forma de programas ou de equipamentos físicos, que coíbam acessos indevidos, com políticas ou regras de segurança, preservando a identidade dos usuários e a integridade dos dados;

1.23.4. A CONTRATANTE deverá ter acesso imediato a qualquer dado armazenado;

1.23.5. A CONTRATADA deverá manter absoluto sigilo sobre todos os dados armazenados do sistema, devendo apenas ser revelado por solicitação expressa de representante legal da CONTRATANTE.

1.23.6. Em caso de rescisão ou término do contrato, a CONTRATADA obriga-se a disponibilizar, sem ônus para a CONTRATANTE, cópia atualizada de todas as bases de dados e informações armazenadas pelos sistemas durante a vigência do contrato, atendendo aos seguintes critérios:

1.23.6.1. Utilizar formato aberto e padrão de mercado para exportação de dados, como CSV, JSON, XML ou outros formatos especificados pela CONTRATANTE;

1.23.6.2. Garantir a integridade, consistência e confidencialidade dos dados durante o processo de transferência;

1.23.6.3. Disponibilizar documentação detalhada dos dados, incluindo metadados, diagramas e modelos necessários para interpretação por parte da CONTRATANTE;

1.23.6.4. O prazo para a transferência completa dos dados e documentação deverá ser acordado com a CONTRATANTE, não ultrapassando 60 (sessenta) dias após o encerramento do contrato;

1.23.6.5. Após a transferência completa e a formalização de pedido da CONTRATANTE, a CONTRATADA será responsável pela desativação e exclusão de todo conteúdo, banco de dados, documentos, dados e informações que estejam em sua posse.

### 1.24. Segurança da informação

1.24.1. Os dados da plataforma deverão ser protegidos pelas normas de sigilo das comunicações e da proteção de dados pessoais;

1.24.2. A CONTRATANTE será proprietária e terá todos os direitos autorais das jornadas de atendimento a ser criada e desenvolvida, dos bancos de dados, inclusive de registro de texto, podendo arquivar, copiar, excluir sem que necessite de autorização da CONTRATADA;

1.24.3. A CONTRATADA não poderá utilizar ou ceder a terceiros o material produzido e cadastros de usuários, inclusive os registros de texto;

1.24.4. A CONTRATADA deverá atender a Lei Geral de Proteção de Dados (LGPD) em sua integralidade.

## 1.25. Sistema de Atendimento

1.25.1. A SOLUÇÃO deverá permitir respostas automatizadas por voz ou texto, utilizadas de acordo com os meios de acesso do cliente, as regras de negócio e configurações na Solução.

1.25.1.1. Deverá prover o atendimento automático, com anunciador por fraseologia, previamente programada, assim como atendimento interativo por menus numéricos, textuais e por comandos de voz, segmentação e encaminhamento das chamadas recebidas, conforme programação implementada;

1.25.1.2. Deverá ser reconhecida a linguagem natural, regionalizada, e poderá ser baseada em dicionário de dados (conversão de voz para texto seguida de busca semântica na lista de comando associados ao menu) ou cognitiva (identificação da intenção da frase pronunciada pelo cliente e busca do menu correspondente);

1.25.1.3. Caso não haja interação por voz, a URA deverá apresentar as opções de menu para escolha pelo cliente por meio de digitação.

1.25.2. Deverá implementar uso de árvores de atendimento com interação por menu numérico, por comandos vocais, visuais e textuais, e por interação direta, simulando o atendimento humano;

1.25.3. Deverá possibilitar a implementação de árvores de atendimento sem a necessidade de uso de códigos-fonte, de forma totalmente gráfica, visando facilitar o uso pelos gestores e administradores;

1.25.4. Deverá permitir a alteração, o desenvolvimento de menus, submenus, de novas árvores de navegação e testes, remotamente, em canais ou módulos isolados do ambiente de produção, antes da ativação e replicação das novas configurações aos outros canais e máquinas.

1.25.4.1. Os fluxos desenvolvidos podem ser aplicados para mais de um canal (URA vocal ou chatbot, por exemplo) se as regras negociais e de experiência do cliente forem aplicáveis.

1.25.5. Deverá permitir a supervisão, a monitoração, a modificação da árvore de menus, a modificação do horário de atendimento, a marcação de datas como feriado e finais de semana, através de interface gráfica, sem a necessidade de reset, paralisação parcial dos grupos de portas e paralisação do sistema de atendimento;

1.25.6. Também deverá permitir configuração da funcionalidade force play para algumas vocalizações, quando necessário, para que o cliente ouça obrigatoriamente toda a mensagem, limpando em seguida o buffer de eventual digitação no decorrer da mensagem, para início da digitação do cliente;

1.25.7. Implementar bots para todos os meios de acesso, com utilização de Inteligência Artificial (IA) Generativa, de maneira a identificar o contexto, entender as perguntas, implementar as respostas corretas e registrar na solução as interações realizadas, finalizando o atendimento ou transferindo a chamada para um atendente.

1.25.7.1. No caso de transferência para um atendente, todo o histórico do atendimento do bot deverá ser repassado para o atendente, visando continuidade do atendimento, da mesma maneira como se estivesse sendo transferido por outro atendente.

1.25.8. Realizar a implementação da automação de ações, como se fosse um operador, para obtenção de informações a serem passadas aos clientes;

1.25.9. Os fluxos de conversação implementados na solução deverão ter suporte para integração com assistentes virtuais via API REST ou Web Services;

1.25.10. A CONTRATADA deve ter profissional em seu quadro de funcionário com experiência para realizar a curadoria da base de perguntas e respostas que serão utilizadas pelo sistema de atendimento nos canais da Solução;

1.25.11. A SOLUÇÃO deverá possibilitar a criação de fluxos de atendimento, por meio de programação de árvores de decisões e perguntas de esclarecimento e de direcionamento dos usuários;

1.25.12. Deverá ser possível a administração da árvore de decisão mapeada e a reclassificação de questões não respondidas ou respondidas erroneamente, como forma de aumentar o aprendizado e melhorar a assertividade do Assistente Virtual cognitivo, sem a necessidade de intervenção da CONTRATADA;

1.25.13. A CONTRATADA deverá realizar o mapeamento de fluxos de atendimento necessários para implementação dos processos de negócio do CONTRATANTE na SOLUÇÃO, nos diversos canais e plataformas;

1.25.14. A SOLUÇÃO deverá possuir a funcionalidade de análise de mensagens enviadas pelos usuários para melhor encaminhamento do fluxo do atendimento;

1.25.15. A SOLUÇÃO deverá permitir o uso de personas e avatares definidos pelo CONTRATANTE assim como botões, links, imagens e emojis quando compatível com o canal/plataforma;

1.25.16. Com o assistente virtual, os usuários poderão solicitar informações sobre os chamados abertos, abertura de chamados, informações sobre outros sistemas.

## **1.26. Tempo Estimado de Espera**

1.26.1. A solução deverá ter mensagens de Tempo Estimado de Espera para os clientes em fila, disponibilizando informações como: tempo estimado de espera; número correspondente à posição do cliente na fila; opção de agendar um retorno de chamada, dentre outras.

1.26.2. A solução deverá permitir a definição de estratégias de roteamento condicionais com base em métrica do tempo médio de espera.

## **1.27. Motor de Decisão**

1.27.1. Prover recurso de motor de decisão de forma a centralizar as regras de negócio, disponibilizando as mesmas de forma consistente através de todos os pontos de contato do cliente;

1.27.2. Prover a dinamização dos menus de atendimento baseado no perfil ou no contexto do cliente, tais como: clientes em atraso com pagamentos, situação cadastral e etc;

1.27.3. Prover de forma segura a centralização das regras de negócio e garantir a independência das áreas de negócio e TI para implementação e manutenção de regras;

1.27.4. Implementar API para acesso de aplicações externas, onde as regras a serem aplicadas seriam geradas em outro sistema, como CRM por exemplo, e estas seriam aplicadas dentro do contexto da solução, com o mesmo poder de influência na solução que teriam se fossem configuradas através da interface do motor de decisão da própria solução;

1.27.5. Implementar diversas esteiras de atendimento, conforme o cliente, o perfil do cliente, o produto selecionado, dentre outros parâmetros a serem definidos;

1.27.6. Permitir o provimento de serviço de transferência dos dados informados pelo cliente por meio de qualquer um dos canais de entrada, para quaisquer outros canais, sem prejuízo dos dados fornecidos quando da transferência;

1.27.7. Capacidade de manter os dados da chamada em um ponto centralizado para que os diversos componentes da solução tenham acesso às informações necessárias;

1.27.8. Possuir chave única de atendimento para seu registro, independente das transferências ou mudanças de meio de acesso ocorridas ao longo do mesmo processo de atendimento.

### 1.28. Pesquisa de Satisfação (Feedback)

1.28.1. Permitir ao final do atendimento ou após o envio de resposta ao cliente ser solicitado ao cliente participação na pesquisa de satisfação;

1.28.2. Permitir que as pesquisas possam ser realizadas em quaisquer meios de acesso, respeitando as suas peculiaridades de maneira automática, via chatbots ou via atendente. Por exemplo, se o meio de acesso for voz, a pesquisa poderá ser feita por vocalização na URA. Se for por chat, apresentado o formulário para preenchimento do cliente, se for por e-mail, acesso a um link com um formulário web ou incluído na mensagem, de maneira que se houver resposta do cliente, esta seja computada na solução. No caso do SMS, o feedback deve ser registrado por meio da resposta do cliente ao SMS. No caso do Whatsapp/Telegram, por meio de bot ao final do atendimento;

1.28.3. O processo de pesquisa deverá ser parametrizável.

1.28.3.1. A Solução deverá possuir formulários nativos e customizáveis, de avaliação de atendimentos de voz, texto e vídeo;

1.28.3.2. Os formulários de avaliação devem permitir diversas estruturas de campos, incluindo campos de itens que são ativados mediante resposta do item anterior.

1.28.4. A pesquisa e as respostas fornecidas pelo cliente devem ficar vinculadas à demanda aberta pelo cliente e serem contabilizadas na Solução para fins estatísticos de avaliação das campanhas, dos atendentes, dos produtos questionados.

1.28.4.1. No caso dos atendentes, tais avaliações deverão compor o currículo dos mesmos, de maneira a serem apresentados como indicadores de desempenho e guardadas como histórico para avaliações do atendimento.

1.28.5. Tais informações podem ser acessadas em dashboards e painéis, conforme configuração solicitada;

1.28.6. A SOLUÇÃO deverá possuir a capacidade de habilitar/desabilitar o mecanismo de pesquisas de satisfação para um produto/serviço específico ou para um canal, conforme definição;

1.28.7. A SOLUÇÃO deverá possuir mecanismo de pesquisas de satisfação referente ao atendimento prestado em sua própria interface, conforme compatibilidade do canal/plataforma.

### 1.29. Linguagem Natural

1.29.1. A SOLUÇÃO deve ser capaz de responder a uma diversidade de perguntas de acordo com os conteúdos definidos, correlacionando perguntas e respostas realizadas durante o atendimento de forma a garantir a compreensão da intenção do usuário na utilização do serviço;

1.29.2. A SOLUÇÃO deve obter a real compreensão da intenção e extrair entidades das mensagens enviadas pelos usuários, utilizando componentes de Inteligência Artificial (IA) Generativa através do chatbot para processamento de NLU (Natural Language Understanding) e NLP (Natural Language Processing) e utilize mecanismos de aprendizado de máquina (Machine Learning);

1.29.3. A SOLUÇÃO deverá permitir, a partir do uso de métodos de Inteligência Artificial (IA) Generativa, o reconhecimento e interpretação da linguagem natural prezando pela coerência no contexto da conversa, com memória e lógica para escolha das respostas mais apropriadas para cada pergunta;

1.29.4. Deverá, ainda, através da aplicação de Inteligência Artificial (IA) Generativa e aprendizado de máquina, possibilitar a constante evolução do entendimento da linguagem do usuário, de seu contexto, de sua intenção (intent) na realização de perguntas, bem como das respostas fornecidas, páginas de direcionamento e web links de referência;

1.29.5. A solução deverá permitir aos usuários a elaboração de perguntas para interação com o Assistente Virtual Inteligente utilizando “linguagem natural”, em língua Portuguesa Brasileira;

1.29.6. A solução deverá ser capaz de tratar linguagem coloquial, gírias e regionalismos, neologismos e tolerância a erros de grafia com propósito de buscar o real entendimento da intenção dos usuários ao efetuarem uma pergunta ou busca por conteúdo;

1.29.7. O modelo de Linguagem Natural ofertado pela solução deverá ser parametrizável contemplando vocabulário, conceitos e termos para prover um atendimento o mais humanizado possível ao usuário e permita a customização de vocabulário específico.

### **1.30. Unidade de Resposta Audível (URA)**

1.30.1. Deverá ser disponibilizada a URA, com recursos para a criação de mensagens dinâmicas para divulgação conforme interesse da CONTRATANTE;

1.30.2. A solução deverá assegurar capacidade simultânea de atendimento automatizado (URA e/ou Agente Virtual) proporcional à demanda de Posições de Atendimento (PAs) do CONTRATANTE ADERENTE, garantindo o atendimento integral aos requisitos deste Termo de Referência, independentemente do modelo de licenciamento, arquitetura ou tecnologia adotada, inclusive portas físicas, sessões simultâneas, concorrência ou modelo elástico em nuvem;

1.30.3. Permitir no primeiro menu de opções, o item de contato com o atendente;

1.30.4. Realizar o desenho ou redesenho da árvore de voz em conjunto com a CONTRATANTE e a programação e gravação da fraseologia será por conta da CONTRATADA;

1.30.5. A CONTRATADA deverá, a partir dos roteiros de atendimento definidos pela CONTRATANTE, sugerir a construção e/ou alteração contínua de árvores de voz no formato Portal de Voz, com as melhores práticas linguísticas e de comunicação digital, visando à racionalização dos atendimentos;

1.30.6. Permitir a opção de contatar o atendente em todas as subdivisões da URA;

1.30.7. Permitir que todos os números 0800, tri-dígitos, e demais números, serão atendidos diretamente na plataforma contratada, para o atendimento da URA e gravação de chamadas, e só serem encaminhados para as PAs as ligações destinadas aos respectivos atendentes, localizadas nos PCSs do Contratante Aderente;

1.30.8. Permitir que a programação da URA (árvore de voz, fraseologia, etc.) possa ser modificada, por cada Contratante Aderente, quando o mesmo considerar necessária a alteração da árvore de voz, durante a vigência do contrato;

1.30.9. Permitir que fraseologias criadas, fornecidas e personalizadas pelo Contratante Aderente sejam disponibilizadas na URA;

1.30.10. Permitir a integração com base de dados;

1.30.11. Vocalizar mensagens fornecidas pela CONTRATANTE para o usuário que aguarda atendimento;

1.30.12. Permitir pesquisa de satisfação junto ao usuário ao término do atendimento humano, quando solicitado pela CONTRATANTE;

1.30.13. Ser capaz de vocalizar a posição do usuário na fila e o tempo estimado para o atendimento;

1.30.14. O canal ou sessão de atendimento automatizado deverá ser liberado imediatamente para recebimento de novas chamadas após a transferência da chamada atual;

1.30.15. A solução deverá gerenciar a disponibilidade dos canais ou sessões de atendimento automatizado, exibindo notificações em caso de indisponibilidade total ou parcial e impedindo o encaminhamento de chamadas enquanto a falha não for sanada;

1.30.16. Disponibilizar relatórios via sistema Web e acessível pelos navegadores mais comuns (Google Chrome, Mozilla Firefox, Microsoft Edge e Safari) com informações de desempenho dos atendimentos realizados, apresentando indicadores que permitam a CONTRATANTE a gestão das informações contidas nas chamadas e atendimentos, em tempo hábil, mantendo assim a qualidade do serviço e diagnóstico da situação por navegação;

1.30.17. Permitir a emissão de relatórios estatísticos referentes a um período contendo, no mínimo:

1.30.17.1. Quantidade de ligações recebidas pela URA;

1.30.17.2. Quantidade de ligações finalizadas pela URA;

1.30.17.3. Quantidade de ligações transferidas para atendimento humano;

1.30.17.4. Quantidade das perdas de ligações na URA discriminadas por motivos;

1.30.17.5. Quantidade das perdas de ligações na transferência para o atendimento humano discriminado por motivos;

1.30.17.6. Informação percentual/absoluta das opções escolhidas;

1.30.17.7. Tempos totais e médios;

1.30.17.8. HMM (Hora de Maior Movimento) e DMM (Dia de Maior Movimento);

1.30.17.9. As opções escolhidas de navegação e a sequência de serviços consultados;

1.30.17.10. Quantidade de ligações, por número e telefone;

1.30.17.11. Quantidade de ligações por número de telefone, por navegação e por árvore da URA.

1.30.18. Apresentar mensagens síncronas, ou seja, toda mensagem deverá ser apresentada ao usuário a partir do seu início, com exceção da música para chamadas em espera ou estacionadas;

1.30.19. Possuir recurso “cut thru”, ou seja, quando for detectada uma discagem do usuário durante o diálogo, o prompt de voz será interrompido de imediato, e a execução desviada para o passo seguinte;

1.30.20. A capacidade de atendimento automatizado deverá ser dimensionada pela CONTRATADA de forma a não comprometer os níveis mínimos de serviço contratados, sendo vedada a limitação artificial de sessões simultâneas que impacte a experiência do usuário.

#### 1.30.21. Comandos de voz

1.30.21.1. Solução tecnológica aplicada a comandos emitidos por voz na URA, em procedimento de conversação natural no diálogo indivíduo-máquina, para aplicação de síntese da fala para texto;

1.30.21.2. Para iniciar conversação com o cliente, identificando na mesma os comandos para atender a demanda de serviço, entregando a informação buscada, encaminhando à célula de atendimento humano conforme assunto reconhecido ou executando operação solicitada;

1.30.21.3. Para aprimoramento e desenvolvimento da estrutura de diálogo, para incorporação de características regionais e temporais de conversação, bem como revisão de conteúdo e forma do diálogo;

1.30.21.4. A solução deverá emitir questionamento inicial ao cliente, de modo a identificar seu interesse, reconhecendo na frase-resposta os comandos para a tomada de decisão e atendimento;

1.30.21.5. A solução deverá possuir dicionário base de interpretação de comandos para interação com os sistemas que atendem aos serviços e produtos constantes da árvore de atendimento;

1.30.21.6. Deverá possuir recursos que reconheçam palavras de estrutura simples e sequências complexas;

1.30.21.7. Reconhecer o idioma português (Brasil), com capacidade de expansão do vocabulário necessário às funcionalidades da solução;

1.30.21.8. A solução deverá permitir o acesso aos recursos de forma dinâmica;

1.30.21.9. A solução deverá resolver as requisições de conteúdo padrão existentes nas emissões de informação do tipo: endereços, horários, datas, orientações pré-determinadas de cunho geral.

1.30.21.10. A Solução deverá permitir o encaminhamento de chamadas para o operador ou bot com o perfil adequado ao atendimento identificado na conversação;

1.30.21.11. A Solução deverá suportar ambiente de simulação (em modo de laboratório) do fluxo da chamada considerando roteiros (scripts) de reconhecimento de voz;

1.30.21.12. A Solução deverá ser configurável por funcionalidades e parâmetros;

1.30.21.13. A Solução deverá reconhecer solicitação do cliente antes ou no meio da mensagem, seja por ação de digitação ou por reconhecimento de voz, finalizando a mensagem e dando continuidade no atendimento conforme comandos emitidos pelo cliente.

#### 1.30.22. Speech to text e text to speech

1.30.22.1. A Solução disponibilizada deverá implementar a funcionalidade de speech to text, responsável pela conversão das informações vocalizadas pelos clientes e atendentes em chamada, para texto.

1.30.22.1.1. O texto transcrito deverá ser disponibilizado em meio digital, em formato TXT, DOC ou CSV;

1.30.22.1.2. Estas informações deverão estar acessíveis no frontend do supervisor, assim como deverá permitir ser disponibilizado para o cliente através de e-mail;

1.30.22.1.3. A transcrição deverá ser disponibilizada em até vinte e quatro horas após o atendimento;

1.30.22.1.4. A realização da transcrição poderá também ser realizada sob demanda à solução, de qualquer arquivo de áudio gerado na solução;

1.30.22.1.5. Os textos transcritos poderão ser utilizados pela solução para fins de avaliação de qualidade do atendimento, para fins de treinamento dos atendentes, prova do atendimento realizado e para obtenção de informações adicionais sobre o humor do cliente, dentre outras informações possíveis de serem extraídas da interação;

1.30.22.1.6. O texto transcrito não substitui a necessidade de gravação das chamadas de voz.

1.30.22.2. Deverá prover sintetizador de voz que possibilite a conversão de texto em voz, com tecnologia de text to speech (TTS).

1.30.22.2.1. TTS será utilizado em operações de Agente Virtual ou URA Ativa, para orientar o cliente a uma operação, cuja decisão deverá ser interpretada por meio de comando ou reconhecimento da voz do cliente.

## 2. Itens de serviço

### 2.1. Medição das Unidades de Serviço

2.1.1. Para fins de medição, entrega e faturamento, as unidades dos serviços contratados deverão observar a seguinte correspondência, conforme especificações do Termo de Referência e valores estabelecidos na Tabela de Preços (Anexo B):

2.1.1.1. Para os serviços de Contact Center com Recurso de Voz, com Recurso de WhatsApp, com Recurso de Redes Sociais e de Comunicação por Vídeo ou Vídeo-Chamada, a unidade de entrega contratada será a Posição de Atendimento (PA).

2.1.1.2. Para os serviços de Automatizações e Integrações – Consultoria Inicial e Implantação, a unidade de entrega contratada será a Unidade de Serviço Técnico (UST).

## 2.2. Serviço de Comunicação por vídeo ou vídeo-chamada

2.2.1. Suportar comunicação e implementar transcodificação de mídia com os codecs de áudio padrões de mercado, com, no mínimo os G.711 (μ-law e a-law);

2.2.2. Suportar protocolos de vídeo: obrigatoriamente H.264 ou H.265 ou VP8 ou AV1 (ou superior), para fins de interoperabilidade com soluções baseadas em WebRTC;

2.2.3. Suportar a configuração mínima de resolução de vídeo XGA (1024x768).

### 2.2.4. Automatizações e Integrações

2.2.4.1. A solução deve permitir a integração dos Serviços de Infraestrutura de Tecnologia para Contact Center em Nuvem com sistemas externos (CRM, Banco de Dados etc.), dos CONTRATANTES Aderente.

2.2.4.1.1. A Solução deve permitir se integrar de forma que a abertura de demandas internas e consulta de demandas (em andamento ou finalizada) possa ser realizada, seja por voz ou por texto, sem a necessidade de envolvimento de uma atendente humano, utilizando recursos de IA generativa.

2.2.4.2. A Solução deve permitir solicitar e enviar todas as informações necessárias para a abertura da demanda interna e realizar consultas por meio de parâmetros pré-definidos.

2.2.4.3. A Solução deve permitir a criação de autoatendimento por voz ou texto que permita realizar ações de forma automática de acordo com a demanda do cliente.

2.2.4.3.1. Tal integração deverá ser implementada via API REST ou Web Services.

## 2.3. Serviço de Contact Center com Recurso de Voz

### 2.3.1. E-mail

2.3.1.1. Componente da solução responsável pelo tratamento dos e-mails entrantes ou iniciados pelos agentes nas campanhas ativas, incluindo confirmações de recebimento e respostas automáticas, bibliotecas com templates configuráveis, roteamento e enfileiramento inteligente baseados nas habilidades dos agentes, na fila de espera e em informações do cliente (segmento, por exemplo) ou em qualquer outro parâmetro definido;

2.3.1.2. Todos os e-mails a serem tratados pela solução serão entregues ou enviados com o endereço de e-mail da CONTRATANTE através de integração SMTP;

2.3.1.3. A solução deverá suportar receber e enviar os e-mails em uma ou mais caixas postais, conforme configurado na solução, devendo ser capaz de transformar as demandas em e-mail e vice-versa, conforme parâmetros e fluxos definidos pela CONTRATANTE para roteamento e tratativa das interações;

2.3.1.4. Permitir o recebimento de E-mails através de caixas-postais, e a resposta do E-mail deverá ser realizada pela mesma caixa-postal ou por outra caixa-postal aderente ao serviço tema constante no assunto ou corpo do e-mail;

2.3.1.5. Tratar mensagens de correio eletrônico com capacidade mínima suportada de 25 MB (vinte e cinco megabytes) por mensagem, devendo a solução permitir configuração do limite de tamanho, para valores superiores ou inferiores, conforme a capacidade técnica do servidor de e-mail da CONTRATANTE e as diretrizes definidas pelo CONTRATANTE ADERENTE.

2.3.1.6. O atendimento à funcionalidade de tratamento de e-mail deverá ocorrer, por meio de mensagens geradas a partir de formulários disponíveis nos sites web da CONTRATANTE ou E-mails enviados diretamente pelos clientes que sejam roteadas pelos servidores da CONTRATANTE para as caixas-postais configuradas na solução.

2.3.1.7. Utilizar e-mail na formatação HTML de texto e imagem, permitindo o envio de e-mails com arquivos anexos.

2.3.1.8. Possuir templates oriundos de biblioteca(s) pré-definida(s), que poderão sofrer alterações de acordo com as necessidades da CONTRATANTE.

2.3.1.9. Implementar recurso para respostas automáticas personalizadas aos clientes que fizerem contato com caixas postais específicas a serem definidas pela CONTRATANTE.

2.3.1.10. Permitir a geração de mensagens automáticas para o mailing indicado ou mesmo em resposta a uma chamada realizada através de outro meio.

2.3.1.11. Possuir a função de programação para enviar mensagens de recebimento para cada fila de atendimento de e-mail.

2.3.1.12. Deverá permitir o envio de arquivos anexos: .jpg, .jpeg, .tiff, .png, .gif, .pdf, .csv, .doc/docx, .xls/xlsx, .txt, .ods, .gdoc, .gsheet, .html, .zip/rar e outros portadores de conteúdo descritivos.

2.3.1.13. Permitir que um agente armazene uma resposta parcial (rascunho) para um E-mail e transfira-a para um outro agente ou serviço que complete a resposta, com autorização de usuário cujos perfis possuam direitos de configuração.

2.3.1.14. Permitir ao administrador do sistema a criação templates de e-mails para cada fila de atendimento do Contact Center.

### 2.3.2. SMS

2.3.2.1. A solução deverá implementar interação com os clientes através de troca de SMS, via integração com sistema de envio de SMS da CONTRATANTE.

2.3.2.2. O cliente poderá receber SMS e respondê-los para a solução, devendo estes ser convertidos internamente em demanda, para tratamento pela ferramenta de tratamento de demandas.

2.3.2.3. A solução deverá preparar as interações por SMS para obedecerem a todas as normas deste meio, inclusive com relação ao seu tamanho.

2.3.2.3.1. As informações citadas poderão ser utilizadas pela solução para realização de respostas automáticas ou passadas para um atendente.

2.3.2.4. Deverá implementar possibilidade de encaminhar mensagens SMS como alerta, informação, protocolo de atendimento, pesquisas de satisfação, em campanhas ou nas situações indicadas no motor de decisões ou em opções realizadas pelo Cliente, independente do meio de acesso dele;

2.3.2.5. Deve tratar respostas, conforme parâmetros e regras definidas, tendo em vista situações em que cliente possa ter digitado as respostas fora do padrão esperado;

2.3.2.6. A solução deve permitir a construção de árvore de decisão a partir do envio e recepção de SMS, podendo conter quantas divisões forem necessárias;

2.3.2.6.1. Solução controlará a qual fluxo de mensagens cada SMS está vinculado, devendo permanecer no máximo 1 fluxo ativo. Ao enviar novo SMS de fluxo distinto, o fluxo anterior é interrompido.

2.3.2.7. A solução deve disponibilizar modo laboratório no qual é possível testar as árvores de decisão antes de disponibilizá-las aos clientes.

### 2.3.3. Tratamento de Voz

2.3.3.1. O acesso do cliente por voz se dará por meio de chamadas telefônicas diretamente realizadas para números específicos.

2.3.3.2. A solução deve permitir a comunicação de Voz entre os agentes e usuários administrativos, bem como recepção e discagem de chamadas externas.

2.3.3.3. Deverá implementar a identificação do número de A (originador da chamada) e realizar análises e buscas de informações com base nesses números.

2.3.3.3.1. Caso o número identificado pertença a cliente já atendido na Solução, o frontend de atendimento deverá ser apresentado ao atendente com todas as informações disponíveis para aquele cliente;

2.3.3.3.2. A Solução deve ser capaz de tratar o cliente de forma personalizada ainda na URA, permitindo vocalização de mensagens e opções específicas de atendimento.

2.3.3.4. Deverá permitir bloquear chamadas recebidas de números da blacklist, conforme parametrização.

2.3.3.5. Permitir o rastreamento de uma chamada de entrada, independente da conexão com a operadora, com todo caminho e atendimentos ocorridos até a sua desconexão.

2.3.3.5.1. A referência do sistema de voz é o usuário da Solução e não o ramal. Todas as identificações e ações de telefonia deverão sempre estar associadas aos usuários dos mesmos ou clientes, logados na solução,

2.3.3.5.2. O ramal telefônico pode ser atribuído a qualquer usuário pela Solução, de maneira dinâmica, conforme configuração direcional realizada na Solução.

2.3.3.6. Deverá permitir implementar, por configuração, facilidades de telefonia, independentemente do ramal alocado para o usuário da Solução tais como: acesso à discagem e uso de linhas externas assim como possibilidade de discagem para números de celular.

2.3.3.7. Possibilitar o uso para todos os usuários da solução, mas configuráveis, de acordo com os usuários, de maneira granular, facilidades básicas tais como: ativação automática do serviço noturno em horário pré-programado; chamada externa transparente ao usuário; chamada em espera ou rechamada; conferência com no mínimo 3 (três) participantes (interna e externa); consulta de chamada em espera; consulta pendular com alternância entre duas ligações; desvio externo local, celular, DDD e DDI; desvio imediato, quando não atende, sobre tom de ocupado (siga-me); estacionamento de chamadas para no mínimo uma chamada; intercalação de chamadas; não perturbe; transferência nas chamadas de entrada e de saída, etc.

2.3.3.8. Qualquer função de roteamento de chamada deverá ser automática e transparente ao usuário.

#### 2.3.4. Discagem Automática

2.3.4.1. A Solução deverá implementar a possibilidade de realização de discagem automática, quando o meio de contato com o cliente for através de voz, gerenciada plenamente pela solução.

2.3.4.2. Implementar os seguintes tipos, configuráveis:

2.3.4.2.1. Discagem sob demanda: o agente revisa os dados e pede para iniciar a discagem;

2.3.4.2.2. Discagem progressiva: uma discagem é iniciada cada vez que um agente fica disponível, sem sua intervenção;

2.3.4.2.3. Discagem preditiva: uma discagem é iniciada antes que um agente fique disponível, baseando-se na expectativa que um estará livre em pouco tempo.

2.3.4.3. Deverá atender aos modos de operação:

2.3.4.3.1. Preview Dialer, deverá exibir para o atendente os dados do cliente antes de realizar a discagem e permitir que ele decida se quer ou não fazer aquela ligação, de modo que o atendente não precise digitar o número de telefone e poderá se preparar para o atendimento antes de contatar o cliente.

2.3.4.3.2. Power Dialer, deverá realizar as discagens sempre que um atendente estiver disponível e, através de uma parametrização de “over-dial”, consulta um “rate” definido, manualmente, com a quantidade de ligações necessárias para que a operação não fique ociosa.

2.3.4.3.3. Predictive Dialer, deverá possuir capacidade de parametrizações, por meio de algoritmo estatístico, capaz de analisar os dados históricos das discagens de cada campanha e prever a quantidade de discagens necessárias para obter a melhor performance;

2.3.4.3.4. No modo Preditivo, deverá ter a capacidade de analisar variáveis como: Tempo Médio de Atendimento (TMA); Tempo Médio de Operação (TMO); Tempo Médio de Fila (TME); Quantidade de agentes disponível; Quantidade de agentes em ligação; Taxa de ligações completadas;

2.3.4.3.5. Todos os contatos deverão ser registrados, apresentando todas as estatísticas das campanhas, inclusive as tentativas sem sucesso.

### 2.3.5. Call-back

2.3.5.1. A Solução deverá prover chamadas de retorno ao cliente nos casos de abandono da fila, quando em espera, ou por interrupção de atendimento não finalizado;

2.3.5.2. Possuir a funcionalidade que permita aos clientes agendar uma chamada automática dos atendentes conforme regras definidas pela CONTRATANTE;

2.3.5.3. Permitir o cliente optar por um horário, a ser escolhido e identificado pelo cliente para o retorno do seu contato, quando da emissão da mensagem de tempo estimado de espera,

2.3.5.4. A solução deverá registrar e retornar a chamada ao cliente, de maneira automática e com questionamento customizado, de forma que, caso o cliente aceite, a chamada será direcionada a um atendente previamente disponibilizado pela inteligência da solução, quando houver o abandono de chamada antes do atendimento.

2.3.5.4.1. Tal processo deverá ser baseado nas regras de negócio configuradas, balizadas pelo cliente, nas habilidades do agente (skill), nas filas e outros parâmetros.

2.3.5.5. Deverá ser possível identificar o sinal de ocupado ou ausência (não atendimento), reinserindo a chamada na fila de retorno de chamada;

2.3.5.6. A solução deverá apresentar ao atendente, no atendimento de um retorno de chamada, informações com os dados pertinentes àquele retorno de chamada, como se fosse um atendimento receptivo;

2.3.5.7. Deverá ser permitido o retorno da chamada, preferencialmente para o mesmo atendente.

### 2.3.6. Transbordo/Transferência de Chamadas

2.3.6.1. A solução deverá implementar transbordo/transferência de chamadas, independentemente do meio de acesso.

2.3.6.1.1. A SOLUÇÃO deve disponibilizar a funcionalidade de transferência do atendimento para um atendente humano, transferindo o contexto e informações do atendimento realizado.

2.3.6.2. Dentre as possibilidades de transbordo possíveis, segue um exemplo a ser realizado:

2.3.6.2.1. A chamada do cliente X, de acordo com as regras estabelecidas, deverá ser direcionada para uma equipe de atendimento e para uma fila específica, por exemplo, fila A. Nesta fila, a chamada deverá ser encaminhada para o atendente Y. Caso Y esteja ocupado, deverá ser enviado para o atendente Z, e assim por diante, conforme determinado pelas regras;

2.3.6.2.2. Caso nenhum atendente da lista inicial esteja disponível, a chamada é direcionada para uma mensagem informando que todos os atendentes daquele grupo estão ocupados e se ele gostaria de receber uma chamada de retorno, ou, aguardar ser atendido por outro canal de atendimento.

2.3.6.2.3. Caso agende o retorno, a solução deverá prover o ajuste para que este retorno seja implementado na fila de retorno do atendente Y ou de sua equipe, realizando a chamada no horário predeterminado, para atendimento.

2.3.6.2.4. Caso o cliente opte por manter-se na chamada, esta será encaminhada para um atendente com o mesmo perfil do Y em outro grupo de atendimento, pré-cadastrado previamente como opção de roteamento, realizando o mesmo ciclo de buscas nos perfis. Caso estejam também todos ocupados, a Solução deverá buscar o primeiro atendente livre com perfil equivalente ao Y em todas as filas para atender a chamada.

2.3.6.2.5. Caso nenhum perfil esteja disponível, a solução informa ao cliente que ele deverá aguardar na fila, ofertando nova escolha de agendamento no mesmo procedimento descrito nesse item;

2.3.6.2.6. Esta fila estará associada ao atendimento do grupo onde o Atendente Y encontra-se inserido.

2.3.6.3. As transferências de chamadas entre filas/sites deverão registrar na origem e destino.

## **2.4. Serviço de Contact Center com recurso WhatsApp**

2.4.1. A Solução deve permitir atendimento a clientes por meio de WhatsApp da empresa Meta;

2.4.2. Deverá ser fornecido assinatura de números válidos para integração do assistente Cognitivo com o aplicativo de mensagem WhatsApp, para atendimento ao público em geral, podendo a CONTRATANTE definir os números entre os disponibilizados em sua faixa de numeração de telefonia fixa;

2.4.3. Efetuar a entrega das demandas a serem atendidas para grupos específicos de atendimento, parametrizáveis pela CONTRATANTE.

2.4.4. A solução deve permitir que o cliente seja respondido pela própria solução, sem necessidade de outros tipos de acesso

2.4.5. Deverá possuir recursos para configurar filtros baseados em regras de negócio.

## **2.5. Serviço de Contact Center com recurso Redes Sociais**

2.5.1. A solução deve permitir, no mínimo, o atendimento a clientes por meio das seguintes redes sociais: Facebook, Instagram, X (antigo Twitter) e LinkedIn.

2.5.2. A solução deve prover os adaptadores para os principais serviços de Mídia Social existentes no mercado (Facebook, Instagram etc.). A função dos adaptadores será de monitorar, verificando as atividades das redes sociais relativas à CONTRATANTE.

2.5.3. A solução deverá prover recursos para, por meio de regras específicas, efetuar o monitoramento dos posts por meio de palavras-chave, frases, pedaços de palavras e múltiplas palavras, transformando-as em demandas internas a serem tratadas por meio de ferramenta de tratamento de demandas.

2.5.3.1. Classificar o sentimento no assunto tratado como positivo, neutro ou negativo.

2.5.4. Permitir análise nas redes sociais que captem palavras com cunhos sociais, com maior visibilidade, conforme parametrizado pela CONTRATANTE.

2.5.5. Efetuar a entrega das demandas a serem atendidas para grupos específicos de atendimento, parametrizáveis pela CONTRATANTE.

2.5.6. A solução deve permitir que o cliente seja respondido pela própria solução, sem necessidade de outros tipos de acesso à rede social.

2.5.7. Deverá possuir recursos para configurar filtros baseados em regras de negócio.

### **2.5.8. Troca de Arquivos**

2.5.8.1. A solução deverá suportar, no mínimo, o envio e recebimento de arquivos por E-mail, mídias de Chat (Instagram Direct Messenger, Messenger do Facebook, DM do Twitter, WhatsApp, Telegram).

2.5.8.2. A solução deverá prover um ambiente de armazenamento temporário de arquivos, visando realizar as trocas de arquivos entre os clientes e os atendentes de forma a não armazenar esses arquivos no ambiente da contratante;

2.5.8.3. A Solução deve permitir, no mínimo, suporte os formatos de arquivos PDF, JPG, JPEG, PNG, DOC/DOCX, TXT, GIF, CSV, XLS/XLSX, MP3, MP4 e ZIP/RAR, sendo desejáveis também os formatos TIFF, GDOC e GSHEET.

2.5.8.4. A solução deve suportar receber arquivos de áudio via WhatsApp e Telegram para escuta pelo atendente de forma a tratar mensagens de áudio dentro da própria solução.

#### **2.5.9. Tratamento de Chat e Instant Messenger**

2.5.9.1. Interface de comunicação responsável pela interação entre a CONTRATANTE e seus clientes, tanto internos quanto externos e deverá ser disponibilizada por meio de API;

2.5.9.1.1. A Solução deverá disponibilizar API para utilização do chat pela CONTRATANTE em seus aplicativos e/ou sites web, visando disponibilização de interface para o cliente acessá-lo via browser comuns de mercado (Microsoft Edge, Mozilla Firefox, Google Chrome ou Safari, versão mais atual), seja via PC, notebook ou telefone móvel.

2.5.9.2. A Solução deve disponibilizar atendimento nos instant messengers, tais como WhatsApp; Facebook Messenger, Telegram, Instagram e outros;

2.5.9.3. Deverá permitir rápido acesso às mensagens mais utilizadas;

2.5.9.4. Utilizar método de criptografia que codifique os dados transmitidos entre o transmissor e o receptor e vice-versa, de forma a inviabilizar a monitoração por terceiros;

2.5.9.5. Permitir a configuração de aviso ao agente de atendimento, por sinal sonoro ou por interface de pop-up da tela de atendimento do agente quando o cliente solicita atendimento online, ou outra forma de destaque da solicitação que venha a disponibilizar;

2.5.9.6. Permitir ao administrador criar notificações automáticas para cada fila de atendimento. A “notificação automática” é um recurso que informa ao cliente mensagens, baseadas em análises e categorização e sem a interação de um atendente;

2.5.9.7. Permitir a realização de, pelo menos, 5 (cinco) sessões simultâneas de chat por operador ativo, conforme parametrização da CONTRATANTE;

2.5.9.8. Utilizar sessões com segurança SSL;

2.5.9.9. Permitir configurar mensagens de informação para o cliente, automáticas ou não;

2.5.9.10. Permitir que o atendente inicie uma chamada de outro meio, a partir de uma chamada corrente;

2.5.9.11. Permitir a transferência da tela do atendimento para atendimento de 2º nível, transferindo o histórico de conversação para o atendente de 2º nível e notificando o cliente;

2.5.9.12. Permitir a parametrização de informações consideradas confidenciais que serão digitadas pelo cliente e que serão ocultadas para o atendente (exemplo: número do CPF);

2.5.9.13. Permitir a comunicação por meio de áudio, vídeo, texto e/ou imagens, podendo esta forma de comunicação ser alterada no decorrer da conversa.

#### **2.6. Serviço de Automatizações e Integrações - Consultoria Inicial**

2.6.1. A CONTRATADA em conjunto com a ATI deverá, em até 90 (noventa) dias após a assinatura do Contrato Mater, definir todos os modelos das documentações a serem produzidas neste serviço de Consultoria inicial para a implantação de Automatizações e Integrações com o serviço de Contact Center;

2.6.2. Não será de responsabilidade da CONTRATADA os ajustes e implementações necessárias nos sistemas da CONTRATANTE para realizar a integração com o serviço de Contact Center, sendo de sua responsabilidade os ajustes e implementações necessárias apenas no serviço de Contact Center, como também dar o apoio necessário à

CONTRATANTE, ou empresa por ela contratada, com informações necessárias para o sucesso da integração e/ou automatização;

2.6.3. Em até 10 dias corridos após o envio da Ordem de Serviço deverá ocorrer a reunião de abertura projeto entre a CONTRATADA e a CONTRATANTE para levantamento dos requisitos e intenções definidas pela CONTRATANTE;

2.6.4. A CONTRATADA deverá elaborar toda a documentação com as especificações necessárias para a implantação das Automatizações e/ou Integrações solicitadas pela CONTRATANTE;

2.6.5. Caso a CONTRATANTE opte por utilizar os serviços de automatizações e integrações – Implantação, presente neste contrato, o material produzido também deverá conter a quantidade de USTs necessárias para sua execução, de acordo com a Tabela 3 – Referência de Quantidade de UST.

2.6.6. Todas as documentações elaboradas deverão ser entregues à ATI para sua avaliação e possível aprovação. A ATI poderá exigir a complementação de informações, caso achem necessário, tendo a CONTRATADA obrigação em atendê-las no prazo definido pela ATI.

## **2.7. Serviço de Automatizações e Integrações - Implantação**

2.7.1. Esse serviço terá contratação opcional, podendo a CONTRATANTE fazer uso de outros contratos que já possua para esta finalidade.

2.7.2. A CONTRATADA deverá prestar todo o suporte necessário para a CONTRATANTE, como também à empresa contratada por esta, para desenvolver a integração do sistema da CONTRATANTE com o serviço de Contact Center;

2.7.3. A CONTRATADA deverá customizar o Assistente Virtual Cognitivo para que, em tempo real, a inteligência artificial identifique e compreenda as intenções e conduza o atendimento das necessidades manifestadas pelo Usuário Externo que venha a estabelecer contato com a CONTRATANTE;

2.7.4. A CONTRATADA deverá realizar a personalização de design, carga de conteúdo e fluxos de atendimento, com base em informações fornecidas pela CONTRATANTE;

2.7.5. A implantação deverá ocorrer em até 60 (sessenta) dias após o recebimento das informações da CONTRATANTE.

2.7.6. É de responsabilidade da CONTRATADA toda a infraestrutura necessária para atendimento dos serviços, tais como: hardwares, softwares, licenças, certificados e quaisquer outros insumos necessários para a prestação do serviço durante toda a vigência do contrato.

2.7.7. A CONTRATADA deverá entregar o caderno de testes com todas as intenções definidas na reunião de abertura do projeto para que a CONTRATANTE realize a homologação do Assistente Virtual Cognitivo.

2.7.8. Após a implantação do Assistente Virtual Cognitivo, a CONTRATANTE realizará os testes de aceitação e emitirá um parecer em até 07 dias corridos, sendo considerado entregue ao atingir uma assertividade de no mínimo 70%.

2.7.9. O Assistente Virtual Cognitivo será considerado entregue se atingir o percentual mínimo de assertividade previsto no item anterior.

### **2.7.10. Implantação do Assistente Virtual Cognitivo**

2.7.10.1. Em até 15 dias corridos, após a emissão da Ordem de Serviço, deverá ocorrer a reunião de abertura projeto entre a CONTRATADA e a CONTRATANTE para levantamento dos requisitos e intenções definidas pela CONTRATANTE.

2.7.10.2. A CONTRATADA deverá customizar o Assistente Virtual Cognitivo para que, em tempo real, a inteligência artificial identifique e compreenda as intenções e conduza o atendimento das necessidades manifestadas pelo Usuário Externo que venha a estabelecer contato com a CONTRATANTE;

2.7.10.3. A CONTRATADA deverá realizar a personalização de design, carga de conteúdo e fluxos de atendimento, com base em informações fornecidas pela CONTRATANTE;

2.7.10.4. A implantação deverá ocorrer em até 90 dias corridos após o recebimento das informações da CONTRATANTE.

2.7.10.5. É de responsabilidade da CONTRATADA toda a infraestrutura necessária para atendimento dos serviços, tais como: hospedagem em nuvem pública, softwares, licenças, certificados e quaisquer outros insumos necessários para a prestação do serviço durante toda a vigência do contrato.

2.7.10.6. A CONTRATADA deverá entregar o caderno de testes com todas as intenções definidas na reunião de abertura do projeto para que a CONTRATANTE realize a homologação do Assistente Virtual Cognitivo.

2.7.10.7. Após a implantação do Assistente Virtual Cognitivo, a CONTRATANTE realizará os testes de aceitação e emitirá um parecer em até 07 (sete) dias corridos, sendo considerado entregue ao atingir uma assertividade de no mínimo 70%.

2.7.10.8. O Assistente Virtual Cognitivo será considerado entregue se atingir o percentual mínimo de assertividade previsto no item anterior.

2.7.11. Para o Serviço de Automatizações e Integrações – Implantação deve-se entender que a unidade refletida na tabela de preços (ANEXO B) a ser considerada é a UST.

### **3. Itens Serviço Técnico Especializado Sob Demanda**

#### **3.1. Condições Gerais**

3.1.1. A CONTRATADA deverá realizar manutenção no sistema com atualizações, correções, configurações e ajustes;

3.1.2. O suporte técnico deverá ser acionado via e-mail, site (com abertura de chamado) ou atendimento telefônico em horário comercial (8h às 18h de segunda-feira a sexta-feira);

3.1.3. Tempo máximo para atendimento de 24h úteis contadas a partir da solicitação;

3.1.4. Prestação de apoio na parametrização e operação do sistema junto à CONTRATANTE;

3.1.5. A solução deverá contar ainda com suporte técnico especializado para prestação de consultoria, realização de Assessment (site survey) para entendimento do ambiente da CONTRATANTE, elaboração de arquitetura, Integrações do Assistente Virtual Cognitivo com as ferramentas, sistemas e banco de dados da CONTRATANTE, criação de dashboard, dentre outras solicitações e demandas de customizações que podem ocorrer sob demanda de cada projeto.

3.1.6. O Pagamento do suporte técnico especializado será realizado por meio de UST.

3.1.7. O consumo de UST será realizado por solicitação da CONTRATANTE para a CONTRATADA, através de Ordem de Serviços com os seguintes tipos de chamado:

3.1.7.1. Chamados de Criação

3.1.7.2. Chamados de Implantação

3.1.7.3. Chamado de exclusão

3.1.7.4. Chamados de suporte.

3.1.8. Serão aplicáveis multas e glosas no caso de descumprimento dos Níveis Mínimos de Serviço, conforme Requisitos de suporte técnico e garantia, bem como no modelo de execução do contrato.

3.1.9. O valor a ser pago à CONTRATADA por cada item consumido levará em consideração a natureza e complexidade do serviço.

3.1.10. Para cada serviço foi estipulado um valor de referência em quantidades de UST ajustado conforme complexidade ou natureza.

3.1.11. A unidade de medida adotada (UST) corresponde ao esforço padronizado para determinada complexidade, independentemente da quantidade de recursos humanos alocados. O pagamento é condicionado à prestação dos serviços e atendimento aos níveis de serviços especificados.

3.1.12. A CONTRATANTE fará uso e efetuará o pagamento apenas das USTs necessárias à implementação e manutenção dos serviços que solicitar, até o limite máximo das USTs estimadas.

3.1.13. Conforme especificações de requisitos negociais do presente no Termo de Referência, será exigido o atendimento mínimo das áreas da tabela abaixo:

Serviço	Métrica
Curadoria	Hora técnica
Consultoria	Hora técnica
Assessmet (Site Survey)	Hora técnica
Plano de Arquitetura	Hora técnica
Integrações com as ferramentas	Hora técnica
Integrações com sistemas	Hora técnica
Integrações com banco de dados	Hora técnica
Criação de Dashboard	Hora técnica
Suporte Assistente Cognitivo	Hora técnica

Tabela 1 – Serviços Técnicos Especializados

3.1.14. Os valores de referência UST especificados na Tabela 3 foi ajustado de acordo com a natureza da solicitação, conforme detalhado na tabela abaixo:

Natureza da Atividades	Complexidade	Fator de ajuste no valor de referência
Criação	Alta	100%
Implantação	Média	80%
Exclusão	Baixa	60%
Suporte	Muito Baixa	50%

Tabela 2 – Natureza da tarefa

3.1.15. As relações dos serviços de suporte técnico especializado do objeto da presente contratação constam na tabela 3.

3.1.16. Esses serviços não são exaustivos, indicam essencialmente itens básicos de serviço de suporte técnico especializado.

3.1.17. A quantidade de USTs ajustada já levam em consideração o Fator de ajuste no valor de referência relacionado na tabela 2.

3.1.18. Na tabela 3 também se encontram os NMS dos chamados de complexidade alta, de média e baixa:

Descrição do serviço	Complexidade	Quantidade UST	Quantidade UST Ajustada
Curadoria	Alta	40	40
Consultoria	Alta	30	30
Assessmet (Site Survey)	Alta	24	24
Assessmet (Site Survey)	Média		19
Assessmet (Site Survey)	Baixa		14
Plano de Arquitetura	Alta	24	24
Plano de Arquitetura	Média		19
Integrações com as ferramentas	Alta	40	40
Integrações com as ferramentas	Média		32
Integrações com as ferramentas	Baixa		24
Integrações com as ferramentas	Muito Baixa		4
Integrações com sistemas	Alta	40	40
Integrações com sistemas	Média		32
Integrações com sistemas	Baixa		24
Integrações com sistemas	Muito Baixa		4
Integrações com banco de dados	Alta	48	48
Integrações com banco de dados	Média		38
Integrações com banco de dados	Baixa		28

Integrações com banco de dados	Muito Baixa		4,8
Criação de Dashboard	Alta	40	40
Criação de Dashboard	Média		32
Criação de Dashboard	Baixa		24
Criação de Dashboard	Muito Baixa		4
Assistente Virtual Cognitivo	Muito Baixa	50	5

Tabela 3 – Referência de Quantidade de UST

3.1.19. A coluna Quantidade de UST Ajustada, além de indicar a quantidade de UST que será paga a cada solicitação de OS, também refletem o prazo máximo para a sua execução em horas. Assim, caso a CONTRATADA não realize a atividades dentro desse prazo, será penalizada conforme tabela de NMS.

3.1.20. Abaixo o resumo das atividades esperadas para a execução do contrato:

3.1.20.1. **Curadoria:** Atividade que tem por objetivo selecionar, organizar e otimizar dados ou conteúdo para desenvolver e operar sistemas de Inteligência Artificial de forma precisa e ética. Envolve etapas como a escolha de dados de alta qualidade, eliminação de vieses, categorização adequada, seleção de algoritmos, verificação de transparência e monitoramento dos resultados, visando aprimorar o desempenho e assegurar que o sistema atenda aos objetivos com responsabilidade e relevância para os usuários internos e externos.

3.1.20.2. **Consultoria:** Identificar e documentar os requisitos de negócio, os objetivos do Assistente Virtual Cognitivo e as necessidades dos usuários para orientar o desenvolvimento da solução, definindo possíveis cenários de uso, além de mapear e criar os fluxos de diálogo do Assistente Virtual Cognitivo, definindo interações de conversação, níveis de escalonamento e respostas para garantir uma experiência fluida e precisa.

3.1.20.3. **Assessmet (Site Survey):** Atividade realizada para o entendimento das necessidades e do ambiente onde a solução de Inteligência Artificial será implementada. Esse levantamento detalhado permite identificar fatores que podem impactar a implementação e operação de sistemas junto ao Assistente Virtual Cognitivo, como infraestrutura, conectividade, redes e segurança.

3.1.20.4. **Plano de Arquitetura:** Atividade realizada para criação de uma estrutura tecnológica que inclui a escolha de ferramentas como APIs de inteligência artificial, plataformas em nuvem e integrações com novos sistemas ou existentes. Também deverá abranger a modelagem de dados para aprendizado, definição de fluxos de conversação e lógica de resposta. Deverá ainda prever escalabilidade automática, segurança e disponibilidade para garantir que o sistema seja robusto e capaz de atender a múltiplos usuários externos simultaneamente.

3.1.20.5. **Integrações Ferramentas, Sistemas e Banco de Dados:** A CONTRATADA deverá conectar a solução com sistemas e plataformas externas essenciais para garantir uma operação eficaz, incluindo a integração com bancos de dados, APIs de inteligência artificial, CRM, sistemas de gerenciamento de usuários, soluções de SSO, e até mesmo serviços de cloud para garantir a escalabilidade e a alta disponibilidade do sistema. Essas integrações são necessárias para permitir que o assistente tenha acesso a dados em tempo real, execute tarefas automatizadas e forneça respostas contextualizadas, além de otimizar a experiência dos usuários externos ao interagir com diferentes sistemas e plataformas.

3.1.20.6. **Criação de Dashboard:** A CONTRATADA deverá realizar o desenvolvimento de interfaces visuais que permitem a monitorização e análise em tempo real do desempenho do assistente e das interações com os usuários externos. A elaboração de dashboards permite que as equipes de TI da CONTRATANTE monitorem o desempenho de

maneira intuitiva, proporcionando melhorias contínuas na experiência dos usuários externos e nos resultados operacionais.

3.1.20.7. **Suporte assistente cognitivo:** A CONTRATADA deverá manter o Assistente Virtual Cognitivo operante por todo o período contratual.

3.1.21. Todas as atividades deverão ser prestadas por pessoal devidamente qualificado, com as comprovações necessárias definidas em cada projeto;

3.1.22. Os serviços serão prestados remotamente pela CONTRATADA, através de profissionais devidamente qualificados para cada projeto;

3.1.23. A CONTRATADA é responsável pela prestação dos serviços caracterizados nas ordens de serviço, devendo utilizar pessoal técnico qualificado, nos quantitativos adequados, para garantir a plena qualidade dos serviços entregues. A definição de composição de recursos, otimização de rotinas ou procedimentos são de responsabilidade da CONTRATADA;

3.1.24. O consumo adicional de horas não previstas não acarretará cobrança adicional ao CONTRATANTE, salvo, excepcionalmente, se expresso em autorização justificada pelo Gestor do Contrato;

3.1.25. O valor será pago, após a verificação da conclusão das métricas e resultados.

#### 4. Chamados de Criação

4.1. Os chamados de criação, envolve atividades de planejamento, criação e diagnóstico.

4.2. A CONTRATADA deverá agendar reunião presencial ou virtual com o CONTRATANTE em até 8 (oito) horas úteis após a abertura do chamado, para tratar da demanda solicitada. No caso de reunião virtual, a CONTRATADA será responsável por prover a infraestrutura tecnológica, restando a CONTRATANTE a responsabilidade por prover terminal de acesso à internet com capacidade de reprodução de áudio e vídeo.

4.3. A CONTRATADA deverá ter a disponibilidade de realizar a reunião em até 24 (vinte e quatro) horas úteis após o contato de que trata o item anterior.

4.4. Após a explicação da demanda, a CONTRATADA deverá apresentar uma agenda com plano de arquitetura contendo no mínimo: Escopo da atividade a ser realizada; Serviços e classificação da sua complexidade, conforme tabela 3; Orçamento detalhado dos serviços da CONTRATADA que serão realizados para implementação do serviço demandado; Profissionais envolvidos da CONTRATADA e da CONTRATANTE; Métricas ou resultados esperados; Cronograma de finalização da atividade, fiscalização e pagamento; Medidas de segurança e continuidade; Previsão orçamentária de consumo de itens UST e Valor total que será consumido do contrato pelo projeto.

4.5. A ATI realizará a análise do plano de arquitetura de modo a verificar se contêm todos os requisitos técnicos requeridos no projeto. Caso contrário, solicitará à CONTRATADA que refaça o plano de arquitetura, sem reinício de contagem de prazo. Durante a análise realizada pela ATI, o prazo da CONTRATADA será suspenso.

4.6. Após o aceite do plano de arquitetura pela ATI, a CONTRATANTE decidirá se os serviços demandados serão implementados.

4.7. Os serviços referentes à elaboração dos planos de arquitetura serão pagos independente da decisão da CONTRATANTE de implementar os serviços descritos nos mesmos.

4.8. O pagamento será realizado de acordo com a tabela 3.

#### 5. Chamados de implantação e exclusão

5.1. Os chamados de implantação, envolvem atividades de execução, alteração, implementação ou exclusão.

5.2. A CONTRATADA deverá agendar reunião presencial ou virtual com o CONTRATANTE em até 08 (oito) horas úteis após a abertura do chamado, para tratar da demanda solicitada. No caso de reunião virtual, a CONTRATADA será responsável por prover a infraestrutura tecnológica, restando a CONTRATANTE a responsabilidade por prover terminal de acesso à internet com capacidade de reprodução de áudio e vídeo.

5.3. A CONTRATADA deverá ter a disponibilidade de realizar a reunião em até 24 (vinte e quatro) horas úteis após o contato de que trata o item anterior.

5.4. A contagem do prazo terá início no dia útil subsequente ao da realização da reunião.

5.5. Após a execução dos serviços (cujos prazos estão designados na coluna Prazo máximo da Tabela 3), a CONTRATANTE realizará a análise dos serviços implementados, para verificar se estão em conformidade com o plano de arquitetura. Caso contrário, solicitará à CONTRATADA que refaça os serviços, sem reinício de contagem de prazo. Durante a análise realizada pela CONTRATANTE, o prazo da CONTRATADA será suspenso.

5.6. A CONTRATANTE poderá solicitar à CONTRATADA demanda de execução, alteração, implantação ou exclusão sem que tenha existido correspondente demanda de planejamento, criação e diagnóstico. Sendo assim, a demanda de implantação poderá ter como fonte algum plano de arquitetura elaborado pela própria CONTRATANTE.

5.7. A fonte da demanda deverá fazer parte da OS de execução, alteração ou implantação.

## 6. Chamados de suporte

6.1. Os chamados de suporte serão classificados por severidade, de acordo com o impacto no Assistente Virtual Cognitivo da CONTRATANTE.

6.2. Os possíveis níveis de severidade são:

6.2.1. **Severidade 1:** Sistema crítico, em produção, está parado ou fora de funcionamento, e não há meios de contornar a falha.

6.2.2. **Severidade 2:** Sistema crítico, em produção, está apresentando falhas de funcionamento, sem causar interrupção do serviço, mas afetando significativamente seu desempenho. Impacto crítico aos usuários.

6.2.3. **Severidade 3:** Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impactos operacionais moderados a pequenos. Impacto moderado aos usuários internos ou externos.

6.2.4. **Severidade 4:** Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features ou melhorias. Impacto mínimo aos usuários internos ou externos.

6.3. Para mensurar os NMS dos chamados de suporte, serão utilizados indicadores relacionados à severidade e ao estado dos chamados, para os quais foram estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA, conforme descrito na tabela adiante. Os chamados terão início da contagem de prazo no momento da comunicação do chamado à CONTRATADA.

Descrição do nível de serviço	Tempo máximo de resolução	Objetivo Mensal
Chamados com severidade 1	2 horas corridas*	99%
Chamados com severidade 2	6 horas corridas*	98%
Chamados com severidade 3	16 horas úteis**	90%
Chamados com severidade 4	40 horas úteis**	90%

Tabela 4 – Chamado de Suporte

*\*Hora corrida: Compreendida o período de 0h às 24h, 7 dias por semana, 365 dias por ano.*

*\*\*Hora útil: Compreende o período de 8h às 18h, de segunda a sexta-feira, excetuando-se feriados nacionais.*

6.4. Será admitida solução de contorno na resolução de chamados de severidade 2 para fins de atendimento dos prazos estipulados na Tabela 4.

6.4.1. Solução de contorno é a redução ou eliminação do impacto de um incidente ou problema para o qual uma resolução completa ainda não está disponível.

6.5. Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente.

6.6. É da CONTRATADA o ônus da prova de alegação de que o não atendimento do nível de severidade estabelecido quando o chamado técnico for originado por falha, interrupção ou qualquer outra ocorrência nos serviços prestados pelas concessionárias de serviços de telecomunicações ou energia elétrica, indisponibilidade de dados, inconsistência de dados e informações geradas pela CONTRATANTE, infraestrutura e capacidade de ambiente de tecnologia Contratante ou de terceiros.

6.6.1. Caso seja verificado que a falha foi ocasionada por inoperância, falha, ou configuração incorreta nos sistemas integrados da CONTRATANTE, não serão aplicadas penalidades ou glosas à CONTRATADA.

6.7. Considera-se um problema plenamente solucionado quando os serviços forem restabelecidos sem restrições e de forma definitiva, ou seja, quando não se tratar de uma resolução paliativa.

6.8. Toda e qualquer intervenção no ambiente produtivo resultante de suporte técnico deve ser executada somente mediante prévia autorização da CONTRATANTE, a partir de informações claras dos procedimentos que serão adotados e executados pela CONTRATADA.

6.9. No final do atendimento e resolução da ocorrência, o técnico da CONTRATADA realizará, em conjunto com representantes da CONTRATANTE, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.

6.10. Ao término dos testes e do atendimento (fechamento do chamado), a CONTRATADA deverá registrar, detalhadamente, por e-mail, as causas do problema e a resolução adotada.

6.11. Nos casos em que o atendimento não se mostrar satisfatório, a CONTRATANTE fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado. Durante os testes, o prazo da CONTRATADA será suspenso.

## **ADENDO XV – GESTÃO DO PROJETO, SERVIÇOS, CONTINUIDADE E RESPOSTA A INCIDENTES**

### **1.Objetivo**

1.1. Este adendo estabelece as diretrizes, responsabilidades, rotinas e melhores práticas a serem adotadas pela CONTRATADA na gestão do projeto e dos serviços contratados, bem como no processo de assunção e transição da rede PE-Conectado II para a Nova Rede Corporativa.

1.2. A CONTRATADA é integralmente responsável pelo gerenciamento do projeto, devendo garantir controle, rastreabilidade, mitigação de riscos, aderência técnica e alinhamento estratégico em todas as fases da execução contratual, com observância às melhores práticas nacionais e internacionais em gerenciamento de projetos, segurança cibernética e continuidade de serviços.

1.3. O cumprimento das exigências aqui estabelecidas é obrigatório, e a não conformidade com os prazos, padrões técnicos e processos poderá resultar nas penalidades previstas no contrato.

### **2.Estrutura de Governança do Projeto, Serviços e Contrato**

2.1. Governança, no contexto deste projeto, é o conjunto de instâncias, papéis e mecanismos formais de supervisão e decisão, estruturados para assegurar o alinhamento da execução contratual aos objetivos técnicos, operacionais e estratégicos da Nova Rede Corporativa.

2.2. A estrutura de governança do projeto deverá assegurar o controle, o alinhamento estratégico, a rastreabilidade e a coordenação entre todas as partes envolvidas. Essa estrutura será responsável por acompanhar a execução, promover a tomada de decisão com base em dados, garantir o cumprimento de escopo, prazos, requisitos técnicos e apoiar a resolução de conflitos e a mitigação de riscos.

2.3. Deve ser instituído o Comitê Diretor do Projeto (CDP), instância máxima de governança estratégica, composto por representantes da alta gestão da CONTRATANTE e da CONTRATADA. Este comitê será responsável por deliberar sobre temas críticos, eventuais atrasos no projeto, validar diretrizes gerais do projeto, resolver impasses institucionais e aprovar eventuais exceções que extrapolem os limites de atuação do Comitê Técnico de Governança (CTG) ou da gestão ordinária do contrato. As reuniões deste comitê ocorrerão trimestralmente ou mediante convocação extraordinária, conforme a complexidade das pautas a serem tratadas.

2.4. Deve ser instituído um Comitê Técnico de Governança (CTG), com foco na avaliação técnica contínua da execução contratual, sendo composto por especialistas da CONTRATANTE e da CONTRATADA, incluindo obrigatoriamente o Fiscal do Contrato. Este comitê será responsável pelo acompanhamento de requisitos técnicos, conformidade de entregas, análise de NMSs, validação de planos de ação e apoio técnico à gestão de riscos e qualidade. Terá reuniões mensais e poderá ser acionado extraordinariamente mediante eventos críticos ou incidentes de impacto.

2.5. A CONTRATANTE deverá designar formalmente o Gestor do Contrato, que atuará como seu representante institucional responsável pelo acompanhamento da execução contratual, com atribuições voltadas à análise da conformidade das entregas, supervisão do cumprimento das cláusulas contratuais, controle orçamentário e financeiro, avaliação da qualidade dos serviços prestados e proposição de medidas administrativas em caso de descumprimento contratual. O Gestor do Contrato também atuará como elo entre a CONTRATANTE e os demais agentes envolvidos na governança do projeto, incluindo o Comitê Técnico de Governança e o Fiscal do Contrato.

2.6. A CONTRATANTE deverá designar formalmente o Fiscal do Contrato, responsável por acompanhar a execução contratual em campo, verificar a conformidade técnica dos serviços prestados, garantir o cumprimento das cláusulas contratuais pela CONTRATADA e comunicar formalmente ao Gestor do Contrato eventuais irregularidades, desvios ou não conformidades identificadas. Compete ainda ao Fiscal manter interlocução direta com o preposto da CONTRATADA e zelar pela aderência entre o executado e o que foi contratado.

2.7. Deve ser instituída pela CONTRATANTE a Comissão de Auditoria (CA), coordenada pela ATI/SAD, com a atribuição de estabelecer os parâmetros técnicos de execução, operação e atualização dos procedimentos de aferição da qualidade relacionados aos Níveis Mínimos de Serviço (NMS). A CA poderá ser composta por servidores públicos, profissionais terceirizados e representantes de entidades físicas ou jurídicas formalmente designadas para o desempenho dessas atividades.

2.8. A Comissão de Auditoria poderá designar Verificador(es) Independente(s), pessoa física ou jurídica, responsável(is) pela execução total ou parcial dos procedimentos de aferição da qualidade dos serviços contratados, conforme os critérios técnicos, metodologias e periodicidade estabelecidos pela própria Comissão. As análises e pareceres técnicos emitidos pelo Verificador Independente servirão de insumo qualificado para as decisões do Comitê Técnico de Governança e para eventual aplicação de medidas administrativas pela CONTRATANTE.

2.9. A CONTRATADA deverá designar formalmente o Gestor da CONTRATADA, que atuará como ponto focal operacional junto à CONTRATANTE. Caberá a esse gestor assegurar o cumprimento das obrigações contratuais, coordenar as equipes técnicas, garantir a qualidade dos serviços prestados e manter comunicação contínua com o Gestor do Contrato, respondendo de forma tempestiva às solicitações e notificações formais.

### 3. Plano de Projeto

3.1. A CONTRATADA deverá elaborar e apresentar à CONTRATANTE o Plano do Projeto detalhado, contendo:

3.2. Escopo do Plano

3.2.1. O plano deverá abranger todas as atividades necessárias para a assunção, migração, instalação, configuração,

estabilização dos serviços e comunicação, garantindo uma transição segura, contínua e com impacto mínimo aos Contratantes Aderentes.

3.3. O Plano do Projeto deverá conter, no mínimo:

3.3.1. Plano de Gerenciamento do Escopo deverá apresentar a descrição da solução a ser implantada, abrangendo as tecnologias envolvidas, os serviços, a infraestrutura, os equipamentos (hardware), as premissas, as restrições e a Estrutura Analítica do Projeto (EAP), estruturada em dois níveis, sendo o primeiro correspondente às fases de implantação e o segundo aos pacotes de trabalho que caracterizam as principais entregas. O plano também deverá incluir uma descrição detalhada das fases de implantação, a metodologia a ser adotada, os processos de homologação, os critérios de aceitação dos serviços, bem como os requisitos técnicos e pré-requisitos indispensáveis à correta implementação da solução.

3.3.2. O Plano de Gerenciamento do Cronograma deverá apresentar o detalhamento das atividades previstas, com a identificação dos marcos principais, prazos, dependências e caminhos críticos, devendo ser elaborado em ferramenta de gerenciamento de projetos compatível, que permita o acompanhamento contínuo da execução, o controle de desvios e a realização de eventuais ajustes sempre que necessário.

3.3.2.1. À critério da CONTRATADA, uma ferramenta de gerenciamento de projetos poderá ser utilizada para garantir funcionalidades adequadas para a gestão colaborativa, controle de versões, rastreamento de entregas e gestão de riscos, cronograma e comunicação.

3.3.2.2. Todos os documentos, marcos, artefatos, atas, registros de reuniões, entregas parciais e eventos relevantes da execução do projeto deverão ser obrigatoriamente enviados para todos os membros fixos do Comitê Diretor e Técnico da CONTRATANTE.

3.3.3. Plano de Gerenciamento de Riscos deverá conter a identificação dos riscos conhecidos que possam impactar a transição e a implantação da Nova Rede Corporativa, contemplando uma análise qualitativa e quantitativa, definição de escala de probabilidade e impacto, e as respectivas estratégias de mitigação, prevenção e contingência a serem adotadas pela CONTRATADA.

3.3.4. Plano de Gerenciamento da Comunicação deverá descrever a estrutura de comunicação do projeto, contendo a identificação das partes interessadas, os canais e meios formais de comunicação, a matriz de recorrência e responsabilidades estrutura organizacional, e os artefatos obrigatórios, tais como atas, relatórios de progresso, registros de mudanças, termos de aceite e entre outros documentos que garantam a rastreabilidade e a transparência da execução contratual.

3.3.5. Plano de Gerenciamento da Qualidade e Integração deverá estabelecer as políticas, processos, critérios, responsabilidades e procedimentos que serão utilizados pela CONTRATADA para assegurar a conformidade das entregas com os padrões técnicos exigidos no contrato, bem como garantir a coordenação entre os diversos elementos do projeto e a consolidação das informações necessárias à tomada de decisão, onde deverão estar contemplados, no mínimo:

3.3.5.1. Os métodos de verificação e validação técnica dos serviços entregues, incluindo critérios objetivos de aceitação, processos de homologação, auditorias e testes de qualidade a serem aplicados em todas as fases do projeto.

3.3.5.2. A definição das interfaces entre planos de gerenciamento, unidades técnicas e processos operacionais, visando promover a integração funcional e a rastreabilidade das decisões e entregas.

3.3.5.3. A consolidação e controle das informações essenciais à gestão do projeto, incluindo artefatos, relatórios, métricas de desempenho e indicadores de conformidade.

3.3.5.4. A definição das responsabilidades das partes envolvidas na qualidade e na integração do projeto, com destaque para a atuação dos analistas de qualidade previstos contratualmente pela CONTRATANTE.

3.3.5.5. Os mecanismos de acompanhamento da execução integrada do projeto, em alinhamento com o Escritório de Projetos, com os comitês técnicos e com as ferramentas de gestão aprovadas pela CONTRATANTE.

3.3.6. Plano de Gerenciamento de Mudanças deverá definir o processo formal a ser seguido pela CONTRATADA para solicitação, análise, aprovação, implementação e registro de alterações no escopo, cronograma ou características técnicas do projeto, assegurando que todas as mudanças sejam devidamente justificadas, documentadas e autorizadas pela CONTRATANTE antes de sua execução.

3.3.7. Plano de Assunção deverá ser elaborado pela CONTRATADA com o objetivo de garantir que a transição da rede PE-Conectado II para a Nova Rede Corporativa ocorra de forma segura, planejada e com o menor impacto possível à

operação dos órgãos aderentes, contemplando a estruturação técnica, os prazos, os requisitos e os procedimentos necessários para a migração, ativação e estabilização dos serviços contratados.

3.3.7.1. A CONTRATADA será integralmente responsável pela execução do Plano de Assunção, devendo assegurar que a implantação da Nova Rede Corporativa atenda aos requisitos contratuais e técnicos exigidos, sem prejuízo à continuidade dos serviços e ao cumprimento dos prazos estabelecidos.

3.3.7.2. O Plano de Assunção deverá identificar riscos, levantar pré-requisitos e definir medidas para mitigação de impactos operacionais, de forma a subsidiar a implantação da nova infraestrutura dentro dos prazos exigidos neste Termo de Referência.

3.3.7.3. A CONTRATADA deverá, no mínimo:

3.3.7.3.1. Realizar o mapeamento e o planejamento de mitigação de riscos técnicos e operacionais que possam comprometer a migração e ativação da nova rede, propondo estratégias para redução ou eliminação de seus efeitos.

3.3.7.3.2. Levantar os pré-requisitos técnicos e estruturais indispensáveis à correta instalação, ativação e operação dos serviços contratados.

3.3.7.3.3. Validar a aderência da solução, dos serviços e dos equipamentos implantados aos requisitos contratuais e aos níveis de serviço acordados, garantindo conformidade técnica plena.

3.3.7.3.4. Executar testes e auditorias técnicas preliminares que assegurem a compatibilidade, resiliência e desempenho da nova solução antes da sua ativação definitiva.

3.3.7.3.5. Propor ajustes ou otimizações técnicas, sempre que identificadas oportunidades de melhoria na eficiência da implantação ou na qualidade dos serviços.

3.3.7.3.6. Elaborar os procedimentos operacionais para transição e ativação dos serviços, incluindo mecanismos de rollback que permitam reverter a migração em caso de falhas críticas.

3.3.7.3.7. Desenvolver e apresentar um cronograma detalhado das atividades relacionadas à migração e à ativação dos serviços, alinhado com a CONTRATANTE e compatível com os marcos definidos no projeto, de modo a minimizar impactos em todas as etapas da execução.

3.3.7.4 Diretrizes para Execução do Plano de Assunção

3.3.7.4.1. A CONTRATADA deverá realizar todas as verificações necessárias dentro do escopo do novo projeto, sem interferir na operação da rede atual.

3.3.7.4.2. Quaisquer dependências ou condicionantes identificadas que possam afetar a ativação da Nova Rede Corporativa deverão ser comunicadas formalmente à CONTRATANTE, em até 3 (três) dias úteis, acompanhadas de análise de impacto e proposta de solução.

3.3.7.4.3. Todos os serviços deverão ser implantados conforme as especificações contratuais, sendo de responsabilidade da CONTRATADA garantir sua plena funcionalidade antes da transição definitiva.

3.3.7.4.4. A CONTRATADA deverá entregar relatórios técnicos detalhados sobre o mapeamento de riscos, pré-requisitos e as ações de mitigação propostas, conforme o cronograma definido pela CONTRATANTE.

3.3.7.4.5. A CONTRATADA será totalmente responsável pelo cumprimento das obrigações descritas, não sendo permitido alegar desconhecimento de riscos ou necessidades previamente mapeadas para justificar atrasos ou falhas na entrega do projeto.

3.3.7.4.6. O descumprimento das exigências estabelecidas no Plano de Assunção poderá resultar em penalidades contratuais e adoção de medidas corretivas, conforme previsto no contrato.

3.4. Equipe do Projeto

3.4.1. A CONTRATADA deverá indicar formalmente os responsáveis técnicos pelo projeto, incluindo as interfaces operacionais, comerciais, preposto e um Gerente de Projeto dedicado, devidamente qualificado com as certificações exigidas do ADENDO IX.

3.4.2. O Gerente de Projeto designado pela CONTRATADA deverá coordenar, planejar, integrar, executar, controlar, comunicar todas as atividades do projeto, participar ativamente de reuniões de acompanhamento, responder formalmente pelos compromissos assumidos e assegurar o cumprimento do escopo, cronograma, níveis de serviço e demais obrigações previstas contratualmente.

3.4.3. A CONTRATADA deverá manter uma equipe técnica qualificada e dimensionada de forma compatível com as demandas do projeto, assegurando disponibilidade contínua dos recursos necessários para atendimento às etapas de planejamento, implantação, testes, estabilização, operação e suporte.

3.4.4. A CONTRATADA deverá elaborar e submeter à aprovação da CONTRATANTE uma Matriz RACI detalhada,

relacionando todas as macroatividades do projeto, com a designação das responsabilidades de cada parte (Responsável, Aprovador, Consultado e Informado), visando a clareza nas interações e responsabilidades de execução.

### 3.5. Prazos para Entrega e Aprovação

3.5.1. A CONTRATADA deverá apresentar o Plano do Projeto completo, incluindo seus planos componentes e o cronograma de assunção dos serviços, no prazo máximo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão das Ordem de Serviço (OS) de instalação do Centro Integrado de Inteligência e Segurança Cibernética – CIISC (Serviços e Soluções, Adendos VIII e IX).

3.5.2. A CONTRATANTE terá até 5 (cinco) dias úteis, contados do recebimento da documentação, para proceder com a análise técnica e emissão de parecer quanto à aprovação ou necessidade de ajustes no Plano do Projeto.

3.5.3. Caso sejam identificadas inconsistências, omissões ou necessidade de ajustes, a CONTRATADA deverá apresentar a versão readequada no prazo máximo de 10 (dez) dias corridos, contados a partir da notificação formal da CONTRATANTE.

3.5.4. Após a aprovação do Plano do Projeto, a migração, instalação, ativação e estabilização dos serviços deverão ser executadas conforme o cronograma físico apresentado e validado pela CONTRATANTE.

3.5.5. A CONTRATADA deverá concluir integralmente o processo de assunção no prazo máximo de 365 (trezentos e sessenta e cinco) dias corridos, contados a partir da emissão da Ordem de Serviço para instalação dos serviços vinculados ao Centro Integrado de Inteligência e Segurança Cibernética – CIISC, conforme disposições constantes nos Adendos VIII e IX do Termo de Referência.

## 4. Fases do Projeto

### 4.1. Fase de Apresentação

4.1.1. Esta fase terá início imediatamente após a emissão da Ordem de Serviço (OS) referente à instalação dos serviços do Centro Integrado de Inteligência e Segurança Cibernética – CIISC.

4.1.2. Seu objetivo é promover o alinhamento entre a CONTRATANTE e a CONTRATADA quanto à estrutura organizacional do projeto, escopo, cronograma, definição de responsabilidades, reuniões previstas, rotinas de acompanhamento e demais aspectos essenciais para o início da execução contratual.

4.1.3. A apresentação do Plano do Projeto pela CONTRATADA deverá ocorrer em até 45 (quarenta e cinco) dias corridos contados a partir da emissão da OS do serviço CIISC.

4.1.4. Deverá ser realizada uma reunião de apresentação, na qual a CONTRATADA deverá apresentar formalmente à CONTRATANTE o conteúdo do Plano do Projeto, expondo suas diretrizes, estrutura, cronograma e planos associados, bem como entregar sua versão documental completa. Na mesma ocasião, a CONTRATADA deverá apresentar os responsáveis técnicos e comerciais, as interfaces operacionais, o Preposto e o Gerente de Projeto designado.

4.1.5. A CONTRATANTE reserva-se o direito de solicitar ajustes adicionais no Plano do Projeto sempre que verificar incompatibilidade com os requisitos contratuais, regulatórios ou técnicos estabelecidos.

4.1.6. A fase será considerada concluída somente após a validação formal do Plano do Projeto pela CONTRATANTE.

### 4.2. Fase Inicial (Ajuste)

4.2.1. A Fase Inicial terá início imediatamente após a apresentação formal do Plano do Projeto pela CONTRATADA, devendo ocorrer, impreterivelmente, até o 46º (quadragésimo sexto) dia corrido contado a partir da emissão da Ordem de Serviço (OS) referente à instalação dos serviços do Centro Integrado de Inteligência e Segurança Cibernética – CIISC.

4.2.2. Durante esta fase, a CONTRATADA deverá intensificar as ações de acompanhamento técnico do projeto, priorizando a articulação com a CONTRATANTE, o mapeamento de riscos técnicos e operacionais e o levantamento de pré-requisitos físicos, lógicos e institucionais necessários à implantação dos serviços previstos no Plano de Assunção.

### 4.2.3. Reuniões Semanais de Alinhamento

4.2.3.1. Durante a Fase Inicial, deverão ser realizadas reuniões semanais de alinhamento entre a CONTRATANTE e a CONTRATADA, com o objetivo de acompanhar o progresso da execução, avaliar os entregáveis do período, mitigar riscos, revisar a aderência às exigências técnicas e promover os ajustes operacionais necessários à evolução do projeto.

4.2.3.2. As reuniões deverão contar com a participação de gestores, especialistas técnicos e representantes

operacionais de ambas as partes, conforme a pauta a ser definida previamente.

4.2.3.3. A duração prevista para cada reunião será de até 2 (duas) horas, sendo sua frequência mantida até a entrada da Fase de Implementação Plena, salvo se acordado de forma diversa entre as partes.

#### 4.3. Fase de Implementação Plena

4.3.1. A Fase de Implementação Plena deverá ter início até o 60º (sexagésimo) dia corrido contado a partir da emissão da Ordem de Serviço (OS) relativa à instalação dos serviços do Centro Integrado de Inteligência e Segurança Cibernética – CIISC.

4.3.2. Esta fase corresponde ao período de maior intensidade operacional do projeto, abrangendo a ativação, migração, validação técnica e estabilização dos serviços da Nova Rede Corporativa em ambiente de produção.

4.3.3. Durante esta fase, deverão ser mantidas e, quando necessário, ampliadas as rotinas de acompanhamento previstas neste adendo, de modo a garantir o controle técnico, a mitigação de riscos, o monitoramento da execução e o cumprimento dos marcos estabelecidos no cronograma.

##### 4.3.3.1. Reuniões Diárias (Daily Stand-Up Meeting)

4.3.3.1.1. As reuniões diárias de acompanhamento deverão ser realizadas obrigatoriamente durante a Fase de Implementação Plena, com o objetivo de monitorar a execução das atividades operacionais, promover o alinhamento entre as equipes e identificar, de forma ágil, impedimentos que possam comprometer o andamento do cronograma.

4.3.3.1.2. Deverão participar das reuniões as equipes operacionais da CONTRATADA e da CONTRATANTE diretamente envolvidas na execução técnica dos serviços.

4.3.3.1.3. A duração da reunião diária deverá ser de, no máximo, 15 (quinze) minutos, priorizando objetividade e foco nos pontos críticos da execução.

4.3.3.1.4. A CONTRATADA deverá apresentar, durante a reunião, um resumo técnico contendo o status das atividades em andamento, ações executadas, observações relevantes, impedimentos identificados e próximos passos.

4.3.3.1.5. Ao término de cada reunião, a CONTRATADA deverá consolidar e enviar à CONTRATANTE um Diário de Bordo, contendo os registros formais da reunião, os apontamentos técnicos tratados, o acompanhamento do cronograma, a atualização do backlog dos serviços com Ordem de Serviço (OS) emitida, bem como demais informações relevantes à execução.

##### 4.3.3.2. Reuniões Semanais de Acompanhamento Operacional

4.3.3.2.1. As reuniões semanais de acompanhamento operacional deverão ocorrer durante a Fase de Implementação Plena, com o objetivo de avaliar os impactos operacionais das implantações em andamento, solucionar conflitos técnicos, prestar suporte às áreas impactadas e planejar as entregas subsequentes.

4.3.3.2.2. Deverão participar das reuniões as equipes técnicas da CONTRATADA e da CONTRATANTE, com participação ampliada de coordenadores e gestores das áreas diretamente envolvidas na execução.

4.3.3.2.3. A duração prevista para cada reunião será de até 2 (duas) horas.

##### 4.3.3.3. Reuniões Mensais do Comitê Técnico de Governança

4.3.3.3.1. As reuniões mensais do Comitê Técnico de Governança deverão ser realizadas com o objetivo de conduzir auditorias de conformidade, analisar o cumprimento dos Acordos de Nível de Serviço (SLAs), revisar riscos operacionais e propor ações corretivas ou preventivas, sempre que necessário.

4.3.3.3.2. Participarão dessas reuniões os especialistas técnicos e gestores designados pela CONTRATANTE e pela CONTRATADA, preferencialmente os mesmos integrantes da governança contínua da implantação.

4.3.3.3.3. A duração prevista para cada reunião será de até 3 (três) horas.

##### 4.3.3.4. Reuniões Mensais do Comitê Diretor do Projeto

4.3.3.4.1. O Comitê Diretor do Projeto deverá se reunir mensalmente para validar marcos do projeto, deliberar sobre replanejamentos e desvios relevantes, tomar decisões estratégicas e autorizar escalonamentos de demandas conforme a criticidade.

4.3.3.4.2. Deverão participar dessas reuniões os executivos e representantes da alta gestão da CONTRATANTE e da CONTRATADA, além de convidados estratégicos, conforme definido previamente na pauta.

4.3.3.4.3. A duração prevista para cada reunião será de até 1 (uma) hora.

4.3.3.4.4. As reuniões do Comitê Diretor deverão ocorrer, preferencialmente, em semanas intercaladas às reuniões do Comitê Técnico de Governança, de forma a garantir sinergia entre os níveis técnico e estratégico da governança.

4.3.3.4.5. A periodicidade das reuniões do Comitê Diretor poderá ser revista e ajustada, mediante consenso entre os membros dos comitês ou por decisão do Gestor do Contrato da CONTRATANTE, conforme a complexidade e o estágio

do projeto.

#### 4.4. Fase de Operação e Suporte (Após a implementação)

4.4.1. Esta fase terá início de forma progressiva, à medida que os serviços forem implantados, homologados e aceitos formalmente pela CONTRATANTE. A transição para o regime permanente de operação e suporte não depende da conclusão integral do Plano de Assunção, sendo autorizada a entrada em operação dos serviços validados, que deverão ser monitorados com base nos Níveis Mínimos de Serviço (NMS), conforme estrutura estabelecida neste Termo de Referência.

4.4.2. Durante esta fase, deverão ser mantidas as seguintes rotinas de acompanhamento, observando-se os ritos de governança definidos contratualmente.

##### 4.4.2.1. Reuniões Semanais de Gestão de Serviços

4.4.2.1.1. Estas reuniões terão como objetivo analisar o desempenho operacional dos serviços em regime permanente, realizar o monitoramento contínuo dos Níveis Mínimos de Serviço (NMS), avaliar incidentes críticos e aplicar ações corretivas e preventivas conforme necessidade identificada.

4.4.2.1.2. Participarão das reuniões as equipes operacionais da CONTRATADA, compostas por Especialistas de Atenção, Qualidade e Técnicos, juntamente com a equipe técnica da CONTRATANTE.

4.4.2.1.3. A duração prevista para cada reunião será de até 1 (uma) hora.

##### 4.4.2.2. Reuniões Mensais do Comitê Técnico de Governança

4.4.2.2.1. Estas reuniões terão como objetivo a apresentação e análise dos relatórios mensais de desempenho, qualidade e segurança da rede, com ênfase nos indicadores operacionais, conformidade com os NMS, ocorrências críticas e planos de ação para correção de desvios.

4.4.2.2.2. Compete também ao comitê, quando aplicável, validar a aplicação de glosas e penalidades previstas contratualmente, com base nas evidências técnicas apresentadas, inclusive pelo Verificador Independente.

4.4.2.2.3. Participarão das reuniões as equipes operacionais da CONTRATANTE e da CONTRATADA, incluindo Especialistas de Atenção, Qualidade e Técnicos designados para a governança contínua da operação.

4.4.2.2.4. A duração prevista para cada reunião será de até 3 (três) horas.

##### 4.4.2.3. Reuniões Trimestrais do Comitê Diretor do Projeto

4.4.2.3.1. As reuniões trimestrais do Comitê Diretor do Projeto terão como objetivo avaliar a maturidade da operação, propor inovações técnicas, recomendar ações de melhoria contínua e assegurar a sustentabilidade técnica, contratual e gerencial dos serviços em execução.

4.4.2.3.2. Deverão participar executivos da CONTRATANTE e da CONTRATADA, com possibilidade de inclusão de convidados estratégicos, conforme definido previamente em pauta.

4.4.2.3.3. A duração prevista para cada reunião será de até 1 (uma) hora.

4.4.2.3.4. A periodicidade das reuniões do Comitê Diretor poderá ser revista e ajustada, mediante consenso entre os membros dos comitês ou por decisão do Gestor do Contrato da CONTRATANTE, observada a complexidade e o estágio da operação.

#### 4.4.3. Transição para o Regime Permanente de Operação e Suporte

4.4.3.1. A transição dos serviços da fase de implantação para o regime permanente de operação e suporte deverá ocorrer de forma gradual, acompanhando a conclusão da migração e homologação de cada serviço para a Nova Rede Corporativa.

4.4.3.2. Cada serviço migrado, uma vez validado pela CONTRATANTE, será considerado operacional e passará a ser gerido pela estrutura de suporte estabelecida para a fase de operação, conforme os níveis de serviço, controles e indicadores definidos contratualmente.

4.4.3.3. A CONTRATADA deverá garantir que, ao final do Plano de Assunção, todos os serviços estejam completamente desassociados da infraestrutura da rede PE-Conectado II, não restando dependências técnicas, operacionais ou documentais.

4.4.3.4. A formalização da transição completa para o regime permanente deverá ser registrada durante a Reunião de Encerramento do Plano de Assunção.

#### 4.5. Fase de Encerramento do Projeto

4.5.1. Esta fase deverá consolidar o cumprimento integral das obrigações contratuais assumidas pela CONTRATADA, promover a finalização das atividades técnicas e administrativas previstas, formalizar a transição definitiva para o ambiente de operação e registrar os aprendizados do projeto, assegurando sua rastreabilidade e a efetividade da

gestão ao longo do ciclo de vida do contrato.

4.5.2. Deverá ser iniciada após o cumprimento de todas as etapas do Plano de Assunção e deverá ser concluída em até 365 (trezentos e sessenta e cinco) dias corridos, contados a partir da emissão da Ordem de Serviço relativa à instalação dos serviços vinculados ao Centro Integrado de Inteligência e Segurança Cibernética – CIISC, conforme previsto nos Adendos VIII e IX do Termo de Referência.

4.5.3. A CONTRATADA deverá observar, no mínimo, as seguintes entregas e ações obrigatórias para o encerramento do projeto:

4.5.3.1. A CONTRATADA deverá apresentar relatório executivo final consolidado do projeto, contendo:

4.5.3.1.1 Sumário de entregas com datas e status de execução;

4.5.3.1.2 Análise do cumprimento do escopo, prazos, cronograma físico e NMSs;

4.5.3.1.3 Avaliação de desempenho dos serviços e das ações de mitigação de riscos.

4.5.3.2. A CONTRATADA deverá entregar toda a documentação técnica ao longo das fases do projeto, de forma progressiva, conforme os serviços forem sendo implantados e homologados. Na etapa final, deverá apresentar a consolidação dessa documentação em meio digital, devidamente organizada, contendo no mínimo:

4.5.3.2.1. Projeto lógico e documentação de arquitetura da rede implantada, incluindo topologias, plantas, diagramas físicos de conexão, interconexão entre equipamentos, AS-Built e fluxos de rede;

4.5.3.2.2. Documentação de configuração dos ativos de rede, contemplando:

4.5.3.2.2.1 Configurações realizadas em cada equipamento (firewalls, switches, roteadores, controladoras, access point, entre outros);

4.5.3.2.2.2. Arquivos de backup e versionamento de configuração, quando aplicável;

4.5.3.2.2.3. Estrutura lógica e física implementada, contendo descrição detalhada das VLANs, endereçamento IP, rotas, listas de controle de acesso (ACLs), protocolos e demais elementos da solução;

4.5.3.2.2.4. Relacionamento entre serviços e funcionalidades habilitadas por ativo;

4.5.3.2.3. Inventário técnico dos produtos e componentes instalados, contendo modelo, versão, fabricante e localização de cada item;

4.5.3.2.4. Documentos relacionados à segurança da informação, contemplando as configurações aplicadas aos equipamentos e sistemas, com destaque para: política de senhas e perfis de acesso utilizados; estrutura de controle de privilégios e autenticação; procedimentos de auditoria e rastreabilidade de alterações; além da configuração do sistema de coleta e armazenamento de logs, indicando os eventos registrados, sua periodicidade, destino e critérios de retenção, especialmente quando direcionados a equipamentos de guarda de logs previstos na solução.

4.5.3.2.5. Procedimentos operacionais padrão (POPs), fluxogramas de processos, manuais técnicos de operação, manutenção preventiva e corretiva, além de orientações para restauração em caso de falha, quando aplicável.

4.5.4. A CONTRATADA deverá apresentar formalmente das Lições Aprendidas, contendo:

4.5.4.1. Principais acertos e boas práticas identificadas;

4.5.4.2. Desvios e pontos de melhoria;

4.5.4.3. Recomendações para projetos futuros e evolução da Rede Corporativa.

4.5.5. A CONTRATADA e a CONTRATANTE deverão realizar uma Reunião de Encerramento do Plano de Assunção, com a participação de membros do Comitê Técnico e Diretor, das partes interessadas e dos principais stakeholders do projeto, com o objetivo de formalizar a conclusão das atividades de migração da rede PE-Conectado II para a Nova Rede Corporativa.

4.5.5.1. Validação das entregas previstas no Plano de Assunção, com base nos critérios técnicos, operacionais e documentais estabelecidos;

4.5.5.2. Validação da migração integral dos serviços para a nova rede, confirmando a inexistência de dependências técnicas ou operacionais da infraestrutura anterior e formalizando a entrada definitiva no regime permanente de operação e suporte.

4.5.5.3. A Reunião de Encerramento do Plano de Assunção deverá incluir a análise do cumprimento do prazo contratual para conclusão desta etapa. Caso seja constatado descumprimento, a CONTRATANTE poderá, a seu critério, aplicar as penalidades previstas no contrato, inclusive em momento anterior à referida reunião, caso entenda que o atraso comprometeu a execução, o cronograma ou a continuidade dos serviços.

4.5.5.4. Em qualquer hipótese, a aplicação de penalidades deverá observar o devido processo administrativo, garantindo à CONTRATADA o pleno exercício do contraditório e da ampla defesa, nos termos da Lei nº 14.133/2021

(Nova Lei de Licitações e Contratos Administrativos), do edital da licitação e do contrato firmado entre as partes.

4.5.6. A CONTRATADA deverá garantir que todas as obrigações contratuais estejam concluídas e documentadas.

4.6. Registro das Reuniões

4.6.1. A CONTRATADA será responsável pela elaboração das atas de todas as reuniões previstas neste adendo, realizadas durante todas as fases do projeto (Apresentação, Inicial (Ajuste), Implementação Plena, Operação e Suporte e Encerramento do Projeto).

4.6.2. As atas deverão descrever, conforme a natureza, público e os objetivos da reunião, informações como: data, participantes, temas discutidos, tomadas de decisões, ações acordadas, pontos de atenção, próximos passos, pendências identificadas, indicadores apresentados entre outras deliberações.

4.6.3. As atas deverão ser encaminhadas à CONTRATANTE em até 1 (um) dia útil após a realização de cada reunião, por meio do canal oficial de comunicação definido no Plano de Projeto, observando-se os critérios de padronização, rastreabilidade e acesso estabelecidos pela CONTRATANTE.

4.7. As reuniões previstas nesta seção, independentemente da fase do projeto em que estejam inseridas, poderão ter sua periodicidade, duração e composição de participantes ajustadas, desde que haja comum acordo entre a CONTRATANTE e a CONTRATADA, devidamente formalizado em comunicação oficial do projeto. Tais flexibilizações não poderão, em nenhuma hipótese, comprometer os ritos mínimos de governança, o acompanhamento da execução contratual, a rastreabilidade das decisões ou a efetividade da gestão do projeto.

4.8. A entrega da documentação deverá ocorrer de forma progressiva, ao longo do período de assunção, acompanhando a homologação e ativação dos respectivos serviços, de modo a garantir a rastreabilidade, a conformidade técnica e o suporte à operação desde as primeiras etapas de implantação.

#### **ADENDO XVI - REGIME DE SUPORTE E MANUTENÇÃO DOS SERVIÇOS (LOTE 1)**

1. Este adendo tem como objetivo estabelecer os critérios, modalidades e condições operacionais para o suporte técnico e regime de manutenção dos serviços contratados no âmbito do LOTE 1 da Nova Rede Corporativa do Estado de Pernambuco.

2. O regime padrão de suporte técnico a ser oferecido pela CONTRATADA será de 12 horas por dia, 5 dias por semana (12x5), aplicável a todos os serviços prestados nos Pontos Conectados Seguros (PCS), exceto aqueles que já tenham a obrigatoriedade de ser 24x7 conforme tabela Limites de Tempos para Correções de Falhas do ADENDO II, abrangendo, mas não se limitando a: Links de Acesso (LAP, LME e LAT), Solução Unificada de Segurança (UTM), Rede Sem Fio (Wi-Fi) e Pontos de Voz.

3. A alteração do regime padrão de suporte técnico (12x5) para os regimes diferenciados de 12x7 ou 24x7 somente poderá ser efetuada mediante emissão de Ordem de Serviço (OS) formal por parte da CONTRATANTE. Esta OS deverá indicar os horários de funcionamento dos PCS contemplados, de modo a alinhar o regime de suporte com as necessidades operacionais específicas de cada localidade.

4. A CONTRATANTE poderá, conforme demanda específica e justificativa técnica aprovada, contratar regimes diferenciados de manutenção, sendo eles:

- 12x7: 12 horas por dia, 7 dias por semana;
- 24x7: 24 horas por dia, 7 dias por semana.

5. A contratação de regimes diferenciados aplica-se exclusivamente aos serviços ativos nos PCS e deverá constar explicitamente nas Ordens de Serviço ou contratos acessórios vinculados ao TR.

6. Não será permitida a sobreposição de regimes de suporte técnico para um mesmo PCS.

7. O objetivo da adoção desses regimes distintos é garantir flexibilidade à Administração Pública, permitindo adequar a cobertura de suporte às necessidades operacionais dos diversos órgãos usuários, otimizando recursos e assegurando a continuidade dos serviços em locais críticos.

8. Em qualquer dos regimes contratados, a CONTRATADA deverá assegurar o cumprimento dos prazos máximos de atendimento e resolução definidos nos Níveis Mínimos de Serviço (NMS), que permanecem vigentes e obrigatórios,

conforme previsto no ADENDO II. O eventual descumprimento das obrigações assumidas poderá ensejar a aplicação de penalidades contratuais, inclusive glosas proporcionais aos serviços impactados, conforme estabelecido na legislação vigente e nos instrumentos contratuais.

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**ANEXO II**  
**DECLARAÇÕES COMPLEMENTARES**

A empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, sediada \_\_\_\_\_, por intermédio do seu representante legal o(a) Sr(a) \_\_\_\_\_, portador(a) da Carteira de Identidade nº \_\_\_\_\_ SSP/\_\_\_\_\_ e CPF nº \_\_\_\_\_, sob as penas da lei e para os fins dispostos neste Edital:

**DECLARA** que cumpre o disposto no inciso XXXIII do art. 7º da Constituição Federal;

**DECLARA** que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas;

**DECLARA** que não possui em seu quadro societário ou de pessoal agente público do órgão ou entidade licitante ou contratante, nos termos do art. 9º, §1º da Lei 14.133/2021;

**DECLARA** que não incorre em qualquer uma das vedações impostas no art. 14 da Lei 14.133/2021 aplicáveis ao objeto da presente licitação;

**DECLARA** que atende às disposições da Lei Geral de Proteção de Dados (LGPD).

Recife, XX de XXXX de XXXX

\_\_\_\_\_  
**REPRESENTANTE DA EMPRESA**

**CNPJ XXX**

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**

**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**ANEXO III**  
**DECLARAÇÃO DE CONHECIMENTO DAS CONDIÇÕES LOCAIS PARA O**  
**CUMPRIMENTO DAS OBRIGAÇÕES**

A empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, sediada \_\_\_\_\_, por intermédio do seu representante legal o(a) Sr(a) \_\_\_\_\_, portador(a) da Carteira de Identidade nº \_\_\_\_\_ SSP/\_\_\_\_\_ e CPF nº \_\_\_\_\_, sob as penas da lei e para os fins dispostos neste Edital, **DECLARA** que está ciente e concorda com as condições contidas no Edital de Pregão Eletrônico nº XX e seus anexos, bem como **atesta** que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

Recife, XX de XXXX de XXXX

\_\_\_\_\_  
**REPRESENTANTE DA EMPRESA**  
**CNPJXXX**

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**ANEXO IV**  
**DECLARAÇÃO DE CONHECIMENTO PLENO DAS CONDIÇÕES E**  
**PECULIARIDADES DA CONTRATAÇÃO**

Eu, Sr(a) \_\_\_\_\_, portador(a) da Carteira de Identidade nº \_\_\_\_\_ SSP/\_\_\_\_\_ e CPF nº \_\_\_\_\_, na qualidade de responsável técnico da empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, sediada \_\_\_\_\_, **DECLARO**, sob as penas da lei e para os fins dispostos neste Edital, possuir conhecimento pleno das condições e peculiaridades da contratação referentes ao Edital de Pregão Eletrônico nº XX e seus anexos.

Recife, XX de XXXX de XXX.

\_\_\_\_\_  
**RESPONSÁVEL TÉCNICO DA LICITANTE**

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**ANEXO V**  
**MINUTA DE CONTRATO PRESTAÇÃO DE SERVIÇOS**

**CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DE PERNAMBUCO, ATRAVÉS DA SECRETARIA XXX E A EMPRESA XXXXXX, EM DECORRÊNCIA DO PREGÃO ELETRÔNICO Nº 90323/2025, PROCESSO Nº 4338.2025.AC-10.PE.90323.SAD.ATI:**

O **ESTADO DE PERNAMBUCO**, através da **SECRETARIA XXXX**, inscrita no CNPJ/MF sob o nº XXX, com sede na \_\_\_\_\_, nesta cidade, doravante designada **CONTRATANTE**, neste ato representada pelo(a) \_\_\_\_\_(nome e cargo), portador da matrícula funcional nº XXXXX, no uso da competência conferida pelo \_\_\_\_\_, e a empresa \_\_\_\_\_, inscrita no CNPJ (MF) sob o nº \_\_\_\_\_, sediada em \_\_\_\_\_, representada neste ato por \_\_\_\_\_(nome e função que exerce na contratada), conforme atos constitutivos da empresa OU procuração apresentada nos autos, doravante designada **CONTRATADA**, têm entre si justo e acordado, e celebram o presente **CONTRATO**, mediante as seguintes cláusulas e condições, que mutuamente outorgam e estabelecem, sujeitando-se às disposições previstas na Lei Federal nº 14.133, de 1º de abril de 2021, nos Decretos Estaduais nº 53.384, de 22.08.2022 e 54.142, de 14.12.2022, e demais normas aplicáveis.

**CLÁUSULA PRIMEIRA - DO OBJETO**

Constitui objeto do presente **CONTRATO** a prestação de serviços de rede corporativa segura com acesso à Internet, envolvendo implantação, operacionalização e melhoria contínua de serviços de acesso à Internet, conectividade de rede local e datacenter, voz, comunicação unificada, contact center, segurança e operação integrada de redes de computadores, visando atender as necessidades dos órgãos da Administração Direta, Indireta, Fundos Especiais, Autarquias e Fundações Públicas

integrantes do Poder Executivo do Estado de Pernambuco, nas condições estabelecidas no Termo de Referência, na proposta da **CONTRATADA** e nos demais documentos constantes do processo administrativo em epígrafe.

**PARÁGRAFO ÚNICO:** Nos termos do item 3.1.6 do Termo de Referência, poderão aderir ao Contrato dos Serviços da Nova Rede Corporativa:

I. Todos os Órgãos e Entidades da Administração Direta e Indireta, inclusive Fundacional, do Poder Executivo Estadual, a seguir denominada CONTRATANTE aderente, mediante Contrato de Adesão ao Contrato Mater.

II. Os Poderes Judiciário e Legislativo Estadual, bem como, o Ministério Público Estadual e Tribunal de Contas do Estado, mediante convênios específicos celebrados com o Governo do Estado, e assinatura do Contrato de Adesão, assim como, as Organizações Sociais que mantenham ou venham a manter Contrato de Gestão com o Estado.

III. Todos os entes denominados CONTRATANTES aderentes arcarão com todas as despesas decorrentes dos Termos de Adesão firmados com a CONTRATADA.

IV. A adesão das Organizações Sociais ao Contrato deverá ser devidamente consignada no Contrato de Gestão e contabilizada como aporte de recursos estaduais.

## CLÁUSULA SEGUNDA - DA DOCUMENTAÇÃO

São partes integrantes deste **CONTRATO** para todos os fins de direito, o processo relativo ao **PREGÃO ELETRÔNICO Nº 90323/2025, PROCESSO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**; e todos os seus anexos, assim como a proposta apresentada pela **CONTRATADA**.

## CLÁUSULA TERCEIRA - DO PRAZO DE VIGÊNCIA E PRORROGAÇÃO

**PARÁGRAFO PRIMEIRO:** O prazo de vigência do **CONTRATO** é de 48 (quarenta e oito) meses, contados da data de sua assinatura, prorrogável por 2 (dois) períodos iguais de 36 (trinta e seis), até o limite de 120 (cento e vinte) meses, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, observadas as condições de vantajosidade, interesse público e disponibilidade orçamentária.

**PARÁGRAFO SEGUNDO:** A prorrogação fica condicionada ao ateste, pela autoridade competente, de que há interesse na manutenção dos serviços e de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a **CONTRATADA**.

**PARÁGRAFO TERCEIRO:** A pesquisa para aferição da vantajosidade econômica da prorrogação contratual será realizada mediante utilização dos parâmetros estabelecidos no art. 12 da Portaria SAD nº 2.679, de 29.09.2021, ou em eventual norma que a altere ou substitua.

**PARÁGRAFO QUARTO:** O **CONTRATO** não poderá ser prorrogado quando a **CONTRATADA** tiver sido penalizada com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar, observadas as abrangências e os limites temporais de aplicação, sendo excepcionalmente admitida a prorrogação, pelo período mínimo necessário à conclusão de um novo certame, de modo a evitar a descontinuidade do serviço ou o custo de uma contratação emergencial.

**PARÁGRAFO QUINTO:** Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a prorrogação.

**PARÁGRAFO SEXTO:** O início da vigência da adesão está condicionada à assinatura do respectivo Termo pelos representantes do Contratante Principal, órgão Aderente e Contratada.

**PARÁGRAFO SÉTIMO:** Os Termos de Adesão terão sua vigência subordinada à do Contrato Corporativo.

**PARÁGRAFO OITAVO:** Haverá prorrogação automática da vigência dos Termos de Adesão quando da prorrogação do Contrato Corporativo condicionada sua eficácia ao apostilamento de empenhos correspondentes ao período prorrogado.

#### CLÁUSULA QUARTA - DO PREÇO

**PARÁGRAFO PRIMEIRO:** A **CONTRATANTE** pagará à **CONTRATADA** o valor global de R\$ XXX (XXX), sendo o valor mensal de R\$ XXX (XXX), conforme estabelecido na proposta, parte integrante deste **CONTRATO**.

**PARÁGRAFO SEGUNDO:** O valor do **CONTRATO** compreende os custos diretos e indiretos decorrentes de sua execução, incluindo tributos, encargos sociais, trabalhistas, previdenciários, fiscais e

comerciais, seguros, despesas de administração, lucro, eventuais custos com transporte, frete e outras despesas correlatas necessárias ao cumprimento integral do objeto da contratação.

**PARÁGRAFO TERCEIRO:** O valor global indicado é meramente estimativo e os pagamentos devidos à **CONTRATADA** serão feitos conforme medições dos serviços efetivamente realizados.

## CLÁUSULA QUINTA - DA DOTAÇÃO ORÇAMENTÁRIA

**PARÁGRAFO PRIMEIRO:** Os recursos financeiros para fazer face às despesas da contratação do objeto desta licitação correrão por conta dos Órgãos ou Entidades (Órgãos Aderentes) que aderirem ao Contrato de Prestação de Serviços (Contrato-Mater) cujos Programas de Trabalho e Elementos de Despesas constarão nos respectivos termos de adesão e notas de empenho, observadas as condições estabelecidas no Edital, a saber:

I. As despesas decorrentes da instalação e operacionalização do Serviço Nova Rede Corporativa SEGURANÇA & CONECTIVIDADE, serão suportadas pelas DOTAÇÕES ORÇAMENTÁRIAS dos órgãos e entidades do Poder Executivo Estadual, no Elemento 3.3.90.39: Serviços de Terceiros – Pessoas Jurídicas, no elemento 3.3.90.39.27 para despesas relativas aos serviços despesas consumo de infraestrutura da rede, internet corporativa, serviço de operação, acesso dedicado; ou à conta das disponibilidades orçamentárias e financeiras das entidades que não dependem do Tesouro Estadual.

**PARÁGRAFO SEGUNDO:** No(s) exercício(s) seguinte(s), as despesas correrão à conta dos recursos próprios para atender às despesas de mesma natureza, cujo empenho será objeto de termo de apostilamento no início de cada exercício financeiro.

**PARÁGRAFO TERCEIRO:** A inexistência de créditos orçamentários no início de cada exercício financeiro impede a continuidade do ajuste, devendo a **CONTRATANTE** promover a extinção do **CONTRATO**, sem ônus, na forma dos Parágrafos Segundo e Terceiro da Cláusula Décima Sétima.

## CLÁUSULA SEXTA - DO REAJUSTE E DA REVISÃO

**PARÁGRAFO PRIMEIRO:** Os preços contratados são fixos e irrevogáveis no prazo de um ano, contado da data de elaboração do orçamento estimado, ocorrida em 07/11/2025.

**PARÁGRAFO SEGUNDO:** O preço do **CONTRATO** será reajustado em periodicidade anual contada a partir da data de elaboração do orçamento estimado, utilizando-se, para tanto, o Índice de Custo a

Tecnologia da Informação - ICTI, fornecido pelo IPEA, que incidirá exclusivamente em relação às obrigações iniciadas e concluídas após a ocorrência da anualidade, nos termos da Lei Estadual nº 17.555/2021 e do Decreto nº 52.153, de 17 de janeiro de 2022.

**PARÁGRAFO TERCEIRO:** A **CONTRATADA** deverá pleitear o reajuste de preços durante a vigência do **CONTRATO**, mediante requerimento formal, no prazo de até 12 (doze) meses após completado o período aquisitivo da anualidade, nos contratos de vigência inicial plurianual, e antes de eventual prorrogação, sob pena de, não o fazendo tempestivamente, ocorrer a preclusão do seu direito ao reajuste.

**PARÁGRAFO QUARTO:** Os pedidos de reajustamento deverão ser analisados e respondidos pela Administração no prazo máximo de até 60 (sessenta) dias, contados a partir da instrução completa do requerimento pela **CONTRATADA**.

**PARÁGRAFO QUINTO:** Caso, na data da prorrogação contratual, ainda não tenha sido analisado o pedido de reajuste tempestivamente formulado, deverá ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro ao reajustamento, sob pena de preclusão.

**PARÁGRAFO SEXTO:** O reajustamento será formalizado mediante apostilamento, exceto se a sua concessão coincidir com a prorrogação contratual, quando poderá ser formalizado por termo aditivo.

**PARÁGRAFO SÉTIMO:** O direito ao reajustamento poderá ser objeto de renúncia expressa, parcial ou integral, bem como de negociação entre as partes, com vistas a garantir a vantajosidade da manutenção do ajuste para o interesse público, nos termos do art. 6º da Lei Estadual nº 17.555, de 2021.

**PARÁGRAFO OITAVO:** Nos reajustes subsequentes ao primeiro, a anualidade será contada a partir da data do fato gerador que deu ensejo ao último reajuste concedido ou objeto de renúncia.

**PARÁGRAFO NONO:** Será assegurado o restabelecimento do equilíbrio econômico-financeiro inicial do **CONTRATO** em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do **CONTRATO** tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no **CONTRATO**.

**PARÁGRAFO DÉCIMO:** O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do **CONTRATO** e antes de eventual prorrogação, sob pena de preclusão.

**PARÁGRAFO DÉCIMO PRIMEIRO:** Os pedidos de restabelecimento do equilíbrio econômico-financeiro do **CONTRATO** deverão ser analisados e respondidos pela Administração no prazo máximo de até 90 (noventa) dias, contados a partir da instrução completa do requerimento pela **CONTRATADA**.

**PARÁGRAFO DÉCIMO SEGUNDO:** A extinção do **CONTRATO** não configura óbice para o reconhecimento do direito ao reajuste ou ao restabelecimento do equilíbrio econômico-financeiro **CONTRATO**, desde que requeridos tempestivamente, hipóteses em que serão concedidos a título de indenização por meio de Termo de Quitação.

**PARÁGRAFO DÉCIMO TERCEIRO:** Em situações excepcionais de flutuação atípica dos preços de mercado, quando a variação do índice adotado implicar em reajuste desproporcional, poderá ser negociada entre as partes a adoção de preço compatível, desde que previsto em edital ou contrato.

## CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATANTE

**PARÁGRAFO PRIMEIRO:** É dever da **CONTRATANTE** exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, em especial:

I.Prestar à **CONTRATADA** as informações e esclarecimentos que esta vier a solicitar para o desenvolvimento dos trabalhos;

II.Expedir ordem de serviço para o início da execução do **CONTRATO**, com a antecedência prevista no Termo de Referência ou, em sua ausência, observando prazo razoável para adoção das medidas iniciais a cargo da **CONTRATADA**;

III.Comunicar, por escrito, à **CONTRATADA** toda e qualquer ocorrência relacionada com a execução do serviço, inclusive vícios e incorreções, para que sejam corrigidos, no todo ou em parte, às suas expensas;

IV.Acompanhar e fiscalizar a execução do **CONTRATO**, através de fiscal especialmente designado para este fim;

V.Indicar, formalmente, o gestor do **CONTRATO** para acompanhamento da execução contratual, utilizando-se dos procedimentos de acompanhamento da execução dos serviços, conforme previsto no Termo de Referência e neste instrumento;

VI. Encaminhar à **CONTRATADA** os relatórios de acompanhamento da execução dos serviços, devidamente elaborados e assinados pelo fiscal do **CONTRATO**, com os registros de eventuais falhas verificadas e das medidas corretivas necessárias;

VII. Analisar e atestar as Faturas e Notas Fiscais emitidas e efetuar os respectivos pagamentos nas condições e nos prazos estabelecidos.

VIII. Liberar o pagamento da parcela incontroversa da execução do objeto contratado, quando houver controvérsia sobre a dimensão, qualidade e quantidade do objeto executado.

IX. Aplicar as sanções previstas na lei e neste **CONTRATO**;

X. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

XI. Proferir, no prazo de 30 (trinta) dias a contar da data do protocolo do requerimento, admitida a prorrogação motivada desse prazo por igual período, decisão explícita sobre todas as solicitações e reclamações relacionadas à execução do presente **CONTRATO**, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

XII. Responder a eventuais pedidos de reajustamento no prazo máximo de 60 (sessenta) dias e aos pedidos de restabelecimento do equilíbrio econômico-financeiro no prazo máximo de 90 (noventa) dias, contados a partir da instrução completa do requerimento.

XIII. Cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenha acesso em razão do certame ou do contrato administrativo, independentemente de declaração ou de aceitação expressa.

XIV. Comunicar à **CONTRATADA** qualquer alteração posterior do projeto feita pela **CONTRATANTE**, na situação descrita no art. 93, §3º, da Lei nº 14.133, de 2021;

XV. Além das obrigações listadas acima, serão requeridas as obrigações específicas dispostas no Adendo I do Termo de Referência (Das Obrigações da Contratada e da Contratante):

### **OBRIGAÇÕES DA CONTRATANTE**

1. A **CONTRATANTE** Principal possui as seguintes obrigações:

- 1.1. Prestar assessoramento no dimensionamento dos valores físicos e financeiros dos serviços contratados;
  - 1.2. Padronizar e formalizar as demandas e solicitações realizadas pelos CONTRATANTES aderentes;
  - 1.3. Controlar os fluxos contratuais junto aos Órgãos de Controle do Governo, bem como, junto a CONTRATADA e aos CONTRATANTES aderentes;
  - 1.4. Controlar, através da emissão de Ordens de Serviço, os limites contratuais Nova Rede Corporativa como um todo;
  - 1.5. Avaliar as condições do atendimento dos serviços de telemática, propor melhorias e estabelecer modelos visando a melhor execução destes serviços;
  - 1.6. Prover informações gerenciais referentes aos resultados dos serviços prestados pela Nova Rede Corporativa;
  - 1.7. Gerenciar e dar suporte ao controle da capacidade disponibilizada pelos recursos tecnológicos integrantes dos serviços contratados através da nova Rede, prestando assessoramento nas questões de qualidade, desempenho e inovação tecnológica, bem como, avaliando e aprovando os planos de implantação e o dimensionamento dos recursos técnicos para atendimento às solicitações;
- Acompanhar e analisar os registros das ocorrências, dos fatos relevantes e dos níveis de qualidade contratados, utilizando-se da solução de Sistemas Gerenciais previstos e dos relatórios emitidos.
- 1.8. Instaurar o processo de aplicação de penalidades para os casos de falhas e/ou atrasos na execução dos serviços da Nova Rede Corporativa e/ou que atinjam um ou mais de um CONTRATANTE aderente.

**2. A CONTRATANTE aderente Técnica tem como responsabilidade a Gestão Técnica Corporativa da nova Rede, contratando, hospedando e gerenciando os serviços de uso compartilhado, sendo suas obrigações:**

- 2.1. Efetuar os pagamentos relativos aos serviços formalmente contratados específicos à sua competência como Gerente Técnica da nova Rede, mediante efetiva comprovação dos serviços prestados aos órgãos do Poder Executivo, que dependem de recursos do Tesouro Estadual;

- 2.2. Adotar medidas visando um eficaz relacionamento com os fornecedores de serviços de telemática, de forma a ensejar o melhor desempenho e a melhor qualidade na prestação dos serviços contratados;
- 2.3. Fazer o acompanhamento da execução dos serviços contratados;
- 2.4. Analisar as questões relacionadas com o desenvolvimento dos serviços de telemática, identificando eventuais problemas e propondo medidas preventivas e corretivas;
- 2.5. Prestar apoio técnico aos usuários, acompanhando todos os serviços em fase de implantação, como também verificar e avaliar os serviços instalados e em operação;
- 2.6. Fornecer à SAD e às CONTRATANTES aderentes informações gerenciais e sobre fatos que possam levar à aplicação de penalidades contra qualquer fornecedor dos serviços da Nova Rede Corporativa, ou mesmo à rescisão do contrato;
- 2.7. Controlar e avaliar tecnicamente os serviços solicitados através das Ordens de Serviços formalizadas, bem como o acompanhamento da execução técnica destes serviços;
- 2.8. Acompanhar a execução das Ordens de Serviços, verificando, registrando, controlando suas conclusões e os eventos e ocorrências relacionados a estas, facilitando a interlocução entre os CONTRATANTES aderentes e a CONTRATADA, tendo como objetivo a efetiva conclusão dos serviços solicitados dentro dos requisitos exigidos;
- 2.9. Receber os serviços, observando os requisitos técnicos associados aos mesmos, em conformidade com todas as exigências especificadas nos itens e subitens deste Termo e seus Adendos;
- 2.10. Fornecer dados estatísticos referentes à utilização dos recursos da Nova Rede Corporativa;
- 2.11. Registrar formalmente às ocorrências e as falhas ocorridas nos serviços da da Nova Rede Corporativa;
- 2.12. Gerenciar, administrativamente e tecnicamente, as soluções operacionalizadas pela Nova Rede Corporativa, hospedando o conjunto no ambiente operacional denominado de Centro Integrado de Inteligência e Segurança Cibernética, que também atenderá as demandas repassadas via Service desk;

2.13. Deverá, durante o período de assunção da Nova Rede Corporativa de telemática, realizar imediatamente a retirada e/ou redução dos níveis dos serviços compartilhados da nova Rede à medida que os serviços da Nova Rede Corporativa forem sendo ativados;

2.14. Responsabilizar-se, em casos de danos decorrentes de culpa da CONTRATANTE, incluindo situações constatadas de mau uso, perda, roubo, furto ou extravio, pelos prejuízos causados aos equipamentos disponibilizados pela CONTRATADA, quando estes estiverem localizados em propriedades da CONTRATANTE, na execução dos serviços objeto deste Contrato. O ressarcimento será realizado com base nos preços praticados pelo mercado para um novo equipamento, igual ou similar, mediante apresentação à CONTRATANTE de documento de cotação com valores obtidos de, no mínimo, três empresas e respectiva Nota Fiscal de compra do novo equipamento.

### **3. Os CONTRATANTES aderentes têm as seguintes obrigações:**

3.1. Realizar a previsão orçamentária e financeira para lastrear os pagamentos dos serviços contratados, em conformidade com os respectivos exercícios financeiros, diretrizes e legislação vigente no âmbito dos Poderes que integram;

3.2. Formalizar o Termo de Adesão ao Contrato Mater nos prazos estipulados pela CONTRATANTE Principal;

3.3. Relacionar os serviços a serem contratados através do Adendo ao Termo de Adesão ao Contrato Mater;

3.4. Formalizar as Ordens de Serviços referente aos serviços solicitados nos seus respectivos Termos de Adesão;

3.5. Acompanhar a execução dos serviços solicitados, atestar e arcar com os devidos pagamentos dos serviços efetivamente executados;

3.6. Realizar as possíveis contestações de faturas, caso haja, suspendendo o pagamento e aguardando a resposta da CONTRATADA.

3.7. Efetuar os pagamentos relativos aos serviços contratados, mediante efetiva comprovação e atesto dos serviços prestados;

3.8. Atender às orientações e regras formalizadas pela CONTRATANTE Principal e pela CONTRATANTE aderente Técnica;

3.9. Designar servidor para cumprir a função de Gestor de Telemática, o qual deverá ser responsável pelos assuntos contratuais, orçamentários, financeiros, técnicos e operacionais, respectivamente, fiscalizando a execução físico-financeira, bem como, a qualidade da prestação dos serviços contratados de acordo com a legislação vigente;

3.10. Responsabilizar-se, em casos de danos decorrentes de culpa da CONTRATANTE, incluindo situações constatadas de mau uso, perda, roubo, furto ou extravio, pelos prejuízos causados aos equipamentos disponibilizados pela CONTRATADA, quando estes estiverem localizados em propriedades da CONTRATANTE, na execução dos serviços objeto deste Contrato. O ressarcimento será realizado com base nos preços praticados pelo mercado para um novo equipamento, igual ou similar, mediante apresentação à CONTRATANTE de documento de cotação com valores obtidos de, no mínimo, três empresas e respectiva Nota Fiscal de compra do novo equipamento;

3.11. A CONTRATANTE poderá emitir Notificação Extrajudicial, estipulando prazo específico para que se providenciem os instrumentos jurídicos necessários para a regularização contratual, sob pena de sofrer auditoria dos Órgãos de controle, além das consequências legais cabíveis, caso configure-se mora no processo de formalização contratual por parte do CONTRATANTE aderente, conforme item 2.3.2 do Adendo I do Termo de Referência;

3.12. Deverá, durante o período de assunção da Nova Rede Corporativa de telemática, realizar imediatamente a retirada dos serviços contratados da nova Rede à medida que os serviços contratados da Nova Rede Corporativa de corporativa forem ativados;

3.13. A CONTRATANTE estará isenta de responsabilização a partir da data de ciência por parte do CONTRATANTE aderente da Notificação Extrajudicial referida no item 2.3.11 do Adendo I do Termo de Referência.

## CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATADA

**PARÁGRAFO PRIMEIRO:** Deve a **CONTRATADA** cumprir todas as obrigações estipuladas neste **CONTRATO** e respectivos anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, em especial:

I.Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos, ferramentas e utensílios, na quantidade, qualidade e tecnologia demandadas, de acordo com as especificações indicadas no Termo de Referência;

II.Cumprir o cronograma de execução do **CONTRATO**;

III.Reparar, corrigir, complementar ou substituir, às suas expensas, no todo ou em parte, conforme o caso, no prazo de até XXX (XXXXX) dias úteis contado da respectiva notificação, ou no prazo fixado pelo fiscal do **CONTRATO**, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

IV.Submeter, por escrito, para análise e aprovação prévia da **CONTRATANTE**, quaisquer mudanças nos métodos executivos que fujam às especificações do TR, do memorial descritivo ou instrumento congênere;

V.Designar preposto que tenha poder para resolução de possíveis ocorrências durante a execução contratual, o qual deverá disponibilizar endereço de e-mail válido e número de telefone móvel que permita contato imediato com o fiscal do **CONTRATO** de forma permanente;

VI.Substituir o preposto designado se houver recusa motivada da **CONTRATANTE** quanto à anterior indicação;

VII.Atender às determinações regulares do fiscal do **CONTRATO** ou autoridade superior, prestando todos os esclarecimentos solicitados e atendendo prontamente às solicitações e reclamações formuladas;

VIII.Relatar ao fiscal do **CONTRATO**, por escrito, toda e qualquer ocorrência anormal afeta à prestação dos serviços;

IX.Comunicar à **CONTRATANTE**, no prazo máximo de 05 (cinco) dias úteis, qualquer alteração no Contrato Social ou no endereço comercial;

X.Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do **CONTRATO**;

XI.Comprovar, conforme o caso, no início da execução contratual e sempre que solicitado pelo fiscal, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, durante toda a vigência do **CONTRATO**, com a indicação dos empregados que preencheram as referidas vagas;

XII.Alocar os empregados necessários ao perfeito cumprimento do objeto deste **CONTRATO**, com habilitação e conhecimento adequados;

XIII. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

XIV. Não contratar, durante a vigência do **CONTRATO**, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente da **CONTRATANTE** ou de agente público que tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do **CONTRATO**, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

XV. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pela **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

XVI. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto, cuja inadimplência não transfere a responsabilidade à **CONTRATANTE** e não poderá onerar o objeto do **CONTRATO**, sendo que eventual pessoal alocado ao **CONTRATO** não terá qualquer vínculo empregatício com a **CONTRATANTE**;

XVII. Guardar sigilo sobre todas as informações obtidas em decorrência da execução do **CONTRATO** e cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenha acesso em razão do certame ou do contrato administrativo, independentemente de declaração ou de aceitação expressa;

XVIII. Manter, durante o prazo de vigência do **CONTRATO**, todas as condições de habilitação exigidas na licitação, inclusive sua inscrição no CADFOR-PE;

XIX. Realizar, conforme previsto no Termo de Referência, a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da **CONTRATANTE**;

XX. Realizar os serviços de manutenção e assistência técnica no local indicado no Termo de Referência;

XXI. Não transferir a outrem, no todo ou em parte, o objeto do **CONTRATO**, ressalvadas as hipóteses de subcontratação autorizada no Termo de Referência e neste **CONTRATO**;

**XXII.** Apresentar, suplementar ou estender a garantia de execução contratual, se exigível, no prazo assinalado no **CONTRATO**;

**XXIII.** Além das obrigações listadas acima, serão requeridas as obrigações específicas dispostas no Adendo I do Termo de Referência (Das Obrigações da Contratada e da Contratante):

**Obrigações aplicáveis a todos os lotes:**

1. A CONTRATADA obriga-se a executar os serviços na forma e termos reportados neste Termo, especificações técnicas e demais disposições contidas nos seus Adendos e Anexos, bem como, na sua proposta de preço. A CONTRATADA deverá constituir Unidade(s) Gerencial(is) que trate(m) tanto da área Contratual como também da área Técnica, com o objetivo de manter estreita ligação com a CONTRATANTE Principal (Secretaria de Administração - SAD) e a CONTRATANTE aderente Técnica (Agência Estadual de Tecnologia da Informação - ATI), respectivamente, a fim de assegurar a perfeita execução dos serviços contratados.
2. A CONTRATADA deve, no prazo de até 45 (quarenta e cinco) dias corridos contados a partir da emissão da OS do serviço CIISC, designar formalmente seu(s) representante(s) técnicos e gerenciais, com disponibilidade para atendimento presencial na cidade do Recife, capazes de atender a todas as necessidades administrativas oriundas do contrato, bem como aos assuntos técnicos relacionados à qualidade e quantidade da prestação dos serviços contratados. Além disso, durante toda a vigência do contrato, a CONTRATADA deve disponibilizar, não necessariamente nas dependências da CONTRATANTE Principal, um preposto para atividades técnico-administrativas, devidamente munido das ferramentas necessárias, que atue como interlocutor entre a CONTRATADA e a CONTRATANTE Principal, prestando o suporte necessário para a eficiente execução dos serviços.
3. A CONTRATADA deve planejar os serviços de forma a não interferir no andamento normal das atividades desenvolvidas no local e em seu entorno.
4. A CONTRATADA deve responder por todos os ônus e obrigações concernentes às legislações Fiscal, Previdenciária, Trabalhista e Comercial, inclusive os decorrentes de acidentes de trabalho.
5. A CONTRATADA deve responder financeiramente, sem prejuízo de medidas outras que possam ser adotadas, por quaisquer danos causados à União, Estado, Município ou terceiros, em razão da execução dos serviços.

6. A CONTRATADA deve manter, durante a prestação dos serviços, seus funcionários e subcontratados devidamente identificados por crachá, sempre que estiverem na execução de suas funções. Deve ainda manter sua equipe técnica sempre provida de veículos, EPI's, ferramental, instrumentos e equipamentos, devidamente aferidos e calibrados, adequados ao trabalho e em perfeitas condições de uso.
7. A CONTRATADA deve garantir que os prepostos indicados deverão participar da prestação do serviço do objeto contratado, admitindo-se a substituição por profissionais de experiência equivalente ou superior.
8. A CONTRATADA deve garantir a presença do seu referido preposto nas reuniões gerenciais mensais, realizadas com a CONTRATANTE Principal e com a CONTRATANTE aderente Técnica, para tratar do desempenho e das ocorrências surgidas a cada mês, referentes à Nova Rede Corporativa.
9. A CONTRATADA deve manter nos locais dos serviços, equipe técnica suficiente, formalmente designada, composta de profissionais habilitados e de capacidade comprovada, com capacidade para assumir perante uma auditoria ou fiscalização a responsabilidade técnica dos mesmos, inclusive com poderes para deliberar sobre qualquer determinação de emergência que se torne necessária.
10. A CONTRATADA deve manter nos locais dos serviços a serem instalados e/ou operacionalizados, além da equipe técnica retromencionada, auxiliares necessários ao perfeito controle dos padrões exigidos, assim como promover, às suas expensas e segundo as especificações e normas técnicas, o controle tecnológico dos equipamentos e materiais a serem empregados nos serviços.
11. A CONTRATADA deve facilitar a ação da auditoria a quem competir, atendendo as especificações contidas neste Termo, na inspeção dos serviços, prestando todas as informações e esclarecimentos solicitados, inclusive de ordem administrativa, bem como sobre os documentos relativos ao processo.
12. A CONTRATADA deve entregar à CONTRATANTE Principal e às CONTRATANTES aderentes, quando da entrega dos serviços por parte da CONTRATADA, o Termo de Recebimento correspondente, registrando todas as alterações e complementações efetuadas, caso houver, no decorrer do prazo contratual, observando, obrigatoriamente, as normas da CONTRATANTE Principal.

13. A CONTRATADA deve relatar oportunamente à CONTRATANTE Principal e às CONTRATANTES aderentes, ocorrências ou circunstâncias que possam acarretar dificuldades no desenvolvimento dos serviços.
14. A CONTRATADA deve dar à CONTRATANTE Principal e às CONTRATANTES aderentes, imediata ciência de fatos irregulares que venham a ocorrer durante a execução do Contrato.
15. A CONTRATADA deve prover os dados necessários para o devido acompanhamento dos processos que se façam necessários durante a execução do objeto desta licitação.
16. A CONTRATADA deve disponibilizar à CONTRATANTE, através de diversos meios eletrônicos, as informações atualizadas do andamento da execução dos serviços contratados na forma de Relatórios Gerenciais pertinentes, conforme especificados no Termo de Referência.
17. A CONTRATADA deve responsabilizar-se, em casos fortuitos e força maior, pelos prejuízos causados aos seus equipamentos disponibilizados.
18. A CONTRATADA deve fornecer os recursos técnicos e humanos, operacionais dentro dos requisitos exigidos neste Termo e seus adendos.
19. A CONTRATADA deve prover capacidade operacional suficiente para a plena prestação dos serviços de telemática da Nova Rede Corporativa, dentro da sua abrangência.
20. A CONTRATADA deve arcar com todos os custos relativos aos encargos sociais e obrigações trabalhistas e previdenciárias relativas da equipe empregada na execução dos serviços, bem como, impostos, taxas, emolumentos, seguros ou outros valores que incidam, direta ou indiretamente sobre os serviços ora contratados.
21. A CONTRATADA deve responder por danos causados à CONTRATANTE, ou a terceiros, decorrentes de falhas ou irregularidades na execução dos serviços.
22. A CONTRATADA deve manter, durante toda execução do contrato, as mesmas condições de habilitação e qualificação exigidas na licitação.
23. A CONTRATADA deve facilitar o acompanhamento e fiscalização dos serviços pela CONTRATANTE.
24. A CONTRATADA é a responsável pelo fornecimento de todos os serviços e recursos especificados nos itens e subitens do Termo de Referência, os quais serão devidamente formalizados a partir de instrumentos contratuais específicos, como Edital e seus Anexos.

25. A CONTRATADA deve fornecer os recursos técnicos, humanos e operacionais, dentro dos requisitos exigidos neste Termo e seus Adendos.
26. A CONTRATADA deve atender as Ordens de Serviços emitidas pela CONTRATANTE, dentro dos requisitos e prazos especificados e exigidos neste Termo.
27. A CONTRATADA deverá realizar a remessa de equipamentos ou componentes, às suas expensas, para a prestação do serviço de manutenção/conserto. Toda e qualquer despesa logística ou operacional será de responsabilidade da CONTRATADA.
28. A CONTRATADA deve providenciar a substituição temporária e/ou permanente, sem ônus para a CONTRATANTE, de todos os recursos técnicos necessários ao funcionamento da solução do serviço contratado, quando na constatação de uma falha.
29. A CONTRATADA deve realizar todos às configurações, ajustes, substituições e testes necessários dos recursos da solução adotada, para os serviços contratados da Nova Rede Corporativa, mantendo os mesmos em condições de pleno funcionamento.
30. A CONTRATADA deve prover, quando solicitado pela CONTRATANTE, laudo técnico identificando a causa da falha na prestação do serviço contratado e, quando for o caso, identificar o uso indevido por parte do usuário.
31. A CONTRATADA deve manter sempre atualizadas as informações referentes ao funcionamento dos serviços contratados, tais como status, cliente, local, data, hora etc., acessíveis à CONTRATANTE em sistema via Web.
32. A CONTRATADA deve utilizar ferramentas, equipamentos e recursos adequados, para a realização de análise, diagnóstico e correção de eventuais falhas na prestação dos serviços;
33. A CONTRATADA deve encaminhar aos CONTRATANTES aderentes, até o quinto dia útil do mês subsequente da efetiva execução dos serviços, as Notas Fiscais/Faturas correspondentes à prestação dos serviços contratados, contendo a descrição detalhada de cada serviço, para os devidos atestos e pagamentos, sendo estas através de Sistema via WEB, com possibilidade de extração no formato de planilha eletrônica, impressas e em meio digital gravadas no formato de arquivo (.txt), conforme modelo elaborado pela FEBRABAN, versão V3R0 ou mais recente, ou, alternativamente, no padrão XML - Nota Fiscal Eletrônica (NF-e), reconhecido nacionalmente para fins de validação fiscal e operacional.

34. A CONTRATADA deve fornecer ferramentas para controle e gestão de faturas, para o CONTRATANTE aderente, discriminadas e em formato eletrônico de planilha. Os acessos a essa ferramenta devem ser restritos, garantindo que somente cada CONTRATANTE aderente possa recuperar, consultar e manusear os dados do seu Órgão e vinculadas, com exceção da Secretaria de Administração (SAD), que poderá ter os mesmos direitos de acesso para todos os CONTRATANTES aderentes da Administração Pública Estadual.

35. A CONTRATADA deve responder a contestação, enviando a fatura, que está momentaneamente suspensa, com uma nova data de vencimento, com prazo de no mínimo 20 (vinte) dias, garantindo que os valores divergentes, caso haja, sejam descontados na fatura posterior.

36. A CONTRATADA deve registrar e atualizar todos os dados do faturamento referente aos serviços prestados, no sistema de informações de faturamento da CONTRATADA, visando e permitindo o acompanhamento por parte do CONTRATANTE aderente.

37. A CONTRATADA deve ceder à CONTRATANTE, em caráter definitivo, o direito patrimonial das bases de dados, e os respectivos SGBDs (Sistemas Gerenciadores de Banco de Dados), resultantes dos serviços executados durante a vigência do contrato, entendendo-se por resultados quaisquer bases de imagens, áudios, vídeos, estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

38. A CONTRATADA deve observar o Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014) que fala da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas, da Da Guarda de Registros de Conexão, da Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão, Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações , Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros, Da Requisição Judicial de Registros e da ATUAÇÃO DO PODER PÚBLICO.

39. A CONTRATADA deve manter processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27002, item 5.12 – Classificação da Informação, processo necessário segundo o Decreto Nº 7.845/2012, Capítulo III, Do Tratamento de Informação Classificada. Esta classificação da informação deve ser acessível à CONTRATANTE.

40. A CONTRATADA deve manter processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da

informação, item 8.2 – Avaliação do risco de segurança da informação. Este item fornece diretrizes sobre como identificar, avaliar e tratar riscos relacionados à segurança da informação.

41. A CONTRATADA deve nomear responsável pela segurança da informação, à semelhança das orientações contidas na ISO/IEC 27002:2022, Controle 5.2 aborda a implementação e gestão de responsabilidades de segurança da informação.

42. A CONTRATADA deve seguir as políticas de segurança da informação que forem desenvolvidas no item de evolução de maturidade em segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27002 – Política de segurança da informação.

43. A CONTRATADA deve dar ciência à CONTRATANTE, formal e imediatamente, sobre qualquer anormalidade verificada referente à propriedade, sigilo e segurança das informações durante a prestação dos serviços.

44. A CONTRATADA deve guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da CONTRATANTE, sendo vedada à sua cessão, locação ou venda a terceiros sem prévia autorização formal da CONTRATANTE Principal.

45. A CONTRATADA deve zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

46. A CONTRATADA deve estar cientes de que a estrutura computacional da CONTRATANTE não poderá ser utilizada para fins particulares.

47. A CONTRATADA deve entregar à CONTRATANTE toda e qualquer documentação produzida decorrente da prestação de serviços, objeto desta licitação, bem como, ceder à CONTRATANTE, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia.

48. A CONTRATADA deverá disponibilizar à CONTRATANTE, a qualquer tempo, mediante solicitação, de forma imediata ou no prazo máximo definido pela CONTRATANTE, toda e qualquer informação, dado, registro, log, configuração, documentação técnica, inventário, métricas, relatórios, bases de

dados e demais elementos relacionados aos serviços contratados e à infraestrutura da Nova Rede Corporativa da CONTRATANTE, independentemente do estado de adimplência contratual, incluindo situações de inadimplemento, suspensão de pagamentos, rescisão ou encerramento contratual;

48.1. Para fins deste item, todas as informações, dados e registros, ainda que armazenados, processados ou geridos em ambientes, sistemas ou plataformas sob responsabilidade ou domínio da CONTRATADA, serão considerados de propriedade exclusiva da CONTRATANTE, não podendo ser retidos, restringidos, condicionados, indisponibilizados ou utilizados como mecanismo de garantia, pressão ou compensação contratual;

48.2. Consideram-se abrangidos por esta obrigação quaisquer artefatos informacionais produzidos pela CONTRATADA a partir de dados da CONTRATANTE ou de sua operação, incluindo análises, consolidações, enriquecimentos, correlações, indicadores, inteligência operacional, modelos, scripts, parametrizações e quaisquer outras formas de tratamento ou transformação da informação;

48.3. A CONTRATADA deverá garantir que tais informações sejam fornecidas em formato aberto, estruturado, legível e passível de reutilização, sem qualquer tipo de bloqueio tecnológico, criptográfico ou dependência de ferramentas proprietárias que impeçam ou dificultem seu acesso e uso pela CONTRATANTE.

49. A CONTRATADA deve informar à CONTRATANTE sobre qualquer acesso indevido, invasão ou ataque sofrido nos servidores ou serviços onde estejam hospedados cada solução CONTRATADA.

50. A CONTRATADA deve instalar e operacionalizar todos os serviços referentes ao respectivo Lote, conjuntamente com a CONTRATADA dos serviços ofertados na solução da nova Rede, até a completa finalização da assunção de todos os serviços para Nova Rede Corporativa.

51. A CONTRATADA, deve fornecer e manter a versão mais recente de todos os componentes (hardware e software) das soluções CONTRATADAS.

52. A CONTRATADA deve fornecer AS Built com toda documentação técnica completa e original de todos os componentes fornecidos da prestação dos serviços, quando solicitado pela CONTRATANTE, em língua portuguesa, em meio impresso e/ou meio eletrônico. Quaisquer atualizações da documentação devem ser fornecidas, sem ônus para a CONTRATANTE, durante a vigência do contrato.

53. A CONTRATADA deve realizar a configuração de todos os equipamentos fornecidos nas soluções da Nova Rede Corporativa e a integração ao ambiente atual da nova Rede.
54. A CONTRATADA deve realizar vistoria no ambiente da CONTRATANTE aderente, quando da instalação de novos serviços, para levantamento de dados do referido ambiente e adequação dos mesmos, conforme exigências do Termo de Referência.
55. São de responsabilidade da CONTRATADA os custos referentes à energia elétrica para o funcionamento das soluções que eventualmente envolvam serviços instalados em via pública.
56. A CONTRATADA deve manter os técnicos encarregados dos serviços de manutenção e assistência técnica previamente relacionados, para ter livre acesso aos recursos inerentes à prestação dos serviços da Nova Rede Corporativa, a fim de executar os serviços de manutenção, respeitando as normas de segurança vigentes e as da CONTRATANTE aderente.
57. A CONTRATADA deve entregar lista dos profissionais, juntamente com as cópias de suas identidades funcionais, com foto, aos gestores de cada CONTRATANTE aderente, de modo que sejam devidamente cadastrados para acesso às suas dependências. Esta lista deverá ser atualizada e redistribuída sempre que houver alteração no quadro funcional da CONTRATADA.
58. A CONTRATADA deve fornecer relatórios específicos para cada CONTRATANTE, contendo as informações relativas aos serviços contratado, de acordo com as especificações do Termo de Referência.
59. A CONTRATADA será a responsável pelo fornecimento de todos os serviços e recursos especificados nos itens e subitens do Termo de Referência, o qual será devidamente, formalizado a partir de instrumentos contratuais específicos, conforme Edital e seus anexos.
60. A CONTRATADA deve atender obrigatoriamente a todos os requisitos, prazos e especificações técnicas, para prestação dos serviços da Nova Rede Corporativa.
61. As obrigações acima listadas não excluem outras eventualmente listadas no Termo de Referência.

**Obrigações aplicáveis ao LOTE 01:**

1. A CONTRATADA deve substituir qualquer integrante da equipe técnica, caso esteja alocado nas instalações da CONTRATANTE, durante a execução dos serviços, somente após a anuência da

CONTRATANTE Principal e das CONTRATANTES aderentes, mediante a comprovação de experiência equivalente ou superior do substituto proposto.

2. A CONTRATADA deve cumprir os prazos e condições contidos no item de Plano de Assunção dos serviços em operação conforme item e subitens correspondentes no Termo de Referência.

3. A CONTRATADA deve apresentar todas às Notas Fiscais de remessa dos equipamentos de Telemática providos para a prestação de todos os serviços da Nova Rede Corporativa, no momento da entrega e aceite, pelos gestores, desses serviços, onde todas as referidas NF de remessa, acima citadas.

4. A CONTRATADA deve manter processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27002, item 7.1 – Inventário de ativos. A base com estas informações deve ser acessível à CONTRATANTE.

5. Obrigações Relacionadas a Implementação das Soluções e Suporte junto com os Fabricantes:

5.1. Suporte Diferenciado do Fabricante para as soluções abaixo mencionadas:

5.1.1. Solução unificada de segurança de rede;

5.1.2. Serviço de rede sem fio com segurança (interno, externo e temporário);

5.1.3. Solução para gerenciamento de acessos à rede;

5.1.4. Solução de proteção, detecção e resposta para servidores;

5.1.5. Solução de segurança de confiança zero;

5.1.6. Solução de proteção, detecção e resposta para dispositivos de tráfego de rede;

5.1.7. Solução de segurança de identidade privilegiada;

5.1.8. Solução de filtro de mensagens indesejadas;

5.1.9. Solução de filtro de aplicações WEB;

5.1.10. Solução de monitoramento e análise de eventos de segurança;

5.1.11. Solução de automação de resposta a incidentes de segurança;

5.1.12. Solução para guarda de LOGs.

5.2. A CONTRATADA deverá garantir que todas as soluções fornecidas possuam contrato ativo de suporte técnico junto ao fabricante, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), em nível corporativo (enterprise ou equivalente), contemplando, no mínimo:

5.2.1. Abertura ilimitada de chamados técnicos junto ao fabricante;

5.2.2. Atendimento em regime ininterrupto (24x7);

5.2.3. Suporte para diagnóstico, troubleshooting, correção de falhas e orientação técnica especializada;

5.2.4. Acesso a atualizações, patches, correções de segurança e upgrades de software/firmware;

5.2.5. Escalonamento para níveis avançados de suporte do fabricante, conforme severidade e criticidade do incidente;

5.2.6. A CONTRATADA será responsável por registrar, acompanhar, gerenciar e realizar o devido escalonamento dos chamados técnicos junto aos fabricantes;

5.2.7. Para incidentes críticos, a CONTRATADA deverá disponibilizar relatórios de análise de causa raiz (Root Cause Analysis – RCA), elaborados com base nas informações técnicas disponíveis, incluindo, sempre que aplicável, análise e contribuições do fabricante, contendo, no mínimo:

5.2.7.1. identificação da causa do incidente;

5.2.7.2. ações corretivas adotadas;

5.2.7.3. recomendações para prevenção de recorrência.

5.2.8. A CONTRATADA deverá garantir comunicação contínua com os fabricantes, assegurando a coleta e a pronta disponibilização à CONTRATANTE de boletins técnicos, notificações de vulnerabilidades, atualizações críticas e demais informações relevantes que possam impactar a segurança, estabilidade ou desempenho das soluções;

5.2.9. A CONTRATADA deverá garantir que todas as atualizações de software e firmware sejam precedidas de análise técnica quanto ao impacto no ambiente;

5.2.10. Sempre que demandado pela CONTRATANTE, a CONTRATADA deverá viabilizar a participação do fabricante em reuniões técnicas para apoio na análise de incidentes, esclarecimentos técnicos ou evolução da solução;

5.2.11. A CONTRATADA deverá assegurar o alinhamento técnico entre CONTRATANTE, CONTRATADA e fabricante para definição do High Level Design (HLD) e implantação da arquitetura, contemplando requisitos de rede, segurança, alta disponibilidade e aderência às melhores práticas;

5.2.12. A CONTRATADA deverá acionar o suporte especializado do fabricante, inclusive com atuação hands-on, sempre que necessário, durante a fase de implantação ou operação, garantindo a correta configuração e aderência às boas práticas e aos requisitos do projeto.

6. A CONTRATADA será responsável por toda a infraestrutura interna (física e elétrica) necessária ao PCS, restrita à infraestrutura para a implantação e operação do serviço contratado/solução adotada.

6.1. A CONTRATADA deve projetar, instalar, manter e atualizar toda a infraestrutura física interna do PCS (endereço/site) necessária para instalar e operar os equipamentos do projeto que atenderão ao serviço contratado. Todas as instalações devem seguir rigorosamente as normas e padrões técnicos aplicáveis, garantindo segurança, confiabilidade e desempenho da rede. As responsabilidades da CONTRATADA incluem assegurar a conformidade com os requisitos estabelecidos para a infraestrutura física, conforme detalhado a seguir:

6.1.1. Rede Interna (LAN): Fornecimento e organização do cabeamento estruturado, utilizando par trançado Cat 6A ou superior e fibra óptica, conforme a necessidade técnica. O cabeamento deverá suportar conexões de 2,5 Gbps e 10 Gbps, incluindo backhaul da rede sem fio, garantindo compatibilidade por meio de conversores de mídia quando necessário. A infraestrutura deverá incluir patch panels, racks, organizadores de cabos, tampas cegas e demais acessórios seguindo as normas ANSI/TIA-568.2-D e ISO/IEC 11801.

6.1.2. Conversores de Mídia: A CONTRATADA será responsável pelo fornecimento, instalação e configuração de conversores de mídia sempre que necessário para garantir a integração entre os diferentes meios físicos da infraestrutura de conectividade e da rede sem fio. Os conversores deverão ser compatíveis com interfaces de fibra óptica (monomodo e multimodo) e cabeamento em par trançado (Cat 6A ou superior), suportando velocidades de 2,5 Gbps e 10 Gbps, conforme a necessidade do ambiente. Deverão atender aos padrões IEEE 802.3bz (2,5GBASE-T), IEEE 802.3an (10GBASE-T) e IEEE 802.3ae (10GBASE-SR/LR).

6.1.3. Conexões e Conectores: Fornecer e instalar conectores RJ45 de alta qualidade, adaptadores ópticos adequados e, quando necessário, módulos ópticos (GBICs/SFP/SFP+/XFP) compatíveis com

os equipamentos utilizados na solução. Os módulos fornecidos deverão atender às especificações de velocidade e tipo de fibra exigidos para cada ambiente, incluindo padrões como LC, SC e MPO, conforme necessidade, seguindo as Normas/Padrões: ISO/IEC 11801, ANSI/TIA-568.2-D, IEC 61754.

6.1.4. Calhas e Canaletas: Para acomodação segura dos cabos, evitando interferências e danos físicos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

6.1.5. Organizadores de Cabos: Utilização de organizadores de cabos para evitar emaranhados e facilitar a manutenção. Conforme Normas/Padrões: ANSI/TIA-568.2-D.

6.1.6. Racks e Gabinetes: Racks apropriados para montagem e organização dos equipamentos de rede. Conforme Normas/Padrões: EIA-310-D, IEC 60297.

6.1.7. Etiquetagem e Documentação: Todos os cabos, conexões e equipamentos devem ser devidamente etiquetados e documentados. Conforme Normas/Padrões: ANSI/TIA-606-C (Administration Standard for Telecommunications Infrastructure).

6.1.8. Patch Panels: Utilização de patch panels para a terminação de cabos de rede, permitindo fácil gerenciamento e organização das conexões. Conforme Normas/Padrões: ANSI/TIA-568.2-D.

6.1.9. Testes e Certificações de Cabos: Realização de testes e certificações de todos os cabos instalados para garantir a conformidade com os padrões de desempenho especificados. Conforme Normas/Padrões: ANSI/TIA-1152-A (Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling).

6.2. A CONTRATADA é responsável pela infraestrutura elétrica necessária para instalar todos os aparelhos e equipamentos do projeto que atenderão ao serviço contratado, devendo projetar, implementar e manter essa infraestrutura de forma a assegurar a segurança e eficiência energética. As instalações elétricas devem seguir as normas e padrões técnicos estabelecidos, garantindo a qualidade e conformidade do serviço. As responsabilidades da CONTRATADA para a infraestrutura elétrica são detalhadas a seguir:

6.2.1. Tomadas: Instalação de tomadas adequadas para todos os aparelhos e equipamentos, com número suficiente para evitar sobrecarga. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

6.2.2. **Aterramento:** Sistema de aterramento adequado para proteger os equipamentos contra surtos e descargas elétricas. Conforme Normas/Padrões: NBR 5419 (Proteção contra Descargas Atmosféricas).

6.2.3. **Estabilizadores:** Estabilizadores de tensão para garantir a alimentação elétrica estável dos equipamentos de rede. Conforme Normas/Padrões: IEC 62040 (Uninterruptible power systems – UPS).

6.2.4. **No-Breaks (UPS):** Sistemas de alimentação ininterrupta para garantir a continuidade do serviço em caso de falha de energia, com autonomia mínima de 15 minutos. Conforme Normas/Padrões: IEC 62040 (Uninterruptible power systems – UPS).

6.2.5. **Cabos Elétricos:** Utilização de cabos elétricos de qualidade, dimensionados corretamente para suportar a carga dos equipamentos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

6.2.6. **Quadro de Distribuição:** Instalação de quadros de distribuição elétrica para organizar e proteger os circuitos elétricos. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

6.2.7. **Disjuntores:** Utilização de disjuntores adequados para proteção contra sobrecorrente e curto-circuito. Conforme Normas/Padrões: NBR 5361 (Disjuntores).

6.2.8. **Proteção contra Interferências Eletromagnéticas (EMI):** Adoção de medidas para minimizar as interferências eletromagnéticas que podem afetar o desempenho da rede. Conforme Normas/Padrões: IEC 61000 (Electromagnetic Compatibility).

6.2.9. **Isolamento e Proteção de Cabos:** Uso de materiais isolantes e proteções adequadas para os cabos elétricos, evitando danos e riscos de curto-circuito. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 60332 (Testes de cabos elétricos).

6.2.10. **Proteção contra Desbalanceamento de Cargas:** Implementação de medidas para prevenir e corrigir desbalanceamento entre fase-terra-neutro e outros problemas elétricos que podem impactar no bom funcionamento dos equipamentos. A responsabilidade pela correção de quaisquer problemas detectados, tanto na instalação quanto na manutenção, será da CONTRATADA, devendo seguir Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 61000-4-30 (Compatibilidade Eletromagnética - Parte 4-30: Técnicas de Medição de Qualidade da Energia Elétrica).

6.2.11. Manutenção Preventiva e Corretiva: Realização de manutenção preventiva e corretiva de toda a infraestrutura elétrica para garantir a continuidade e segurança dos serviços. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão).

6.2.12. Filtros de Linha com Tomadas Adicionais: Permissão para o uso de filtros de linha com tomadas adicionais, desde que dimensionados para não ocasionar sobrecargas. Estes devem seguir as normas de segurança específicas para garantir que não causem incidentes. Conforme Normas/Padrões: NBR 14136 (Plugues e Tomadas para Uso Doméstico e Similar), NBR 13571 (Fios e Cabos Elétricos).

6.2.13. Prevenção e correção contra fuga de corrente (baixa isolação, folgas em bornes, cabos e conectores etc.), mau aterramento etc.): Adoção de medidas para garantir a melhor proteção dos cabos e componentes elétricos, prevenindo riscos de curto-circuito e falhas na rede. Conforme Normas/Padrões: NBR 5410 (Instalações Elétricas de Baixa Tensão), IEC 60228 (Conductors of Insulated Cables).

6.3. A CONTRATADA poderá utilizar a infraestrutura elétrica e física interna preexistente, desde que esta atenda integralmente aos requisitos de qualidade e normas aplicáveis. Neste caso, a CONTRATADA assumirá a responsabilidade pela manutenção preventiva e corretiva da infraestrutura utilizada.

6.1.2.7. A CONTRATADA é responsável pelo fornecimento de um kit mínimo infraestrutura que garanta o perfeito funcionamento de todos os equipamentos da solução ofertada, assegurando a qualidade de entrega do serviço. O kit mínimo de ativação deve incluir:

6.1.2.7.1. Rack para armazenamento de todos equipamentos e elementos elétricos de proteção (filtro de linha, no-break e estabilizador).

6.1.2.7.2. Infraestrutura elétrica completa, incluindo tomadas e proteções elétricas adequadas.

6.1.2.7.3. No-break obrigatório para todos os PCs.

6.1.2.7.4. Materiais elétricos e de rede interna necessários para instalação e operação dos equipamentos.

6.1.2.8. Disposições Específicas para Serviços de Natureza Temporária

6.1.2.8.1. Considerando as características operacionais específicas de determinados serviços temporários contratados no âmbito da Nova Rede Corporativa do Estado de Pernambuco, aplicam-se as condições excepcionais previstas neste item às seguintes modalidades:

- Serviço de Rede Sem Fio Temporário com Segurança, conforme previsto no ADENDO IV – SERVIÇO DE REDE SEM FIO;
- Link de Acesso Temporário (LAT) – Tipo 1, Tipo 2 e Tipo 3, conforme previsto no ADENDO V – SERVIÇO DE CONECTIVIDADE DE REDE LOCAL.

6.1.2.8.2. Para os serviços elencados no subitem anterior, o faturamento mínimo será sempre correspondente a 30 (trinta) dias corridos, ainda que o período efetivo de utilização seja inferior, como em casos de eventos pontuais, ações emergenciais ou projetos de curta duração.

6.1.2.8.3. Para viabilizar agilidade na ativação e economicidade nas execuções temporárias, fica autorizada a utilização de equipamentos com uso prévio, desde que:

- Estejam em perfeito estado de funcionamento;
- Sejam livres de danos aparentes;
- Estejam atualizados com as versões mais recentes de firmware ou software do fabricante;
- Atendam integralmente às exigências técnicas, funcionais e de segurança dispostas no Termo de Referência de Referência e nos respectivos Adendos vinculados aos serviços.

6.1.2.8.4.A exceção prevista no item 9.3 abrange também os equipamentos e soluções integrantes da Solução Unificada de Segurança de Rede de Última Milha – Tipo 1 ou Tipo 2, conforme especificado no ADENDO III – SEGURANÇA DE REDE LOCAL, quando estes forem utilizados em conjunto com os serviços temporários listados no item 9.1. Nestes casos, o faturamento da UTM seguirá as mesmas condições do serviço temporário associado, com faturamento mínimo de 30 (trinta) dias corridos e limitado ao período de utilização do respectivo serviço temporário.

6.1.2.8.5.Os serviços de natureza temporária citados neste item, bem como as respectivas soluções de segurança associadas conforme disposto no item 9.4, não estarão sujeitos à carência mínima de 6 (seis) meses prevista no Termo de Referência para os demais serviços. Para estes casos, a carência mínima será de 30 (trinta) dias corridos, contados a partir da ativação do serviço.

6.1.2.9. O faturamento dos serviços será permitido exclusivamente para os itens previstos na Tabela de Preços constante do Termo de Referência, vedando-se qualquer cobrança adicional por atividades acessórias ou operacionais.

6.1.2.10. A execução dessas atividades deverá ocorrer de forma organizada e sem impacto na continuidade dos serviços prestados pela CONTRATANTE, respeitando as normas e boas práticas aplicáveis. A CONTRATADA deverá planejar, documentar e comunicar previamente quaisquer intervenções, garantindo total transparência e alinhamento com os gestores responsáveis.

6.1.2.11. O descumprimento dos prazos ou a não realização das atividades conforme as especificações poderá resultar em glosas, penalidades contratuais e demais sanções cabíveis, conforme previsto no Termo de Referência e na regulamentação vigente.

6.1.2.12. A CONTRATADA deverá implementar, manter, operar e evidenciar a execução dos processos e controles descritos a seguir, em conformidade com as melhores práticas de gestão de serviços de TI, alinhadas à ISO/IEC 20000-1:2018 ou versão superior aplicável, assegurando sua efetividade, mensurabilidade, rastreabilidade e aderência contínua. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

6.1.2.12.1. Implementação e manutenção de um Sistema de Gestão de Serviços (SGS) formalmente documentado, com escopo definido, controle de versões e mecanismo de melhoria contínua;

6.1.2.12.2. Estabelecimento, aprovação e divulgação de política de gestão de serviços, alinhada aos objetivos institucionais da CONTRATANTE;

6.1.2.12.3. Definição formal de papéis, responsabilidades e autoridades, incluindo proprietários de processos e responsáveis por controles;

6.1.2.12.4. Manutenção de catálogo de serviços atualizado, contendo descrição, escopo, requisitos, dependências, níveis de serviço e público-alvo;

6.1.2.12.5. Processo estruturado para planejamento, transição, validação e entrada em operação de novos serviços ou alterações;

6.1.2.12.6. Elaboração, testes periódicos e manutenção de planos de continuidade e recuperação de serviços de TI críticos;

- 6.1.2.12.7. Procedimentos formalizados para resposta a incidentes graves e desastres, incluindo tempos de recuperação (RTO) e ponto de recuperação (RPO);
- 6.1.2.12.8. Processo de gerenciamento de incidentes com registro, categorização, priorização, escalonamento, resolução e encerramento formal;
- 1.2.12.9. Processo de gerenciamento de requisições de serviço com definição de critérios de priorização, prazos e fluxo de atendimento;
- 1.2.12.10. Processo de gerenciamento de problemas com identificação de causa raiz, base de erros conhecidos e ações de mitigação;
- 1.2.12.11. Processo de habilitação de mudanças com avaliação de risco, aprovação formal, plano de rollback e revisão pós-implementação;
- 1.2.12.12. Gerenciamento de implantações com controle de versões, testes, validação e autorização prévia para entrada em produção;
- 1.2.12.13. Gerenciamento de configuração e ativos de serviço, com inventário atualizado, controle de itens de configuração (CIs) e mapeamento de dependências;
- 1.2.12.14. Processo de gerenciamento de acesso, com concessão, revisão periódica e revogação de acessos baseada em perfis e segregação de funções;
- 1.2.12.15. Monitoramento contínuo de serviços, infraestrutura e processos, com geração de alertas e tratamento proativo de eventos;
- 1.2.12.16. Definição, apuração e reporte de indicadores de desempenho (KPIs) e níveis de serviço (SLAs), com análise crítica periódica;
- 1.2.12.17. Processo estruturado de comunicação com a CONTRATANTE, incluindo tratamento de reclamações, solicitações e feedbacks;
- 1.2.12.18. Planejamento e execução de auditorias internas periódicas do SGS, com registro de evidências e planos de ação;
- 1.2.12.19. Processo de tratamento de não conformidades, com ações corretivas e preventivas, análise de causa e acompanhamento de eficácia;
- 1.2.12.20. Programa contínuo de capacitação, com trilhas de treinamento, avaliação de eficácia e registro formal;

1.2.12.21. Processo de gestão de fornecedores envolvidos na prestação do serviço, incluindo avaliação de desempenho e conformidade;

1.2.12.22. Gestão de riscos aplicada ao SGS, com identificação, análise, tratamento e monitoramento contínuo dos riscos;

1.2.12.23. Controle documental e de registros do SGS, garantindo integridade, confidencialidade, disponibilidade e versionamento;

1.2.12.24. Todos os processos e controles deverão ser suportados pela ferramenta de ITSM, garantindo rastreabilidade ponta a ponta;

1.2.12.25. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados.

1.2.13. A CONTRATADA deverá fornecer documentação técnica completa, atualizada e rastreável, de forma progressiva, ao término de cada fase, entrega técnica ou ativação relevante, bem como na implantação integral do objeto, incluindo obrigatoriamente documentação do tipo AS BUILT, refletindo fielmente a configuração efetivamente implantada.

1.2.13.1. A documentação AS BUILT deverá contemplar, no mínimo, quando aplicável ao serviço entregue:

1.2.13.1.1. Diagramas lógicos e físicos atualizados da rede;

1.2.13.1.2. Topologia detalhada (LAN, WAN, WLAN, backbone, interligações, redundâncias);

1.2.13.1.3. Endereçamento IP, VLANs, rotas e políticas de roteamento;

1.2.13.1.4. Configurações de equipamentos ativos (switches, roteadores, firewalls, controladoras, etc.);

1.2.13.1.5. Políticas implementadas (ACLs, regras de firewall, segmentações, QoS, etc.);

1.2.13.1.6. Inventário completo de ativos instalados, com modelo, número de série, firmware/versão e localização física;

1.2.13.1.7. Mapeamento de portas físicas e lógicas;

1.2.13.1.8. Documentação de integrações com sistemas externos;

1.2.13.1.9. Registro de parametrizações específicas realizadas;

1.2.13.1.10. Relação de licenças instaladas e respectivas vigências;

1.2.13.1.11. Registro de eventuais customizações técnicas executadas;

1.2.13.1.12. A documentação prevista no ADENDO XV para encerramento e consolidação documental.

1.2.13.2. A documentação relativa a cada ativação/fase/entrega deverá ser disponibilizada em até 15 (quinze) dias corridos após o respectivo aceite/homologação pela CONTRATANTE, ou conforme marco equivalente definido no Plano do Projeto, podendo a CONTRATANTE sustar o pagamento da respectiva entrega ou fase até a regularização da documentação.

1.2.13.3. A documentação final consolidada (AS BUILT completo e inventário final), correspondente ao encerramento do Plano de Assunção, deverá ser entregue em até 30 (trinta) dias corridos após a conclusão formal da assunção, sem prejuízo das entregas progressivas, podendo a CONTRATANTE sustar o pagamento da respectiva entrega até a regularização da documentação.

1.2.13.4. Toda a documentação deverá ser entregue em língua portuguesa, em formato digital aberto e editável, com versionamento e histórico de alterações, e atualizada sempre que houver modificação relevante na infraestrutura.

1.2.13.5. A documentação técnica entregue pela CONTRATADA poderá ser submetida à verificação técnica pela CONTRATANTE, com o objetivo de validar sua aderência à infraestrutura efetivamente implantada.

1.2.13.5.1. Caso sejam identificadas inconsistências, omissões ou divergências em relação ao ambiente operacional, a CONTRATADA deverá realizar as correções necessárias no prazo máximo de 10 (dez) dias corridos, sem ônus adicional para a CONTRATANTE.

1.2.13.6. A ausência ou inconsistência da documentação técnica poderá caracterizar inexecução parcial da entrega, sujeitando a CONTRATADA às medidas administrativas cabíveis, conforme previsto no Termo de Referência e no instrumento contratual.

1.2.14. A CONTRATADA será integralmente responsável pelo fornecimento, emissão, renovação, revogação, instalação, configuração e gestão de todos os certificados digitais necessários ao pleno funcionamento da Nova Rede Corporativa, independentemente da tecnologia, módulo ou

componente envolvido (incluindo, mas não se limitando a UTM, NAC, ZTNA, WAF, VPN, portais web, APIs, integrações e demais serviços do Termo de Referência e seus adendos);

1.2.14.1 Os certificados deverão:

1.2.14.1.1. Ser válidos e emitidos por Autoridades Certificadoras confiáveis (públicas ou privadas), conforme o caso de uso;

1.2.14.1.2. Atender aos requisitos de segurança vigentes, incluindo uso de algoritmos e tamanhos de chave aderentes às boas práticas de mercado;

1.2.14.1.3. Garantir suporte a criptografia forte, vedado o uso de protocolos e cifras obsoletas ou consideradas inseguras;

1.2.14.1.4. Ser providos sem ônus adicional à CONTRATANTE, inclusive quanto a licenciamento, cadeia de certificação e renovações durante toda a vigência contratual;

1.2.14.1.5. Permitir sua utilização para todos os cenários da Nova Rede Corporativa, incluindo autenticação de usuários, dispositivos, serviços, inspeção de tráfego criptografado, publicação segura de aplicações e estabelecimento de túneis criptográficos;

1.2.14.1.6. Possibilitar revogação imediata em caso de comprometimento, bem como rotação periódica conforme políticas de segurança;

1.2.14.1.7. Ser plenamente compatíveis com navegadores seguros amplamente utilizados no mercado, bem como com os sistemas operacionais já especificados ao longo do Termo de Referência e seus respectivos adendos, e com as integrações corporativas utilizadas pela CONTRATANTE;

1.2.14.2. A CONTRATADA deverá garantir que não haja interrupção de serviço decorrente de expiração, má configuração ou ausência de certificados digitais, sendo responsável pela gestão proativa de seu ciclo de vida.

1.2.15. Gestão de Ciclo de Vida, Suporte e Licenciamento dos Equipamentos e Soluções:

1.2.15.1. A CONTRATADA deverá garantir que todos os equipamentos, sistemas, softwares, firmwares, licenças e componentes das soluções fornecidas e operadas no âmbito do LOTE 01 permaneçam, durante toda a vigência contratual, dentro de seu ciclo de vida suportado pelo fabricante, observando rigorosamente as políticas oficiais de End of Life (EoL), End of Support (EoS), End of Service Life (EoSL), End of Sale (EoSale) ou equivalentes;

1.2.15.2. A CONTRATADA deverá realizar o acompanhamento contínuo do ciclo de vida dos ativos, mantendo controle atualizado sobre datas de fim de comercialização, datas de fim de suporte

técnico, datas de fim de atualizações de segurança, situação de licenciamento, subscrição e contratos de suporte;

1.2.15.3. Não será admitida, em nenhuma hipótese, a operação de equipamentos ou soluções que:

1.2.15.3.1. Estejam fora do período de suporte do fabricante;

1.2.15.3.2. Não recebam atualizações de segurança;

1.2.15.3.3. Possuam licenças expiradas, suspensas ou em desacordo com os termos contratuais ou do fabricante.

1.2.15.4. A CONTRATADA deverá planejar e executar a substituição, atualização ou migração de quaisquer equipamentos, softwares ou soluções que se aproximem ou atinjam o fim de seu ciclo de vida suportado, de forma proativa, garantindo continuidade dos serviços, manutenção dos níveis mínimos de serviço e preservação da segurança da informação, desempenho e estabilidade do ambiente;

1.2.15.5. A CONTRATADA deverá comunicar formalmente à CONTRATANTE, com antecedência mínima de 6 (seis) meses, a ocorrência de eventos de fim de ciclo de vida (EoL/EoS), apresentando:

1.2.15.5.1. Análise de impacto técnico e operacional;

1.2.15.5.2. Plano de substituição ou atualização;

1.2.15.5.3. Cronograma de execução;

1.2.15.5.4. Garantia de compatibilidade com o ambiente existente.

1.2.15.6. Todos os custos relacionados à manutenção de licenciamento, renovações, atualizações, substituições ou migrações necessárias para manter os ativos dentro de seu ciclo de vida suportado serão de responsabilidade exclusiva da CONTRATADA, não cabendo qualquer ônus adicional à CONTRATANTE;

1.2.15.7. A CONTRATADA deverá manter evidências documentais auditáveis relativas ao ciclo de vida, licenciamento e suporte dos ativos, podendo tais informações ser solicitadas a qualquer tempo pela CONTRATANTE ou por órgãos de controle e fiscalização.

### **1.3. Obrigações aplicáveis ao LOTE 01 e LOTE 02:**

1.3.1. A CONTRATADA deve executar todos os serviços e instalações de acordo com as especificações e demais equipamentos técnicos que integram este Edital, obedecendo rigorosamente às Normas Técnicas da ABNT e das concessionárias de serviços públicos, e as especificações técnicas contidas em todos os adendos/anexos do Termo de Referência.

1.3.2. A CONTRATADA será responsável por realizar, sem ônus para a CONTRATANTE, todas as instalações, mudanças de endereço, mudanças internas, solicitações de serviço, upgrades, ampliações, emissões de relatórios e configurações dos itens contratados, garantindo a execução dentro dos prazos estabelecidos no Termo de Referência e seus Adendos.

1.3.3. A CONTRATADA deve executar o controle tecnológico de materiais, componentes e sistemas construtivos (ensaios laboratoriais) para evidenciar o atendimento às Normas Técnicas da ABNT e dos CONTRATANTES ou das concessionárias de serviços.

1.3.4. A CONTRATADA deve executar, às suas expensas, as ligações definitivas das instalações às redes públicas conforme especificado no Termo de Referência.

1.3.5. A CONTRATADA deve entregar, na mais perfeita ordem e limpeza, as instalações, após a execução do objeto do presente Instrumento, deixando o local totalmente limpo em condições de normais de operações técnicas.

1.3.6. A CONTRATADA deve responsabilizar-se pelo armazenamento e guarda de todos os equipamentos e demais recursos tecnológicos, como cabos, calhas, conectores etc. e ferramentas a serem utilizados na execução da implantação do objeto contratado.

1.3.7. A CONTRATADA deve, em momento definido pela CONTRATANTE Principal, fornecer todos os recursos necessários (equipamentos, pessoal, soluções de telemática etc.) para permitir a migração dos serviços até o momento prestado, para o próximo fornecedor do serviço vencedor da licitação seguinte. De tal forma que possibilite realizar tal transição com os menores impactos possíveis aos CONTRATANTES, garantindo os princípios da continuidade do serviço público. Tal procedimento de transição deverá ser estabelecido e acordado entre a CONTRATANTE, a CONTRATADA atual e a futura. Tal atividade não deverá ter ônus adicionais para a CONTRATANTE.

1.3.8. A CONTRATADA deve prover a gestão de manutenção preventiva e corretiva, no seu próprio ambiente, respeitando os limites estabelecidos dos Níveis Mínimos de Serviços (NMS), definidos neste Termo.

1.3.9. A CONTRATADA deve realizar a manutenção preventiva (diagnóstico padrão, limpeza, verificação de cabos e conectores etc.) dos recursos de telemática, dos serviços da Nova Rede Corporativa, visando, proativamente, mantê-los em pleno funcionamento.

1.3.10. A CONTRATADA deve prover assistência técnica de forma permanente, durante a vigência contratual, evitando gastos adicionais com peças de reposição e manutenção dos equipamentos, isto é, caso ocorra alguma falha, a CONTRATADA garante a substituição do equipamento por um equivalente ou superior, atendendo aos prazos requeridos no nível mínimo de serviço.

1.3.11. A CONTRATADA, deve adotar o Protocolo IPv6 em toda Nova Rede Corporativa, sendo de sua responsabilidade a implantação, configuração, manutenção e gestão de uso de todos os endereços IPv6. Garantir a coexistência, bem como, a interoperabilidade entre IPv6 e IPv4 nos equipamentos conectados nesta Rede e os produtos que suportam ambos os protocolos, mantendo as conexões entre eles, não devendo isolar redes por versão de protocolo IP.

1.3.12. A CONTRATADA deve considerar os conceitos relacionados neste Termo, no que tange a logística de preparação, entrega, instalação, configuração, manutenção preventiva e corretiva dos recursos da solução adotada, na prestação dos serviços contratados da Nova Rede Corporativa.

1.3.13. A CONTRATADA, deve prover e manter os recursos e serviços, a serem operacionalizados para Nova Rede Corporativa em todos os seus endereços contratados;

1.3.14. A CONTRATADA deve disponibilizar, para acesso dos CONTRATANTES aderentes, sistema de gestão da manutenção em plataforma web, fornecendo informações acerca dos itens contratados, seus status, bem como os relatórios de atendimento.

1.3.15. A CONTRATADA deve apresentar à CONTRATANTE aderente, um número de controle para cada atendimento preventivo ou corretivo.

1.3.16. A CONTRATADA deve disponibilizar telefone e endereço eletrônico de atendimento para abertura de chamados, visando o atendimento das demandas no período citado neste Termo.

1.3.17. A CONTRATADA deve garantir que toda a interação com relação a abertura de chamados, manutenção programada e registro de ocorrências, deve ser realizada através do Centro Integrado de Inteligência e Segurança Cibernética (CIISC), para ter um único ponto de Gestão de Demandas e Registro de Ocorrências;

1.3.18. A CONTRATADA deve encaminhar um técnico para prestação de suporte local (on site), quando houver falha(s) na prestação do(s) serviço(s), sem custos adicionais, caso o atendimento remoto não seja efetivo na resolução dos chamados.

1.3.19. A CONTRATADA deve disponibilizar, nos diversos meios de comunicação (help-desk, sistema de acompanhamento de chamados etc.) informações ao CONTRATANTE sobre a situação de atendimento do chamado técnico, o diagnóstico, as providências adotadas e/ou implementadas e a data e hora da solução do incidente.

1.3.20. Infraestrutura de cabos em postes ou equivalente para os **Lotes 1 e 2**

1.3.20.1 Declaração e protocolo:

1.3.20.1.1 Até a assinatura do contrato, as Licitantes provisoriamente classificadas vencedoras deverão apresentar:

1.3.20.1.1.1 Para o Lote 1, apresentar declaração de intenção de ocupação de postes (ou uso de rede subterrânea/própria) nos 14 municípios listados abaixo:

- Arcoverde
- Cabo de Santo Agostinho
- Caruaru
- Garanhuns
- Jaboatão dos Guararapes
- Olinda
- Palmares
- Paulista
- Pesqueira
- Recife
- Salgueiro
- Serra Talhada
- Petrolina
- Vitória de Santo Antão

1.3.20.1.1.2 Para o Lote 2, apresentar declaração de intenção de ocupação de postes (ou uso de rede subterrânea/própria) no município de Recife.

1.3.20.1.1.3 Comprovante de protocolo do pedido de viabilidade técnica junto à distribuidora de energia ou à operadora parceira.

1.3.20.2 Contratos definitivos / autorizações

1.3.20.2.1 A CONTRATADA deverá entregar o contrato de compartilhamento de postes, documento de posse de postes próprios ou autorização formal de terceiro titular da infraestrutura nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.2.1.1 Para a RMR, 90 (noventa) dias;

1.3.20.2.1.2 Para os demais municípios, 150 (cento e cinquenta) dias.

1.3.20.2.1.3 Para o Lote 2, 30 (trinta) dias

1.3.20.3 Vistoria física

1.3.20.3.1 A CONTRATADA deverá apresentar relatório de vistoria atestando liberação dos pontos de fixação nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.3.1.1 Para a RMR, 120 (cento e vinte) dias;

1.3.20.3.1.2 Para os demais municípios, 210 (duzentos e dez) dias.

1.3.20.3.1.3 Para o Lote 2, 60 (sessenta) dias

1.3.20.4 Entrega dos circuitos

1.3.20.4.1 A CONTRATADA deverá ativar integralmente todos os links conforme SLA nos prazos abaixo, contados a partir da assinatura do contrato:

1.3.20.4.1.1 Para a RMR, 180 (cento e oitenta) dias;

1.3.20.4.1.2 Para os demais municípios, 365 (trezentos e sessenta e cinco) dias.

1.3.20.4.1.3 Para o Lote 2, 90 (noventa) dias

1.3.20.5 A CONTRATADA deverá apresentar declaração de que mantém presença física dentro da área de abrangência do novo projeto com, no mínimo, um "ponto de presença" (POP) nos municípios listados no item 96.1.1.1, apresentando registro de infraestrutura existente nestes municípios através de ARTs registradas no CREA ou registro do ponto de presença (estação) na ANATEL em nome da

CONTRATADA ou de SUBCONTRATADA, dentro do prazo de 90 (noventa) dias contados a partir da assinatura do contrato.

#### **1.4. Obrigações aplicáveis ao LOTE 01 e LOTE 03:**

1.4.1. A CONTRATADA deverá implementar, manter e operar, durante toda a vigência contratual, um Sistema de Gestão de Segurança da Informação (SGSI) efetivo, em conformidade com os requisitos da ISO/IEC 27001, contemplando controles compatíveis com o escopo dos serviços contratados e assegurando sua efetividade, mensurabilidade, rastreabilidade e aderência contínua. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

1.4.1.1. Política de segurança da informação formalmente estabelecida, aprovada pela CONTRATANTE, periodicamente revisada e amplamente divulgada;

1.4.1.2. Processo estruturado e contínuo de identificação, análise, avaliação e tratamento de riscos de segurança da informação, com critérios definidos e registro formal;

1.4.1.3. Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP), com testes periódicos e evidências documentadas;

1.4.1.4. Implementação de autenticação multifator (MFA) para acessos privilegiados, administrativos e remotos;

1.4.1.5. Controle de acesso lógico baseado nos princípios de privilégio mínimo, necessidade de conhecimento e segregação de funções;

1.4.1.6. Processo formal de gestão de identidades e acessos (IAM), incluindo concessão, revisão periódica e revogação tempestiva;

1.4.1.7. Processo estruturado de gestão de incidentes de segurança da informação, incluindo detecção, resposta, comunicação, registro e lições aprendidas;

1.4.1.8. Processo contínuo de gestão de vulnerabilidades, incluindo varreduras periódicas, classificação de risco, priorização e remediação;

1.4.1.9. Processo de gestão de mudanças com avaliação de impacto em segurança, aprovação formal e rastreabilidade completa;

- 1.4.1.10. Adoção de controles técnicos de proteção, incluindo criptografia de dados sensíveis em trânsito e em repouso, quando aplicável;
- 1.4.1.11. Implementação de mecanismos de registro e monitoramento (logs), com retenção adequada, integridade e capacidade de auditoria;
- 1.4.1.12. Conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo proteção de dados pessoais e atendimento a direitos dos titulares, quando aplicável ao escopo;
- 1.4.1.13. Controles de segurança física e ambiental nos ambientes computacionais, incluindo controle de acesso, vigilância e proteção contra riscos físicos;
- 1.4.1.14. Gestão de fornecedores e terceiros com acesso a informações ou ativos, incluindo avaliação de segurança e requisitos contratuais;
- 1.4.1.15. Programa contínuo de conscientização e treinamento em segurança da informação, com registro e avaliação de eficácia;
- 1.4.1.16. Execução de auditorias internas com manutenção de evidências e relatórios;
- 1.4.1.17. Tratamento formal de não conformidades, com definição, implementação e acompanhamento de ações corretivas;
- 1.4.1.18. Monitoramento contínuo da eficácia dos controles, com definição de indicadores, métricas e relatórios periódicos;
- 1.4.1.19. Manutenção de documentação e registros do SGSI com controle de versões, integridade e rastreabilidade;
- 1.4.1.20. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados.
- 1.4.2. A CONTRATADA deverá implementar, manter e operar, durante toda a vigência contratual, um Sistema de Gestão de Privacidade da Informação (SGPI), estruturado em conformidade com a ISO/IEC 27701, integrado ao SGSI, assegurando a proteção dos dados pessoais tratados no âmbito do contrato. O sistema deverá garantir efetividade, mensurabilidade, rastreabilidade e aderência

continua, observando integralmente a Lei nº 13.709/2018. A implementação integral dos referidos processos e controles deverá ocorrer no prazo máximo de até 180 (cento e oitenta) dias, contados a partir da assinatura do contrato, constituindo obrigação contratual contínua e sujeita à auditoria a qualquer tempo pela CONTRATANTE:

1.4.2.1. Política de privacidade e proteção de dados pessoais formalmente estabelecida, com diretrizes específicas para tratamento de dados sensíveis e críticos;

1.4.2.2. Designação de Encarregado (DPO) com atuação efetiva, autonomia e capacidade de resposta a incidentes envolvendo dados sensíveis;

1.4.2.3. Classificação da informação e dos dados pessoais, com identificação explícita de dados sensíveis e definição de níveis de proteção diferenciados;

1.4.2.4. Registro detalhado das atividades de tratamento (ROPA), incluindo identificação de tratamentos de alto risco e dados sensíveis;

1.4.2.5. Mapeamento de fluxos de dados com identificação de pontos de exposição, transferência e compartilhamento, especialmente entre órgãos públicos e sistemas críticos;

1.4.2.6. Implementação de controles reforçados para dados sensíveis, incluindo criptografia obrigatória em trânsito e em repouso, controle de acesso restritivo e monitoramento contínuo;

1.4.2.7. Aplicação dos princípios de minimização de dados, limitação de finalidade e necessidade, especialmente em bases contendo dados de saúde, educação e segurança;

1.4.2.8. Processo estruturado para atendimento aos direitos dos titulares, com tratamento prioritário para dados sensíveis;

1.4.2.9. Realização obrigatória de Relatório de Impacto à Proteção de Dados (RIPD/DPIA) para tratamentos que envolvam dados sensíveis ou operações críticas;

1.4.2.10. Processo robusto de gestão de incidentes de privacidade, com notificação tempestiva à CONTRATANTE, autoridades competentes e titulares, quando aplicável;

1.4.2.11. Gestão rigorosa de terceiros, com exigência de níveis equivalentes de proteção de dados e cláusulas contratuais específicas para dados sensíveis;

1.4.2.12. Definição de políticas de retenção e descarte seguro, com critérios diferenciados para dados sensíveis;

1.4.2.13. Monitoramento contínuo e auditoria dos acessos e tratamentos realizados sobre dados sensíveis, com trilhas de auditoria completas;

1.4.2.14. Programa contínuo de capacitação com ênfase em tratamento de dados sensíveis e riscos associados;

1.4.2.15. Monitoramento por indicadores e métricas específicas para privacidade, incluindo eventos envolvendo dados sensíveis;

1.4.2.16. Todos os controles deverão ser auditáveis e formalmente documentados, devendo a CONTRATADA comprovar, de forma contínua, a efetiva implementação e operação dos processos e controles exigidos por meio de evidências objetivas, registros sistêmicos, relatórios e indicadores de desempenho, não sendo suficiente a mera declaração de conformidade, podendo a CONTRATANTE, a qualquer tempo, solicitar tais evidências, bem como acesso aos mecanismos e ferramentas de controle utilizados

## CLÁUSULA NONA – DAS OBRIGAÇÕES PERTINENTES À LGPD

**PARÁGRAFO PRIMEIRO:** São obrigações da CONTRATADA, na qualidade de OPERADORA:

I.Realizar o tratamento dos dados pessoais em estrita conformidade às instruções repassadas pela **CONTROLADORA/CONTRATANTE**;

II.Adotar medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, segundo os padrões técnicos mínimos exigidos pela **CONTROLADORA/CONTRATANTE**;

III.Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma a reduzir o nível de risco ao qual o objeto do **CONTRATO** ou a **CONTRATANTE** está exposta;

IV.Manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

V.Facultar acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade e que tenha assumido compromisso formal de preservar a confidencialidade e

segurança de tais dados, ou ao próprio Titular dos dados, devendo tal compromisso estar disponível em caráter permanente para exibição à **CONTROLADORA/CONTRATANTE**, mediante solicitação;

VI. Permitir a realização de auditorias da **CONTROLADORA/CONTRATANTE** e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações relacionadas à sistemática de proteção de dados;

VII. Informar e obter a anuência prévia da **CONTROLADORA/CONTRATANTE** sobre a utilização de serviços de terceiros para sustentar ou viabilizar o funcionamento da Solução de Tecnologia da Informação e Comunicação – TIC para o desenvolvimento das atividades objeto do **CONTRATO**;

VIII. Apresentar à **CONTROLADORA/CONTRATANTE**, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis;

IX. Auxiliar, em toda providência que estiver ao seu alcance, no atendimento pela **CONTROLADORA/CONTRATANTE** e de obrigações perante Titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

X. Comunicar formalmente e de imediato à **CONTROLADORA/CONTRATANTE** a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

XI. Promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da **CONTROLADORA/CONTRATANTE**, em caso de desligamento de funcionário das atividades inerentes à execução do presente **CONTRATO**;

XII. Obter, quando necessário, o consentimento dos titulares dos dados sob tratamento, nos termos do art. 8º da Lei nº 13.709/2018;

XIII. Abster-se da utilização dos dados pessoais tratados para finalidade diversa da execução dos serviços objeto deste **CONTRATO**;

XIV. Adotar planos de resposta a incidentes de segurança eventualmente ocorridos durante o tratamento dos dados coletados para a execução das finalidades deste **CONTRATO**, bem como dispor de mecanismos que possibilitem a sua remediação, de modo a evitar ou minimizar eventuais danos aos titulares dos dados;

XV.Responsabilizar-se por prejuízos causados à **CONTROLADORA/CONTRATANTE** em razão de coleta e tratamento inadequados dos dados pessoais compartilhados para as finalidades pretendidas no presente **CONTRATO**;

XVI.Responsabilizar-se pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pela **CONTROLADORA/CONTRATANTE**;

XVII.Definir e executar procedimento de descarte seguro dos dados pessoais, que estejam em sua posse, ao encerrar a execução do **CONTRATO** ou após a satisfação da finalidade pretendida;

XVIII.Orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD;

XIX.Exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância;

XX.Manter bancos de dados formados a partir deste **CONTRATO** administrativo em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD, e em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados, com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

**PARÁGRAFO SEGUNDO:** São obrigações da **CONTRATANTE**, na qualidade de **CONTROLADORA**:

I.Fornecer, observadas as diretrizes de sua Política Local de Proteção de Dados Pessoais e Política de Privacidade, as instruções e condições necessárias ao tratamento dos dados pela **OPERADORA/CONTRATADA**;

II.Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

III.Adotar mecanismos transparentes, de fácil compreensão e acesso, que permitam a ciência inequívoca dos titulares dos dados a respeito de sua Política de Privacidade, que deve conter, minimamente, as medidas acima indicadas;

IV.Compartilhar com a **OPERADORA/CONTRATADA** as informações pessoais fornecidas pelos usuários dos serviços públicos por ela prestados, estritamente necessárias à execução do objeto

contrato e nos exatos termos definidos em sua Política de Privacidade, após a aceitação dos termos de uso pelo usuário ou seu representante legal, quando for o caso;

V.Definir quais serão os dados pessoais tratados, bem como as finalidades e as formas de tratamento para cada dado coletado;

VI.Comunicar à autoridade nacional de proteção de dados e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, após o recebimento da comunicação formal feita pela **OPERADORA/CONTRATADA**;

VII.Providenciar a eliminação segura dos dados obtidos para a prestação do serviço e compartilhados com a **OPERADORA/CONTRATADA**, após o término do tratamento, exceto quando necessários ao atendimento das finalidades previstas no art. 16 da Lei Federal nº 13.709/2018, quando estará autorizada a sua conservação;

VIII.Responsabilizar-se pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais e das medidas de segurança estabelecidas em sua Política de Privacidade, no processo de compartilhamento dos dados, a menos que reste comprovado que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

## CLÁUSULA DÉCIMA – DA FISCALIZAÇÃO E DA GESTÃO DO CONTRATO

**PARÁGRAFO PRIMEIRO:** A execução do presente **CONTRATO** deverá ser fiscalizada pela **CONTRATANTE**, sem que essa competência exclua ou reduza a integral responsabilidade da **CONTRATADA**, mesmo perante terceiros, por quaisquer irregularidades constatadas na execução do objeto contratado.

**PARÁGRAFO SEGUNDO:** A **CONTRATANTE** designa **XXXXXX (nome, matrícula e cargo)** como servidor responsável pela fiscalização do **CONTRATO**.

**PARÁGRAFO TERCEIRO:** O fiscal deverá ter pleno conhecimento do **CONTRATO** e das demais condições constantes do Edital e seus anexos, tendo, entre outras, as seguintes atribuições:

a)Fiscalizar a regularidade e adequação dos serviços prestados, de acordo com as especificações previstas no Termo de Referência, e elaborar relatórios de acompanhamento, com os registros de eventuais falhas verificadas e das medidas corretivas necessárias;

- b) Disponibilizar toda a infraestrutura necessária para execução dos serviços na forma e nos prazos definidos no **CONTRATO** e demais anexos do Edital;
- c) Reunir-se com o preposto da **CONTRATADA**, visando a estabelecer as estratégias da execução do objeto, bem como traçar metas de controle, fiscalização e acompanhamento do **CONTRATO**;
- d) Exigir da **CONTRATADA** o fiel cumprimento de todas as condições contratuais assumidas, na forma prevista neste **CONTRATO**;
- e) Comunicar ao gestor do **CONTRATO** a necessidade de alterações do quantitativo do objeto ou modificação da forma de sua execução, em razão de fato superveniente;
- f) Recusar serviço prestado de forma irregular, não aceitando execução diversa daquela que se encontra especificada no Termo de Referência e demais anexos, salvo quando for prestado com qualidade superior e devidamente aceito pela autoridade competente;
- g) Solicitar à **CONTRATADA** justificativa para eventuais serviços não realizados ou realizados inadequadamente, podendo assinalar prazo para correções de eventuais falhas verificadas, conforme avaliação da execução dos serviços;
- h) Atestar as Notas Fiscais/Faturas mensais apresentadas pela **CONTRATADA**, encaminhando-as ao gestor do **CONTRATO** para pagamento;
- i) Verificar a manutenção das condições de habilitação da **CONTRATADA**, acompanhar o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.
- j) Comunicar ao gestor do **CONTRATO**, em tempo hábil, a iminência do término do **CONTRATO** sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.
- k) Comunicar por escrito ao gestor do **CONTRATO** as faltas cometidas pela **CONTRATADA** que sejam passíveis de aplicação de penalidade.

**PARÁGRAFO QUARTO:** A **CONTRATANTE** designa **XXXXXX (nome, matrícula e cargo)** como servidor responsável pela gestão do **CONTRATO**, que, entre outras, terá seguintes atribuições:

- a) Acompanhar e observar o cumprimento das cláusulas contratuais;
- b) Analisar relatórios e documentos enviados pelos fiscais do **CONTRATO**;
- c) Consolidar as avaliações recebidas e encaminhar as consolidações e os relatórios à

**CONTRATADA;**

d) Solicitar abertura de processo administrativo visando à aplicação da penalidade cabível, garantindo a defesa prévia à **CONTRATADA**;

e) Propor aplicação de sanções administrativas pelo descumprimento das cláusulas contratuais apontadas pelos fiscais dos contratos;

f) Providenciar o pagamento das notas fiscais/faturas emitidas pela **CONTRATADA**, e atestadas pelo fiscal do **CONTRATO**, mediante a observância das exigências contratuais e legais;

g) Apurar o percentual de desconto ou glosas da fatura correspondente, em virtude de serviços total ou parcialmente não executados no período de faturamento considerado, por motivos imputáveis à **CONTRATADA**;

h) Manter controle atualizado dos pagamentos efetuados.

**PARÁGRAFO QUINTO:** A ciência da designação deverá ser assinada pelos servidores indicados para atuar como fiscal e gestor do **CONTRATO**, conforme termo em anexo.

**PARÁGRAFO SEXTO:** A substituição do fiscal e do gestor designados, por razões de conveniência ou interesse público, será realizada mediante simples apostilamento ao presente **CONTRATO**, devendo o substituto assinar novo termo de ciência.

**CLÁUSULA DÉCIMA PRIMEIRA – DO PROGRAMA DE INTEGRIDADE**

**PARÁGRAFO PRIMEIRO:** No ato da assinatura do presente **CONTRATO**, será exigida a comprovação da implementação do Programa de Integridade, através da apresentação do Relatório de Perfil e Relatório de Conformidade, nos termos do Decreto Estadual nº 50.365, de 04 de março de 2021, cujos modelos encontram-se disponíveis no sítio da Secretaria da Controladoria Geral do Estado de Pernambuco (<https://www.scge.pe.gov.br/wp-content/uploads/2021/03/Anexo-I-Programa-de-Integridade-na-contratacoes.pdf> e <https://www.scge.pe.gov.br/wp-content/uploads/2021/03/Anexo-II-Programa-de-Integridade-na-contratacoes.pdf>), para avaliação das esferas competentes.

**PARÁGRAFO SEGUNDO:** Caso a **CONTRATADA** não possua Programa de Integridade implantado no momento da assinatura do contrato, será concedido o prazo máximo de até 180 (cento e oitenta) dias, nos termos do art. 17, da Lei Estadual nº 16.722/2019, para as providências cabíveis ao atendimento da Lei.

**PARÁGRAFO TERCEIRO:** O Certificado de Regularidade do Programa de Integridade, emitido pelos órgãos avaliadores, terá validade por 2 (dois) anos, nos termos do art. 9º, da Lei nº 16.722/2019, devendo a **CONTRATADA** renová-lo sempre que expirada a sua validade.

**PARÁGRAFO QUARTO:** Durante a validade do Certificado de Regularidade, fica a **CONTRATADA** obrigada a apresentar os Relatórios de Perfil e de Conformidade atualizados, quando solicitados pela Secretaria da Controladoria Geral do Estado, com intuito de proceder à reavaliação do Programa de Integridade sempre que presentes indícios de atos de fraude e corrupção envolvendo a **CONTRATADA**.

**PARÁGRAFO QUINTO:** A não comprovação da implementação do Programa de Integridade, nos moldes e prazos estabelecidos nesta **CLÁUSULA**, acarretará a aplicação das sanções administrativas específicas previstas na **CLÁUSULA DÉCIMA NONA**.

## CLÁUSULA DÉCIMA SEGUNDA – DAS MEDIÇÕES E DO RECEBIMENTO DOS SERVIÇOS

**PARÁGRAFO PRIMEIRO:** Os serviços executados serão objeto de medição mensal, devendo a **CONTRATADA** encaminhar, até o primeiro dia útil subsequente ao mês em que forem prestados, relatório com a descrição dos serviços realizados e os respectivos valores.

**PARÁGRAFO SEGUNDO:** Os serviços serão recebidos provisoriamente pelo fiscal do **CONTRATO** no prazo de XX(XXX) dias, mediante termo detalhado que ateste o cumprimento das exigências de caráter técnico e administrativo e a comprovação da prestação dos serviços.

**PARÁGRAFO TERCEIRO:** O termo detalhado do recebimento provisório, com a análise das ocorrências registradas na execução do **CONTRATO** serão encaminhados ao gestor para fins de apuração dos descontos e glosas cabíveis na fatura correspondente, em virtude de serviços total ou parcialmente não executados ou, se for o caso, da pontuação obtida na avaliação da qualidade dos serviços em consonância com os indicadores previstos no Instrumento de Medição de Resultado (IMR), conforme Anexo II – Níveis Mínimos de Serviço, do Termo de Referência.

**PARÁGRAFO QUARTO:** O fiscal indicará a retenção ou glosa no pagamento, proporcional à irregularidade verificada, caso se constate que a **CONTRATADA**:

a) não produziu os resultados acordados;

b) deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

c) deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizou tais recursos com qualidade ou quantidade inferior à demandada.

**PARÁGRAFO QUINTO:** A **CONTRATADA** fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados.

**PARÁGRAFO SEXTO:** O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo exigidos por normas técnicas oficiais, às expensas da **CONTRATADA**, e à entrega dos Manuais e Instruções exigíveis.

**PARÁGRAFO SÉTIMO:** Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

**PARÁGRAFO OITAVO:** Até que sejam sanadas todas as eventuais pendências técnicas, o fiscal não deverá emitir o termo de Recebimento Provisório.

**PARÁGRAFO NONO:** Os serviços serão recebidos definitivamente no prazo de XX(XXXX) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente.

**PARÁGRAFO DÉCIMO:** O recebimento definitivo ocorrerá mediante termo detalhado que comprove o atendimento das exigências contratuais, após a análise dos relatórios e de toda documentação apresentada pela fiscalização, com a verificação da qualidade e quantidade do serviço prestado.

**PARÁGRAFO DÉCIMO PRIMEIRO:** Os prazos de recebimento não correrão enquanto pendente a solução, pela **CONTRATADA**, de inconsistências verificadas na execução do objeto.

**PARÁGRAFO DÉCIMO SEGUNDO:** Sanadas as pendências e aplicadas eventuais glosas, a **CONTRATANTE** comunicará à **CONTRATADA** o valor aprovado pela fiscalização e gestão, autorizando a emissão da Nota Fiscal ou Fatura correspondente.

**PARÁGRAFO DÉCIMO TERCEIRO.** No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

**PARÁGRAFO DÉCIMO QUARTO:** O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do **CONTRATO**.

**PARÁGRAFO DÉCIMO QUINTO:** A realização das glosas indicadas não prejudica a aplicação de sanções à **CONTRATADA** em virtude da inexecução dos serviços, quando for o caso.

### CLÁUSULA DÉCIMA TERCEIRA – DO PAGAMENTO

**PARÁGRAFO PRIMEIRO:** O valor dos pagamentos será obtido mediante a aplicação dos preços unitários contratados às correspondentes quantidades de serviços efetivamente executados, aplicando-se eventual desconto ou glosa.

**PARÁGRAFO SEGUNDO:** O pagamento será feito diretamente pela **CONTRATANTE**, no prazo de até 30 (trinta) dias, por meio de ordem bancária para crédito em conta corrente da **CONTRATADA**, à vista de termo de recebimento definitivo dos serviços acompanhado dos documentos de comprovação da regularidade fiscal e trabalhista e da apresentação e atesto da Nota Fiscal ou documento de cobrança equivalente, na forma prevista nos parágrafos seguintes.

**PARÁGRAFO TERCEIRO:** A **CONTRATADA** deverá emitir as notas fiscais em observância às regras de retenção de imposto de renda estabelecidas na Instrução Normativa RFB nº 1.234/2012, e alterações posteriores, de acordo com as alíquotas constantes do Anexo I da referida norma, ou em observância à norma que venha a substituí-la, sob pena de devolução do documento para as correções cabíveis ou de retenção no valor total do documento fiscal, caso não realizadas as correções, nos termos do art. 4º do Decreto nº 55.069, de 25 de julho de 2023.

**PARÁGRAFO QUARTO:** Quando não for possível verificar diretamente no CADFOR-PE, a regularidade fiscal e trabalhista da **CONTRATADA** será comprovada mediante a apresentação das seguintes certidões:

- a) Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND);
- b) Certidões que comprovem a regularidade perante as Fazendas Estadual ou Distrital do domicílio ou sede da **CONTRATADA**;
- c) Certidão de Regularidade do FGTS (CRF); e

d) Certidão Negativa de Débitos Trabalhistas (CNDT).

**PARÁGRAFO QUINTO:** Caso não seja(m) apresentado(s) quaisquer dos documentos de regularidade ou os documentos encaminhados contenham pendências, a **CONTRATADA** terá 10 (dez) dias para sanar a ausência identificada, prazo em que o pagamento correspondente ao mês em referência ficará suspenso.

**PARÁGRAFO SEXTO:** Caso não seja sanada a pendência no prazo estipulado, estará configurada a não manutenção das condições de habilitação pela **CONTRATADA**, devendo a **CONTRATANTE** instaurar processo administrativo para extinção do **CONTRATO** e comunicar aos órgãos de fiscalização da regularidade fiscal quanto à inadimplência da **CONTRATADA**, sem prejuízo da retomada dos pagamentos pelos serviços efetivamente executados.

**PARÁGRAFO SÉTIMO:** Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a **CONTRATADA** providencie as medidas saneadoras.

**PARÁGRAFO OITAVO:** Quando do pagamento, deverá ser efetuada a retenção do imposto sobre a renda, nos termos previstos na Instrução Normativa RFB nº 1.234/2012, e alterações posteriores, ou em norma que venha a substituí-la, além de outras retenções previstas na legislação tributária aplicável.

**PARÁGRAFO NONO:** A **CONTRATADA** regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

**PARÁGRAFO DÉCIMO:** Nos casos de eventuais atrasos de pagamento, verificados por culpa única e exclusiva da **CONTRATANTE**, fica convencionado que a taxa de atualização financeira será calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

Onde:

SIGLA

SIGNIFICADO/ DESCRIÇÃO

EM	Encargos Moratórios
N	Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.
VP	Valor da parcela a se paga.
TX	IPCA
I	Índice de atualização financeira, assim apurado: $I = \frac{\left(\frac{TX}{100}\right)}{365}$

**PARÁGRAFO DÉCIMO PRIMEIRO:** A atualização financeira prevista nesta cláusula será incluída na Nota Fiscal/Fatura do mês seguinte ao da ocorrência.

#### CLÁUSULA DÉCIMA QUARTA - DA ALTERAÇÃO CONTRATUAL

**PARÁGRAFO PRIMEIRO:** A **CONTRATADA** fica obrigada a aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo da **CONTRATANTE**, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do **CONTRATO**.

**PARÁGRAFO SEGUNDO:** Na hipótese de haver acordo entre as partes, as supressões poderão exceder o limite de 25% (vinte e cinco por cento).

**PARÁGRAFO TERCEIRO:** As alterações contratuais serão obrigatoriamente formalizadas mediante celebração de prévio termo aditivo ao presente instrumento, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês, conforme art. 132 da Lei nº 14.133, de 2021).

**PARÁGRAFO QUARTO:** Registros que não caracterizam alteração do **CONTRATO** podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

#### CLÁUSULA DÉCIMA QUINTA - DA SUBCONTRATAÇÃO

**PARÁGRAFO PRIMEIRO:** É permitida a subcontratação parcial do objeto, nas seguintes condições:

**I. Para o LOTE 1, será permitida a subcontratação de até 25% (vinte e cinco por cento) do valor total do contrato.**

a) **NÃO** será permitida a subcontratação do Serviço CIISC – Centro Integrado de Inteligência e Segurança Cibernética (serviços do ADENDO IX do Termo de Referência), exceto para o serviço de acompanhamento de reparos, que poderá ser subcontratado. A subcontratação das demais atividades relacionadas ao CIISC não se mostra técnica nem economicamente vantajosa para a Administração Pública, permanecendo vedada.

**II. Para o LOTE 2, será permitida a subcontratação de até 50% (cinquenta por cento) do valor total do contrato**, da parcela do objeto do presente certame correspondente à execução de serviços técnicos especializados de configuração, monitoramento e mitigação de ataques Anti-DDoS, garantia de alta disponibilidade, resiliência operacional e redundância de acesso à internet, por meio de rotas, sistemas autônomos (AS) e estações geograficamente distintas, tendo em vista que se trata de aspectos técnicos específicos do serviço, cuja adequada implementação é determinante para a continuidade dos serviços críticos da Administração Pública, conforme detalhado na Nota Técnica 5 (SEI nº 83630624) e os subitens 6.10.4.1 e 6.10.4.2 do Termo de Referência.

a) Será permitida a subcontratação de outro provedor para a prestação do serviço de Solução de Internet Corporativa com Proteção Anti-DDoS em alta disponibilidade. Esta subcontratação se justifica por ser tecnicamente vantajosa e benéfica para a Administração Pública.

b) Será permitida a subcontratação de um AS (Autonomous Systems) para fornecimento do segundo link internet com dupla abordagem, sem que isso implique transferência da prestação do serviço contratado, em perda de economicidade ou em detrimento de sua qualidade;

**III. Para o LOTE 3, será permitida a subcontratação do objeto do presente certame, tendo em vista que se trata de aspectos técnicos específicos do serviço, até o limite de 25% (vinte e cinco por cento) do valor total do contrato.**

**IV. A subcontratação do objeto principal fica condicionada à expressa anuência da CONTRATANTE PRINCIPAL.**

**V. Não se caracteriza como subcontratação a utilização, pela CONTRATADA, de redes, circuitos, postes, dutos, fibras ópticas, enlaces, infraestrutura passiva ou ativa pertencentes a outras prestadoras de serviços de telecomunicações, quando admitido pela legislação setorial vigente,**

especialmente nos termos da Lei nº 9.472/1997 (Lei Geral de Telecomunicações) e da regulamentação expedida pela ANATEL.

VI. A subcontratação não exime a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados, cabendo-lhe também a devida supervisão e coordenação dessas atividades.

**PARÁGRAFO SEGUNDO:** Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da **CONTRATADA** pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a **CONTRATANTE** pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

**PARÁGRAFO TERCEIRO:** A subcontratação depende de autorização prévia da **CONTRATANTE**, a quem incumbe analisar os documentos de capacidade técnica da subcontratada, quando for o caso, e avaliar se ela cumpre os requisitos de qualificação necessários para a execução do objeto.

**PARÁGRAFO QUARTO:** É vedada a subcontratação de pessoa jurídica, se esta ou os seus dirigentes mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade **CONTRATANTE** ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do **CONTRATO**, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

## CLÁUSULA DÉCIMA SEXTA - DA GARANTIA DE EXECUÇÃO CONTRATUAL

**PARÁGRAFO PRIMEIRO:** A **CONTRATADA** prestará garantia de execução contratual, no percentual de 5% (cinco por cento) do valor anual do **CONTRATO**, nos termos dos artigos 96 a 98 da Lei nº 14.133, de 2021.

**PARÁGRAFO SEGUNDO:** Caso a **CONTRATADA** opte pelo seguro-garantia, a apólice deverá ser apresentada antes da assinatura do **CONTRATO**, ficando-lhe assegurado prazo mínimo de 1 (um) mês entre a homologação da licitação e a assinatura deste instrumento.

**PARÁGRAFO TERCEIRO:** Caso a **CONTRATADA** opte por uma das demais modalidades de garantia previstas no art. 96, § 1º, da Lei nº 14.1333, a garantia será prestada no prazo de até 10 (dez) dias úteis, após a assinatura do presente **CONTRATO**, prorrogáveis por igual período, mediante justificativa aceita pela **CONTRATANTE**.

**PARÁGRAFO QUARTO:** A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação das sanções administrativas previstas neste instrumento e poderá ensejar a extinção do **CONTRATO**.

**PARÁGRAFO QUINTO:** A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- a) prejuízos advindos do não cumprimento do objeto do **CONTRATO** e do não adimplemento das demais obrigações nele previstas; e
- b) multas moratórias e compensatórias aplicadas pela Administração à **CONTRATADA**.

**PARÁGRAFO SEXTO:** A garantia deverá ter validade durante toda a execução do **CONTRATO** e após 90 (noventa) dias do término do prazo de vigência contratual.

**PARÁGRAFO SÉTIMO:** Nos casos de prorrogação do prazo de vigência do **CONTRATO** ou de alteração do seu valor, por acréscimos, reajuste ou revisão de preços, a garantia deverá ser renovada ou complementada, seguindo os mesmos parâmetros utilizados quando da contratação.

**PARÁGRAFO OITAVO:** Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação ou de multas e indenizações, a **CONTRATADA** obriga-se a fazer a respectiva reposição/complementação no prazo de 10 (dez) dias úteis, contados da data em que for notificada pela **CONTRATANTE**, sendo possível a prorrogação por igual período mediante justificativa aceita pela **CONTRATANTE**.

**PARÁGRAFO NONO:** Na hipótese de suspensão do **CONTRATO** por ordem ou inadimplemento da Administração, a **CONTRATADA** ficará desobrigada de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

**PARÁGRAFO DÉCIMO:** Caso utilizada a modalidade de seguro-garantia:

- a) A apólice permanecerá em vigor mesmo que a **CONTRATADA** não pague o prêmio nas datas convencionadas;
- b) A apólice deverá acompanhar as modificações referentes à vigência do **CONTRATO** principal mediante a emissão do respectivo endosso pela seguradora;
- c) Será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no **PARÁGRAFO NONO**;

d) Ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

**PARÁGRAFO DÉCIMO PRIMEIRO:** A garantia em dinheiro deverá ser efetuada em favor da **CONTRATANTE**, em conta específica XXXXX, com correção monetária.

**PARÁGRAFO DÉCIMO SEGUNDO:** Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

**PARÁGRAFO DÉCIMO TERCEIRO:** Na modalidade de fiança bancária, a garantia deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

**PARÁGRAFO DÉCIMO QUARTO:** A **CONTRATADA** autoriza a **CONTRATANTE** a reter e executar, a qualquer tempo, a garantia, na forma prevista no Edital e neste **CONTRATO**.

**PARÁGRAFO DÉCIMO QUINTO:** A garantia somente será liberada ou restituída após a fiel execução do **CONTRATO**, mediante termo circunstanciado de que a **CONTRATADA** cumpriu todas as cláusulas do **CONTRATO**, ou após a sua extinção por culpa exclusiva da Administração.

**PARÁGRAFO DÉCIMO SEXTO:** O emitente da garantia ofertada pela **CONTRATADA** deverá ser notificado pela **CONTRATANTE** quanto à instauração de processo administrativo para apuração de responsabilidade e aplicação de penalidades, mas o garantidor não é parte legítima para figurar no respectivo processo.

## CLÁUSULA DÉCIMA SÉTIMA - DA EXTINÇÃO DO CONTRATO

**PARÁGRAFO PRIMEIRO:** O **CONTRATO** se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contratantes.

**PARÁGRAFO SEGUNDO:** O **CONTRATO** pode ser extinto antes do prazo nele fixado, sem ônus para a **CONTRATANTE**, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o **CONTRATO** não mais lhe oferece vantagem.

**PARÁGRAFO TERCEIRO:** A extinção antecipada ocorrerá na próxima data de aniversário do **CONTRATO**, desde que a notificação da **CONTRATADA** sobre a não-continuidade seja feita pelo **CONTRATANTE** com pelo menos 2 (dois) meses de antecedência desse dia. Caso a notificação ocorra com menos de 2 (dois) meses da data de aniversário do **CONTRATO**, a extinção se dará após 2 (dois) meses da data da comunicação.

**PARÁGRAFO QUARTO:** Constituem motivos para extinção do **CONTRATO**, independentemente do prazo ou das obrigações nele estipuladas, as situações descritas no art. 137 da Lei nº 14.133, de 2021.

**PARÁGRAFO QUINTO:** A extinção consensual e a extinção unilateral serão precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo, assegurados o contraditório e a ampla defesa.

**PARÁGRAFO SEXTO:** Aplica-se à extinção do **CONTRATO** a disciplina dos arts. 138 e 139 da Lei nº 14.133/2021.

**PARÁGRAFO SÉTIMO:** O termo de extinção, sempre que possível, será instruído com os seguintes documentos:

- a) Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
- b) Relação dos pagamentos já efetuados e ainda devidos;
- c) Indenizações e multas.

## CLÁUSULA DÉCIMA OITAVA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

**PARÁGRAFO PRIMEIRO:** Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a **CONTRATADA** que:

- a) der causa à inexecução parcial do **CONTRATO**, deixando de cumprir as obrigações assumidas no presente instrumento;
- b) der causa à inexecução parcial do **CONTRATO** que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do **CONTRATO**;
- d) ensejar o retardamento da execução contratual sem motivo justificado;

- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do **CONTRATO**;
- f) praticar ato fraudulento na execução do **CONTRATO**;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

**PARÁGRAFO SEGUNDO:** Será aplicável a sanção de advertência quando a **CONTRATADA** descumprir deveres instrumentais ou der causa à inexecução parcial do **CONTRATO** que não acarrete dano à Administração e que não justifique a imposição de penalidade mais grave, em especial pelo descumprimento das obrigações previstas nos itens V a X da **CLÁUSULA OITAVA** deste **CONTRATO** ("Das Obrigações da Contratada").

**PARÁGRAFO TERCEIRO:** Será aplicada multa moratória em razão do atraso no cumprimento das obrigações previstas neste **CONTRATO**, em especial as elencadas nos incisos II e III da **CLÁUSULA OITAVA**, no percentual de até 0,5% (cinco décimos por cento) ao dia, a ser calculada sobre o valor da parcela inadimplida, a partir do dia subsequente ao prazo estipulado para adimplemento da obrigação, independentemente de notificação do contratado para constituição em mora.

**PARÁGRAFO QUARTO:** Após o 30º (trigésimo) dia de atraso injustificado, configura-se o descumprimento total da obrigação e a multa moratória se converterá em multa compensatória, a ser calculada no percentual de 15% (quinze por cento) a 30% (trinta por cento) sobre o valor da parcela inadimplida, podendo dar ensejo à extinção do contrato e aplicação da penalidade de impedimento, se configurado grave dano à Administração.

**PARÁGRAFO QUINTO:** A penalidade de multa compensatória será aplicada nos casos de descumprimento das obrigações contratuais pela **CONTRATADA**, sempre que deles decorrer inexecução parcial do **CONTRATO** que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo, bem como retardamento injustificado à execução ou entrega do objeto contratado, nos termos das alíneas "b" e "d", respectivamente, do **PARÁGRAFO PRIMEIRO**, de acordo com as seguintes regras:

- I. 1% (um por cento) a 5% (cinco por cento) sobre do valor anual do **CONTRATO**, observado o valor mínimo de R\$ 10.000,00 (dez mil reais) e o máximo de R\$ 100.000,00 (cem mil reais), a ser aplicada a quem sofreu a penalidade de advertência e reincidiu pelo(s) mesmo(s) motivo(s);

II.10% (dez por cento) a 20% (vinte por cento), sobre o valor da garantia, no caso de descumprimento da obrigação prevista no inciso XXII da **CLÁUSULA OITAVA**.

III.5% (cinco por cento) a 10% (dez por cento), calculada sobre o valor mensal do **CONTRATO**, a ser aplicada quando a **CONTRATADA** descumprir a obrigação prevista no inciso I da **CLÁUSULA OITAVA**, se a situação não se enquadrar em obrigação contratual específica;

IV.1% (um por cento) a 5% (cinco por cento), calculada sobre o valor mensal do **CONTRATO**, a ser aplicada quando a **CONTRATADA** descumprir as obrigações previstas nos incisos IV , XI e XVII da **CLÁUSULA OITAVA**;

V.10% (dez por cento) a 20% (vinte por cento), calculada sobre o valor mensal do **CONTRATO**, a ser aplicada quando a **CONTRATADA** descumprir as obrigações previstas nos incisos XIX e XX da **CLÁUSULA OITAVA**;

VI.0,5% (cinco décimos por cento) a 2% (dois por cento), calculada sobre o valor do **CONTRATO**, a ser aplicada quando a **CONTRATADA** descumprir a obrigação prevista no inciso XVIII da **CLÁUSULA OITAVA** e não sanar a pendência no prazo estipulado;

VII.5% (cinco por cento) a 10% (dez por cento), calculada sobre o valor mensal do **CONTRATO**, quando a **CONTRATADA** deixar de cumprir a obrigação prevista no inciso XV da **CLÁUSULA OITAVA**;

VIII.5% (cinco por cento) a 10% (dez por cento), calculada sobre o valor da parcela transferida, a ser aplicada quando a **CONTRATADA** descumprir a obrigação prevista no inciso XXI da **CLÁUSULA OITAVA**;

**PARÁGRAFO SEXTO:** As sanções de multa previstas no **PARÁGRAFO QUINTO** poderão ser aplicadas cumulativamente com a penalidade de impedimento de licitar e contratar com a Administração Direta e Indireta do Estado de Pernambuco, pelo prazo de 06 (seis) a 18 (dezoito) meses.

**PARÁGRAFO SÉTIMO:** Na hipótese de inexecução total do **CONTRATO**, prevista na alínea “c” do **PARÁGRAFO PRIMEIRO**, será aplicável a sanção de impedimento de licitar e contratar com a Administração Direta e Indireta do Estado de Pernambuco pelo prazo 18 (dezoito) a 36 (trinta e seis) meses, além de multa compensatória no percentual de 10% (dez por cento) a 20% (vinte por cento) sobre o valor do contrato.

**PARÁGRAFO OITAVO:** Quando do cometimento das infrações previstas nas alíneas “e”, “f”, “g” e “h” do **PARÁGRAFO PRIMEIRO**, ou quando praticadas as infrações descritas nas alíneas “b”, “c” e “d” que

justifiquem a imposição de penalidade mais grave, será aplicável a sanção de declaração de inidoneidade para licitar e contratar com a Administração Pública, pelo período de 03 (três) a 06 (seis) anos, além da multa compensatória de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor do contrato.

**PARÁGRAFO NONO:** A aplicação das sanções previstas neste **CONTRATO** não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à **CONTRATANTE**.

**PARÁGRAFO DÉCIMO:** Todas as sanções previstas neste **CONTRATO** poderão ser aplicadas cumulativamente com a multa.

**PARÁGRAFO DÉCIMO PRIMEIRO:** O valor da multa aplicada e das indenizações cabíveis será objeto de compensação com os pagamentos eventualmente devidos pelo **CONTRATANTE** à **CONTRATADA**, decorrentes do mesmo **CONTRATO** ou de outros contratos administrativos que a **CONTRATADA** possua com a **CONTRATANTE**.

**PARÁGRAFO DÉCIMO SEGUNDO:** Se o valor da multa for superior ao dos pagamentos devidos pelo **CONTRATANTE**, a diferença será descontada da garantia contratual prestada, se houver, ou será cobrada administrativamente na forma prevista na Lei Estadual nº 13.178, de 2006.

**PARÁGRAFO DÉCIMO TERCEIRO:** Não havendo o pagamento integral da multa em sede administrativa, o processo será encaminhado à Procuradoria Geral do Estado para inscrição em Dívida Ativa e cobrança.

**PARÁGRAFO DÉCIMO QUARTO:** A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto no Decreto Estadual.

**PARÁGRAFO DÉCIMO QUINTO:** Na fixação das penalidades, dentro das faixas de multa estabelecidas neste Edital, bem como dos prazos previstos para as demais sanções deverão ser observadas:

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que o cometimento da infração ocasionar ao **CONTRATANTE**, ao funcionamento dos serviços públicos, aos seus usuários ou ao interesse coletivo;
- e) a vantagem auferida em virtude da infração;

f) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle interno.

**PARÁGRAFO DÉCIMO SEXTO:** Em caso de prática da mesma infração ocorrida no prazo igual ou inferior a 12 (dozes) meses, contados da data de publicação da decisão definitiva da condenação anterior, as faixas de multa e os prazos previstos neste **CONTRATO** poderão ser majorados em até 50% (cinquenta por cento), observados os limites máximos previstos em lei.

**PARÁGRAFO DÉCIMO SÉTIMO:** Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na Lei Estadual nº 16.309, de 2018.

**PARÁGRAFO DÉCIMO OITAVO:** A personalidade jurídica da **CONTRATADA** poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste **CONTRATO** ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a **CONTRATADA**, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

**PARÁGRAFO DÉCIMO NONO:** A **CONTRATANTE** deverá comunicar as sanções aplicadas à Secretaria de Administração, para fins de inclusão da **CONTRATADA** nos sistemas E-fisco e PE-Integrado, no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal, observado o prazo máximo de 15 (quinze) dias úteis, contado da data da decisão definitiva de aplicação da sanção.

**PARÁGRAFO VIGÉSIMO:** Além das sanções previstas acima, serão aplicadas as seguintes sanções específicas na presente contratação:

I. Advertência;

a) Será aplicável a sanção de advertência quando a **CONTRATADA** descumprir deveres instrumentais ou der causa à inexecução parcial do **CONTRATO** que não acarrete dano à Administração e que não justifique a imposição de penalidade mais grave, em especial pelo descumprimento das obrigações previstas no Termo de Referência;

II. Multa, de acordo com as seguintes regras:

a) Pelo atraso na entrega do Plano de Assunção ou de Ordens de Serviço, cujos prazos previstos estão na tabela LIMITES DE TEMPO PARA PREPARAÇÃO, INSTALAÇÃO, MUDANÇA DE ENDEREÇO E ENTREGA do Termo de Referência, multa de 3% (três por cento) do valor do referido serviço, por dia decorrido;

## CLÁUSULA DÉCIMA NONA – DAS SANÇÕES ESPECÍFICAS DECORRENTES DO NÃO CUMPRIMENTO DA LEI ESTADUAL Nº 16.722/2019

**PARÁGRAFO PRIMEIRO:** A não apresentação do Programa de Integridade ensejará a aplicação de multa de 0,2% (dois décimos percentuais) incidente sobre o valor global atualizado do contrato, por dia de atraso, contado a partir do 1º dia útil após decurso do prazo estabelecido no **PARÁGRAFO SEGUNDO DA CLÁUSULA DÉCIMA PRIMEIRA**, limitada ao valor máximo de 20% (vinte por cento).

**PARÁGRAFO SEGUNDO:** O não atingimento da pontuação mínima estabelecida no Decreto Estadual nº 50.365/2021 ensejará a aplicação de multa de 0,1% (um décimo percentual) por dia, incidente sobre o valor global atualizado do **CONTRATO**, contado a partir do 1º dia útil após a ciência, pelo representante legal da **CONTRATADA**, da decisão administrativa que declarar a desconformidade do Programa de Integridade, limitada ao valor máximo de 10% (dez por cento).

**PARÁGRAFO TERCEIRO:** A aplicação de multa nas hipóteses previstas nos **PARÁGRAFOS PRIMEIRO e SEGUNDO** desta Cláusula afasta a aplicação, pelos mesmos fatos, da penalidade de multa prevista no **PARÁGRAFO QUINTO da CLÁUSULA DÉCIMA NONA**.

**PARÁGRAFO QUARTO:** O não cumprimento da obrigação de implantar o Programa de Integridade, ou seu cumprimento parcial ou meramente formal, poderá implicar, cumulativamente, na impossibilidade de aditamento contratual, na extinção do contrato por parte da **CONTRATANTE** e na impossibilidade de licitar e contratar com a Administração Pública Estadual, até a efetiva comprovação de implementação do Programa de Integridade, sem prejuízo do pagamento da multa aplicada.

**PARÁGRAFO QUINTO:** A aplicação das sanções previstas nesta Cláusula depende de processo administrativo de apuração de responsabilidade, assegurada a ampla defesa e o contraditório.

## CLÁUSULA VIGÉSIMA - CLÁUSULA ANTICORRUPÇÃO

**PARÁGRAFO PRIMEIRO:** A **CONTRATADA** se compromete a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial a Lei Federal nº 12.846, de 1º de agosto de 2013, a Lei Federal nº 9.613/98 e a Lei Estadual nº 16.309/2018.

**PARÁGRAFO SEGUNDO:** A **CONTRATADA** (i) declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei Federal nº 12.846/2013 e Lei Estadual nº 16.309/2018; (ii) se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei Federal nº 12.846/2013 e Lei Estadual nº 16.309/2018.

**PARÁGRAFO TERCEIRO:** A **CONTRATADA**, no desempenho das atividades objeto deste **CONTRATO**, compromete-se perante a **CONTRATANTE** a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

**PARÁGRAFO QUARTO:** Qualquer descumprimento das regras da Lei Anticorrupção e de suas regulamentações, por parte da **CONTRATADA**, em qualquer um dos seus aspectos, poderá ensejar:

I - Instauração do Processo Administrativo de Responsabilização - PAR, nos termos da Lei Estadual nº 16.309/2018 e do Decreto Estadual nº 46.967/2018, com aplicação das sanções administrativas porventura cabíveis;

II - Ajuizamento de ação com vistas à responsabilização na esfera judicial, nos termos dos artigos 18 e 19 da Lei nº 12.846/2013 e do artigo 39 da Lei Estadual nº 16.309/2018.

**PARÁGRAFO QUINTO:** Sem prejuízo da obrigação de cumprimento das disposições de seus respectivos código de ética e conduta, a **CONTRATADA** se obriga a, no exercício dos direitos e obrigações previstos neste contrato e no cumprimento de qualquer uma de suas disposições: (I) não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente e (II) adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas

ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados.

**PARÁGRAFO SEXTO:** A **CONTRATADA** se obriga a notificar a **CONTRATANTE**, imediatamente, por escrito, a respeito de qualquer suspeita ou violação das legislações anticorrupção vigentes, bem como nos casos em que obtiver ciência de qualquer prática de suborno ou corrupção.

**PARÁGRAFO SÉTIMO:** A comprovada violação de qualquer das obrigações previstas nesta cláusula é causa para a extinção deste **CONTRATO**, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

## CLÁUSULA VIGÉSIMA PRIMEIRA – DA MATRIZ DE RISCOS

**PARÁGRAFO PRIMEIRO:** Este contrato obedecerá à seguinte matriz de riscos:

I. Constituem riscos a serem suportados pela **CONTRATANTE**:

- a) Ocorrência de furto, roubo, dano ou extravio de cabos, equipamentos, peças, componentes e periféricos em ambientes internos e sob controle do site do governo (PCS).
- b) Aumento do dólar superior a 50% durante o período contratual, considerando como referência a taxa PTAX de venda divulgada pelo Banco Central na data de ocorrência do certame, aplicando-se o impacto exclusivamente ao excedente superior a 50% da variação cambial.

II. Constituem riscos a serem suportados pela **CONTRATADA**:

- a) Ocorrência de eventos fortuitos ou de força maior, como fenômenos climáticos e ambientais excepcionais (ex.: chuvas intensas, vendavais, descargas atmosféricas), causando danos a equipamentos e infraestruturas disponibilizados pela **CONTRATADA** para a execução do contrato.
- b) Ocorrência de furto, roubo, dano ou extravio de cabos, equipamentos, peças, componentes e periféricos em ambientes fora do site do governo (PCS).
- c) Aumento do dólar comercial de até 50% durante o período contratual, considerando como referência a taxa PTAX de venda divulgada pelo Banco Central na data de ocorrência do certame, impactando a aquisição de insumos importados.
- d) Implantação de serviços próximo ao encerramento do contrato, não gerando ROI (Return Of Investment) suficiente para a contratada.

## CLÁUSULA VIGÉSIMA SEGUNDA – DOS CASOS OMISSOS

Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas estaduais aplicáveis, e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 (Código de Defesa do Consumidor) e nas normas e princípios gerais dos contratos.

### CLÁUSULA VIGÉSIMA TERCEIRA – DA PUBLICAÇÃO

Nos termos do art. 94 da Lei nº 14.133, de 2021, o presente instrumento contratual será publicado no Portal Nacional de Contratações Públicas (PNCP) em até 20 (vinte) dias úteis contados da data de sua assinatura, bem como no Sistema PE Integrado como condição de sua eficácia.

### CLÁUSULA VIGÉSIMA QUARTA – DA RESOLUÇÃO DE CONTROVÉRSIAS E DO FORO

**PARÁGRAFO PRIMEIRO:** As controvérsias administrativas e litígios decorrentes deste **CONTRATO** deverão ser preferencialmente submetidos à composição da Câmara de Negociação, Conciliação e Mediação da Administração Pública Estadual, conforme art. 11 da Lei Complementar nº 417, de 09.12.2019.

**PARÁGRAFO SEGUNDO:** Fica eleito o Foro da Comarca do Recife para dirimir os litígios decorrentes deste **CONTRATO** que não puderem ser compostos pela conciliação, obedecidos os termos do art. 92, §1º, da Lei 14.133, de 2021.

E, para firmeza e como prova de assim haverem entre si ajustado e contratado, foi lavrado o presente instrumento contratual, o qual depois de lido e achado conforme, foi assinado pelas partes contratantes.

Recife, XX de XXXXXXXXXX de XXXX.

CNPJ XXX  
**CONTRATANTE**  
CNPJ XXX  
**CONTRATADA**

## ANEXO I

### TERMO DE CIÊNCIA DO GESTOR E DO FISCAL DO CONTRATO

#### INTRODUÇÃO

<O Termo de Ciência visa a obter o comprometimento formal e a ciência do encargo por parte daqueles indivíduos designados para atuar como fiscal ou gestor do contrato >

**Referência: Art. 17, III, do Decreto Estadual nº 51.651/2021.**

#### 1. IDENTIFICAÇÃO

**CONTRATO Nº:**XXXX/AAAA

**OBJETO:**<objeto do contrato>

**CONTRATADA:**<nome da contratada>

**CNPJ:**xxxxxxxxxxxxx

**GESTOR DO CONTRATO OU FISCAL DO CONTRATO:** <Nome do gestor do Contrato OU fiscal do Contrato>

**MATRÍCULA:**xxxxxxxxxxxxx

#### 2. CIÊNCIA

EU, \_\_\_\_\_, matrícula \_\_\_\_\_, ocupante do cargo \_\_\_\_\_, pelo presente termo, DECLARO QUE:

estou ciente da minha designação para atuar como gestor/fiscal (indicar conforme o caso) do Contrato nº XXX;

comprometo-me a cumprir as atribuições declinadas na Cláusula XXX do Contrato nº XXX;

estou ciente de que minha substituição poderá ser realizada pela autoridade competente, por razões de conveniência ou interesse público, mediante apostilamento ao contrato.

Recife, XX de XXXXXXXXXX de XXXX.

\_\_\_\_\_  
ASSINATURA DO FISCAL/GESTOR

**ANEXO VI**  
**MODELO DE FOLHA DE ROSTO**

**PROCESSO LICITATÓRIO Nº 4338.2025.AC-10.PE.90323.SAD.ATI**  
**PREGÃO ELETRÔNICO Nº 90323/2025**  
**PROCESSO SEI Nº 0001200180.000817/2023-36**

**FOLHA DE ROSTO**

O Estado de Pernambuco, por intermédio da **SECRETARIA DE ADMINISTRAÇÃO**, torna público, para conhecimento dos interessados, a abertura da licitação, a ser realizada por meio da utilização de recursos de tecnologia da informação – *Internet*, no local e horário a seguir:

**INFORMAÇÕES GERAIS**

ABERTURA DAS PROPOSTAS ATÉ: XX minutos antes do horário previsto para o início da sessão de disputa de preços

SISTEMA ELETRÔNICO UTILIZADO: **COMPRAS.GOV.BR**

ENDEREÇO ELETRÔNICO: [www.gov.br/compras](http://www.gov.br/compras)

**DADOS PARA CONTATO**

AGENTE DE CONTRATAÇÃO:

FONE:

E-MAIL:

E-MAIL ALTERNATIVO:

ENDEREÇO:

Os períodos para recebimento de propostas e para início da sessão de disputa de preços estarão indicados no aviso de abertura do certame.

OBSERVAÇÃO 1: Para todas as referências de tempo será obrigatoriamente adotado o horário de Brasília – DF.

OBSERVAÇÃO 2: Na hipótese de não haver expediente na data fixada, ficará a sessão adiada para o primeiro dia útil subsequente, no mesmo site e hora, salvo as disposições em contrário.



Documento assinado eletronicamente por **MARIA FERNANDA DE CARVALHO NUNES, 4646371.120101** e matrícula **4646371**, em 05/05/2026, às 17:07.

---



A autenticidade deste documento pode ser conferida no site <http://www.peintegrado.pe.gov.br/Validacao.aspx>, informando o código de validação **11ddd04e-be73-48ba-b120-2ff01827f784**

---