TRIBUNAL DE JUSTICA DO ESTADO DO AMAPA
Rua General Rondon, 1295 - Bairro Centro, Macapá/AP, CEP 68900-911
Telefone: - https://www.tjap.jus.br

EDITAL Nº 217/2026

Processo nº 0005241-02.2026.8.03.0901

Torna-se público que o Tribunal de Justiça do Estado do Amapá, por meio da Secretaria de Gestão de Licitações e Contratos, sediada na Av. General Rondon, nº 1295, Centro, Macapá/AP, realizará licitação, na modalidade pregão, de acordo com o contido no Processo Administrativo nº 0005241-02.2026.8.03.0901, nos termos da Lei nº 14.133, de 1º de abril de 2021 e demais legislações aplicáveis, conforme data, horário e endereço indicados a seguir:

Data de sessão: 18/08/2026
Horário da abertura da sessão: 08 horas
Endereço: compras.gov.br - UASG: 925306

1. OBJETO

1.1. O objeto da presente licitação é o registro de preços para aquisição de soluções de segurança da informação incluindo firewalls, soluções de gerenciamento, controle de acesso, acessórios necessários e serviços de sustentação e suporte, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 23 (vinte e três) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. PARTICIPAÇÃO NA LICITAÇÃO

2.1. 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), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

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

2.2. 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, excluída 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.

2.3. É de responsabilidade 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.

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

2.5. Não poderão disputar desta licitação:

2.5.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.5.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.5.2.1. o autor a que se refere este item poderá participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.5.2.2. equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.5.2.3. o disposto neste item não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.5.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.5.3.1. empresa a que se refere este item poderá participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.5.3.2. o disposto neste item não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.5.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.5.4.1. Este impedimento de que trata este item será também aplicado ao 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.

2.5.5. aquele que mantenha 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 licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.5.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.5.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.5.8. agente público do TJAP, mesmo que indiretamente, inclusive na execução do contrato, 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 nº 14.133, de 2021;

2.5.8.1. A vedação de que trata este item estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

2.5.9. pessoas jurídicas reunidas em consórcio;

2.5.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. 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.

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

3.3.1. 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;

3.3.2. 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 7°, XXXIII, da Constituição;

3.3.3. 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;

3.3.4. 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.

3.4. A falsidade da declaração de que trata os itens 3.3 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.5. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

3.6. 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.

3.7. 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.

3.8. 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:

3.8.1. 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

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

3.9. 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:

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

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

3.10. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.9 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.

3.11. 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.

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

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor unitário e total do item;

4.1.2. Marca;

4.1.3. Fabricante;

4.1.4. Quantidade cotada;

4.1.5. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. O licitante não poderá oferecer proposta em quantitativo inferior ao previsto para contratação.

4.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.5. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.6. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.7. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.8.1. O prazo de validade da proposta não será inferior a 90 (noventa) dias, a contar da data de sua apresentação.

4.8.2. Os licitantes devem respeitar os preços máximos estabelecidos neste Edital e seus anexos;

4.8.3. O preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos neste edital e seus anexos.

4.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas do Estado do Amapá e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e endereço indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item.

5.6. critério de julgamento é menor preço por grupo.

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

5.8. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.9. 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 1% (um por cento).

5.10. 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.

5.11. O procedimento seguirá de acordo com o modo de disputa adotado.

5.12. Para o envio de lances no pregão eletrônico, será adotado o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.12.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.12.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.13. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.16. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a

sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.18. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.19. 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.

5.20. 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 e desde que devidamente regulamentados:

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

5.20.2. 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;

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

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

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

5.21.1. empresas estabelecidas no Estado do Amapá;

5.21.2. empresas brasileiras;

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

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

5.22. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados.

5.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.23.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.24. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.24.1. A proposta constitui-se em documento formal, conforme Anexo VIII, no qual devem constar as seguintes informações:

5.24.1.1. Especificações do objeto, contendo descrição dos itens e seus respectivos valores unitários e totais;

5.24.1.2. Dados da empresa, contendo CNPJ, razão social, nome fantasia, e-mail, contato telefônico, número de Whatsapp, nome do representante legal e dados bancários (banco, agência e número da conta corrente); e

5.24.1.3. Assinatura do representante legal da empresa.

5.24.2. Juntamente com a proposta o licitante deverá apresentar os seguintes documentos complementares:

5.24.2.1. As especificações técnicas completas dos equipamentos e softwares ofertados neste certame, deverão ser confirmadas por meio de uma “matriz comprovatória” ou “ponto a ponto” anexada à proposta comercial, incluindo todos os PART NUMBERS relacionados, bem como a inserção de datasheets/folhetos técnicos oficiais do fabricante, sob pena de desclassificação.

5.24.2.2. Todos os equipamentos, módulos, fontes, transceivers, soluções de gerenciamento e plataformas ofertados neste certame, devem ser do mesmo fabricante.

5.24.2.3. O licitante deverá entregar declaração oficial de que os equipamentos, soluções de

gerenciamento e plataformas estão em linha de produção e sem previsão de descontinuidade pelo fabricante, esta declaração deverá ser destinada ao Tribunal de Justiça do Estado do Amapá para este certame específico, com data atual.

5.24.2.4. A proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de “COPIAR” e “COLAR” o descritivo contido no edital não será caracterizado como descritivo da proposta.

5.24.2.5. Visando garantir e comprovar que a solução ofertada atenda as expectativas do CONTRATANTE, o licitante deverá apresentar com sua proposta uma planilha comprovando atender todas as linhas e exigências deste Documento. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.). Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem quaisquer ônus adicionais e independentemente da existência de contrato de manutenção.

5.24.2.6. Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta.

5.24.2.7. Para os ITENS 22 - "BANCO DE HORAS TÉCNICAS" e 23 - "UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON" : Visando garantir a qualidade e boa execução dos serviços de implementação do projeto, a licitante deverá apresentar em sua proposta os PARTNUMBER dos serviços do fabricante do produto que sejam compatíveis aos descritos neste Documento ou apresentar comprovação de entrega de qualidade de serviço por meio de documentos da qualificação técnico operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.

5.24.3. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.25. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e nos itens 2.5 e 2.6 do Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep);

6.1.4. Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, mantido pelo Conselho Nacional de Justiça (https://www.cnj.jus.br/improbidade_adm/consultar_requerido.php); e

6.1.5. Certidão negativa de licitante inidôneo, emitida pelo Tribunal de Contas da União (https://contas.tcu.gov.br/ords/f?p=1660:3:9858666689572::::P3_TIPO_RELACAO:INIDONEO)

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outro.

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de julgamento da proposta.

6.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da Resolução nº 1571/2023 – TJAP.

6.6. Será desclassificada a proposta vencedora que:

6.6.1. contiver vícios insanáveis;

6.6.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.7.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do pregoeiro, que comprove:

6.7.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.7.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.9. Erros meramente materiais não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.9.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.10. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

6.11. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.12. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

6.13. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.14. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.15. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

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

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.2.1. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.3. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia autenticada em cartório ou por servidor público do TJAP, quando houver necessidade com motivo registrado na sessão

pública.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou em formato eletrônico.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei.

7.7. 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.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem 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 entrega das propostas.

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

7.9.1. 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.

7.10. 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.

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

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 02 (duas) horas prorrogável por igual período, contado da solicitação do pregoeiro.

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

7.12.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e Resolução nº 1571/2023 – TJAP, art. 39, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo de 02 horas.

7.16. 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.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante, a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão.

8.3.1. O prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. O prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.3. Na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico www.tjap.jus.br.

8.10.1. O interessado pode requerer instrução para acesso aos autos.

9. DO CONTRATO

9.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado termo de contrato, ou outro instrumento equivalente.

9.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato ou instrumento equivalente, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

9.2.1. A assinatura do termo de contrato observará o disposto nos itens 14.7 a 14.11.

9.2.2. O prazo do item 9.2 poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

9.2.3. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

9.2.4. Deverá ser apresentada, até a assinatura do contrato, a Declaração de Inexistência de Nepotismo, conforme anexo IX.

10. DA ATA DE REGISTRO DE PREÇOS

10.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a ata de registro de preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

10.1.1. A assinatura da Ata de Registro de Preços observará o disposto nos itens 14.7 a 14.11.

10.1.2. Deverá ser apresentada, até a assinatura da Ata de Registro de Preços, a Declaração de Inexistência de Nepotismo, conforme anexo IX.

10.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

10.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e

10.2.2. a justificativa apresentada seja aceita pela Administração.

10.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

10.4. Serão formalizadas tantas atas de registro de preços quantas forem necessárias para o registro de todos os itens constantes no termo de referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

10.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

10.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas,

mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

10.7. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

11. DA FORMAÇÃO DO CADASTRO DE RESERVA

11.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

11.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

11.1.2. dos licitantes que mantiverem sua proposta original.

11.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

11.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

11.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

11.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

11.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

11.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 da Resolução nº 1594/2023/TJAP.

11.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

11.4.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

11.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

12. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

12.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

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

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

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

12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

12.1.2.4. deixar de apresentar amostra; ou

12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital.

12.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

12.1.4. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

12.1.5. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

12.1.6. fraudar a licitação

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

12.1.7.1. agir em conluio ou em desconformidade com a lei;

12.1.7.2. induzir deliberadamente a erro no julgamento;

12.1.7.3. apresentar amostra falsificada ou deteriorada;

12.1.8. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

12.1.9. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

12.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. impedimento de licitar e contratar e

12.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida.

12.3.2. as peculiaridades do caso concreto

12.3.3. as circunstâncias agravantes ou atenuantes

12.3.4. os danos que dela provierem para a Administração Pública

12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2, 12.1.3 e 12.1.4, a multa será de 0,5% a 15% do valor estimado da licitação.

12.4.2. Para as infrações previstas nos itens 12.1.5, 12.1.6, 12.1.7, 12.1.8 e 12.1.9, a multa será de 15% a 30% do valor estimado da licitação.

12.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

12.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2, 12.1.3 e 12.1.4, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.5, 12.1.6, 12.1.7, 12.1.8 e 12.1.9, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2, 12.1.3 e 12.1.4 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 12.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

12.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

12.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

12.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

12.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

13.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

13.2.1. A impugnação e o pedido de esclarecimento poderão ser realizados mediante o envio para o endereço eletrônico licitacoes@tjap.jus.br.

13.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

13.4. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

14. DISPOSIÇÕES GERAIS

14.1. Será divulgada ata da sessão pública no sistema eletrônico.

14.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

14.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

14.4. A homologação do resultado desta licitação não implicará direito à contratação.

14.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

14.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

14.7. O adjudicatário deverá, obrigatoriamente, efetuar seu cadastro como usuário externo no Sistema Eletrônico de Informações (SEI) do Tribunal de Justiça do Estado do Amapá (TJAP), condição necessária para o recebimento de comunicações formais e participação nos trâmites processuais administrativos referentes à contratação.

14.7.1. Para tanto, deverá realizar previamente o pré-cadastro por meio do seguinte link: https://sei.tjap.jus.br/sei/controlador_externo.php?acao=usuario_externo_enviar_cadastro&acao_origem=usuario_externo_avisar_cadastro&id_orgao_acesso_externo=0

14.7.2. Após o preenchimento do formulário eletrônico, o representante legal que enviou a proposta deverá encaminhar cópias digitalizadas do documento de identidade (RG), CPF e comprovante de endereço para o e-mail institucional sei@tjap.jus.br, a fim de viabilizar a validação do cadastro.

14.7.3. As instruções completas para realização do cadastro de usuários externos estão disponíveis no seguinte endereço eletrônico: https://www.tjap.jus.br/portal/sei/acessos.html

14.8. Realizado o cadastro, o Adjudicatário poderá acessar o sistema, por meio do link: https://sei.tjap.jus.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0

14.9. O não cadastramento no Sistema Eletrônico de Informação - SEI/TJAP configura recusa à assinatura do termo de contrato ou à aceitação do instrumento equivalente, caracterizando o descumprimento total da obrigação assumida nos termos do §5º do art. 90 da Lei federal nº. 14.133, de 2021, sujeitando o Adjudicatário às penalidades legais.

14.10. A realização do cadastro como Usuário Externo no SEI-TJAP importará na aceitação de todos os termos e condições que regem o processo eletrônico, admitindo como válida a assinatura eletrônica na modalidade cadastrada (login/senha), tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas, as quais serão passíveis de apuração civil, penal e administrativa.

14.11. A apresentação de proposta à licitação importa em aceitação expressa de recebimento de notificações por meio eletrônico, utilizando-se o Sistema Eletrônico de Informação do Tribunal – SEI/TJAP.

14.11.1. Efetuado o cadastro, as notificações serão encaminhadas exclusivamente ao endereço eletrônico

registrado.

14.11.2. A ausência de manifestação expressa e tempestiva do cadastrado após o encaminhamento de notificação ao endereço eletrônico registrado poderá importar em declaração de revelia, devendo ser observados os prazos legais para defesa prévia e alegações finais

14.12. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

14.13. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

14.14. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

14.15. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.tjap.jus.br.

14.16. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

14.16.1. Anexo I: Termo de Referência;

14.16.2. Anexo II: Estudo Técnico-Preliminar;

14.16.3. Anexo III: Especificações Técnicas Mínimas do Objeto;

14.16.4. Anexo IV: Justificativa Técnica para Indicação de Marca;

14.16.5. Anexo V: Modelo de Ordem de Serviço;

14.16.6. Anexo VI: Minuta de Ata de Registro de Preços;

14.16.7. Anexo VII: Minuta de Contrato;

14.16.8. Anexo VIII: Modelo de Proposta;

14.16.9. Anexo IX: Declaração de Inexistência de Nepotismo

Macapá-AP, data da assinatura eletrônica

Márcio Pantoja Pacheco
Secretário de Gestão de Licitações e Contratos

Documento assinado eletronicamente por **MARCIO PANTOJA PACHECO**, **Secretário(a)**, em 30/07/2026, às 10:09, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015 .

A autenticidade deste documento pode ser conferida no site https://sei.tjap.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0366028** e o código CRC **E280E23C**.

ANEXOS AO EDITAL

ANEXO I - TERMO DE REFERÊNCIA

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O objeto deste termo de referência é o registro de preços para aquisição de soluções de segurança da informação incluindo firewalls, soluções de gerenciamento, controle de acesso, acessórios necessários e serviços de sustentação e suporte, nos termos das condições estabelecidas neste instrumento e conforme tabela abaixo:

GRUPO ÚNICO					
ITEM	**DESCRIÇÃO**	**QTD.**	**UNIDADE DE MEDIDA**	**PREÇO UNITÁRIO ESTIMADO (R$)**	**PREÇO TOTAL ESTIMADO (R$)**

1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	Unidade	981.874,70	1.963.749,40
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	4	Unidade	252.793,11	1.011.172,44
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	4	Unidade	109.501,73	438.006,92
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	6	Unidade	24.216,07	145.296,42
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	20	Unidade	19.548,56	390.971,20
6	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 06	4	Unidade	105.206,58	420.826,32
7	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) COMO SERVIÇO - TIPO 02	240	Firewall por mês	5.927,44	1.422.585,60
8	LICENCIAMENTO UTP PARA NGFW - TIPO 03	2	Unidade	71.830,97	143.661,94
9	LICENCIAMENTO UTP PARA NGFW - TIPO 04	4	Unidade	17.584,07	70.336,28
10	LICENCIAMENTO UTP PARA NGFW - TIPO 05	22	Unidade	13.385,09	294.471,98
11	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA - TIPO 01	10	Unidade	50.918,74	509.187,40
12	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA COMO SERVIÇO - TIPO 01	600	Unidade	1.018,95	611.370,00
13	SOLUÇÃO DE GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO	6	Unidade	14.213,89	85.283,34

14	SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC) PARA GRUPO DE 100 ENDPOINTS	50	Unidade	26.917,83	1.345.891,50
15	SOLUÇÃO DE ACESSO À REDE DE CONFIANÇA ZERO (ZTNA)	20	Unidade	31.347,41	626.948,20
16	SOLUÇÃO DE SERVIÇO DE ACESSO SEGURO DE BORDA (SASE)	1000	Unidade	3.248,68	3.248.680,00
17	SOLUÇÃO DE TOKEN PARA MFA PARA GRUPO DE 50 USUÁRIOS	20	Unidade	34.086,84	681.736,80
18	TRANSCEIVER SFP 1000Base-SX	40	Unidade	634,90	25.396,00
19	TRANSCEIVER SFP+ 10GBase-SR	20	Unidade	814,30	16.286,00
20	TRANSCEIVER SFP+ 10GBase-LR	10	Unidade	1.400,76	14.007,60
21	TRANSCEIVER QSFP+ 40GBase-SR4	10	Unidade	4.756,23	47.562,30
22	BANCO DE HORAS TÉCNICAS	1000	Horas Técnicas	712,70	712.700,00
23	UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON	500	UST	960,26	480.130,00
PREÇO GLOBAL ESTIMADO (R$)					**14.706.257,64**

1.2. O objeto desta contratação é caracterizado como comum.

1.3. O custo estimado total da contratação, que é o máximo aceitável, é de R$ 14.706.257,64 (quatorze milhões, setecentos e seis mil duzentos e cinquenta e sete reais e sessenta e quatro centavos), conforme custos unitários apostos na tabela acima.

1.4. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre contratante e contratado, conforme especificado na matriz de risco constante do Contrato.

1.5. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços registrados, nas seguintes situações:

1.5.1. 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 da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

1.5.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

1.5.3. Serão reajustados os preços registrados, respeitada a contagem da anualidade e o Índice de Custo da Tecnologia da Informação (ICTI)

1.6. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.6.1. A prorrogação prevista nos arts. 106 e 107 da Lei nº 14.133/2021 aplica-se apenas às parcelas de natureza contínua, não alcançando os itens de entrega única. Os prazos de garantia, suporte, atualização e licenciamento observarão as disposições específicas deste Termo de Referência.

1.7. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.8. Prevalecerá o disposto no Termo de Referência, em caso de divergência com o Estudo Técnico Preliminar.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A fundamentação da contratação e seus quantitativos encontra-se pormenorizada no estudo técnico preliminar, apêndice deste termo de referência.

2.2. Esta contratação será processada nos moldes estabelecidos pela Lei nº 14.133/2021.

2.3. O objeto da contratação está previsto no Plano de Contratações Anual 2026, com o DFD nº 269/2025.

2.4. O objeto da contratação também está alinhado com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD) e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do TJAP.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo, encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Com base nas necessidades de negócio e tecnológicas, foram definidos como requisitos necessários e suficientes à escolha da solução de TIC, os seguintes requisitos técnicos e funcionais.

4.1.1. **PADRONIZAÇÃO E INTEROPERABILIDADE DA INFRAESTRUTURA:** A compatibilidade com a infraestrutura existente precisa ser garantida, pois simplifica a integração e a gestão centralizada. Esse alinhamento tecnológico evita problemas de interoperabilidade e facilita a manutenção e o treinamento da equipe interna. Sendo assim, a solução a ser adquirida deverá possuir integração nativa com os dispositivos e serviços Fortinet já existentes no ambiente do TJAP, incluindo FortiGate, FortiAnalyzer, FortiManager, FortiWeb. Além disso, deverá ser compatível com as versões atualmente em operação nos datacenters e redes do Tribunal, permitindo expansão sem necessidade de reconfiguração do ambiente preexistente. E ainda, deverá suportar o gerenciamento centralizado de políticas, logs, configurações e eventos de segurança via FortiManager e FortiAnalyzer.

4.1.2. **MARCA/FABRICANTE:** A solução deverá ser obrigatoriamente da marca Fortinet, visando manter a padronização adotada institucionalmente e a compatibilidade com os demais ativos do ecossistema de segurança do TJAP.

4.1.3. **SOLUÇÃO INTEGRADA:** A definição de uma solução integrada baseia-se na necessidade de expandir e otimizar a infraestrutura de segurança da informação do Tribunal de forma que todos os sistemas (hardwares e softwares) interoperem entre si, ou seja funcionem de maneira conjunta/integrada.

4.1.4. **FERRAMENTA DE GESTÃO CENTRALIZADA:** A gestão e o monitoramento centralizado, proporcionados pelas plataformas para gerenciamento, são essenciais para a administração do ambiente. Essas ferramentas permitem o acompanhamento em tempo real do desempenho, a configuração remota dos dispositivos e a emissão de alertas para ações corretivas, garantindo uma operação proativa.

4.1.5. **DESEMPENHO, DISPONIBILIDADE E CAPACIDADE:** Alto desempenho com suporte à operação em alta disponibilidade (HA), com *failover* automático e capacidade de suportar a carga de trabalho atual e futura estimada, com possibilidade de expansão por licenciamento modular.

4.1.6. **ESCALABILIDADE:** A escalabilidade é outro aspecto crítico, permitindo que a estrutura se expanda de forma horizontal e vertical conforme o aumento das demandas, sem prejudicar o desempenho ou a integridade dos dados. Tal característica possibilitará a incorporação de novos ativos e a atualização dos sistemas de maneira simples e eficaz.

4.1.7. **GESTÃO, AUDITORIA E CONFORMIDADE:** A solução deverá possibilitar: registro e análise de logs de eventos e acessos com geração de relatórios gerenciais e técnicos para fins de auditoria e conformidade com a Resolução CNJ nº 396/2021 (PGSI-JUD); capacidade de integração com ferramentas de SIEM existentes ou futuras; e funcionalidade de alertas em tempo real e *dashboards* personalizáveis para visualização de riscos e ocorrências.

4.1.8. **SEGURANÇA DA INFORMAÇÃO:** A solução deverá possibilitar: Implementação de políticas de segurança em múltiplas camadas, com prevenção de intrusão (IPS), filtragem de conteúdo, controle de aplicações e detecção de anomalias; suporte a autenticação multifator (MFA), integrada ao diretório corporativo (LDAP/Active Directory), com tokens físicos e virtuais; capacidade de realizar segmentação de rede (VLAN, Zonas de Segurança) e aplicação de políticas distintas por tipo de usuário, serviço ou dispositivo; e suporte a SD-WAN segura com balanceamento inteligente de links e definição de rotas por aplicação.

4.1.9. **CAPACITAÇÃO DA EQUIPE TÉCNICA:** A equipe técnica do TJAP possui formação e capacitação tendo em vista a infraestrutura atual, o que permite o uso imediato e eficiente da solução, evitando necessidade de requalificação ou reengenharia. Sendo assim, a solução a ser adquirida deverá ser da marca Fortinet.

4.1.10. **SUPORTE TÉCNICO E GARANTIA:** A garantia das soluções deverá ser fornecida para um período de 60 (sessenta) meses, incluindo atualizações, suporte e renovações automáticas, suporte “on-site” e "online", na modalidade 24x7 e possibilidade de substituição de *hardware* em regime N3BD (*Next Three Business Day*) e manutenção corretiva.

4.1.11. **RESPONSABILIDADE AMBIENTAL:** Além disso, a responsabilidade ambiental deve ser considerada, privilegiando soluções que apresentem alta eficiência energética e práticas de operação ambientalmente responsáveis, reduzindo o impacto ecológico da infraestrutura de TI.

4.1.12. **INDEPENDÊNCIA CONTRATUAL:** A independência contratual assegura que a Instituição não fique excessivamente vinculada a um único fornecedor ou tecnologia, permitindo liberdade para realizar ajustes, substituições ou expansões sem restrições impostas por cláusulas dubiamente exclusivas. Esse fator reduz riscos de dependência, facilita negociações mais vantajosas e garante maior poder de escolha em futuras aquisições, manutenções ou atualizações, promovendo sustentabilidade e autonomia na gestão da infraestrutura.

4.1.13. **ESTADO DE EQUIPAMENTO “NOVO”:** A aquisição de equipamentos novos garante maior vida útil, menor probabilidade de falhas e melhor desempenho operacional. Além disso, reduz a necessidade de manutenções corretivas frequentes, assegura compatibilidade com as tecnologias mais recentes e oferece cobertura integral de garantia do fabricante. Isso contribui para maior confiabilidade, previsibilidade de custos e melhor aproveitamento dos investimentos em infraestrutura.

4.1.14. **REFERÊNCIA TECNOLÓGICA:** Os modelos indicados nas especificações técnicas são apresentados como referência tecnológica, em razão da padronização adotada pela Administração. Será admitido o fornecimento de outros modelos do mesmo fabricante, desde que comprovadamente equivalentes em termos técnicos, funcionais e operacionais e compatíveis com a infraestrutura existente, cuja equivalência será analisada e validada pela Secretaria de Tecnologia da Informação e Comunicação (SETIC).

4.1.15. **REQUISITOS DE SUPORTE TÉCNICO:** Cobertura 24x07 (24 horas por dia x 07 dias por semana); A CONTRATADA deve possuir suporte técnico remoto para a solução de problemas comuns de suporte; A CONTRATADA deve realizar atendimento on-site em até 05 (cinco) dias úteis, com tempo de atendimento contado a partir da abertura do chamado; O FABRICANTE deverá possuir Central de Atendimento online para abertura dos chamados de garantia, comprometendo-se a manter estes registros constando a descrição do problema; Todos os itens de software que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do FABRICANTE; O serviço de suporte deverá ser do FABRICANTE do equipamento ou por assistência técnica qualificada e indicada por este por meio de declaração.

Sustentabilidade

4.2. O licitante deverá atender no que couber, os critérios de sustentabilidade ambiental devendo utilizar, quando disponíveis no mercado, materiais que sejam reciclados, reutilizados e biodegradáveis, bem como priorizar o emprego de mão-de-obra, materiais, tecnologias e matérias-primas de origem local para execução e operação do objeto, bem como respeitar as Normas Brasileiras (NBR) publicadas pela Associação Brasileira de Normas Técnicas (ABNT) sobre resíduos sólidos.

4.3. Deverá a contratada adotar boas práticas de sustentabilidade, baseadas na otimização e economia de recursos e na redução da poluição ambiental, quando da execução da confecção dos equipamentos contratados, tais como uso racional de água, economia de energia elétrica, economia de materiais, separação de resíduos e materiais recicláveis.

4.4. Dessa forma, considerando a necessidade de implantação de práticas de sustentabilidade, deve-se contratar empresas que sejam comprometidas com a sustentabilidade.

4.5. Visando um maior desenvolvimento nacional sustentável, a presente aquisição observará os princípios da economicidade, eficácia, eficiência para melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, inclusive com respeito a impactos ambientais, de forma a utilizar-se da menor quantidade possível de recursos que causem impactos negativos para a sociedade e para o meio ambiente.

4.6. Dessa forma, considerando a necessidade de implantação de práticas de sustentabilidade, deve-se priorizar contratar empresa fornecedora que seja comprometida com a sustentabilidade.

4.7. Todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias), deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, em especial a responsabilidade compartilhada pelo ciclo de vida do produto. A empresa vencedora deverá aplicar o disposto nos Artigos de nºs 31 a 33 da Lei nº 12.305 de 02 de agosto de 2010, no que diz respeito à Logística Reversa.

Indicação de marcas ou modelos

4.8. Na presente contratação será admitida a indicação da marca "Fortinet", conforme justificativa técnica constante no Despacho (id 0292534), o qual foi replicado no anexo V do Edital.

Subcontratação

4.9. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

4.10. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

4.11. Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.12. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.13. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5. MODELO DE EXECUÇÃO CONTRATUAL

Condições de entrega

5.1. Todos os itens (equipamentos) deverão ser entregues nas dependências do CONTRATANTE, pela CONTRATADA.

5.2. Endereço de entrega: “Prédio Anexo da Sede do TJAP (Anexo Desembargador Eduardo Contreras – SITE A) / Av. Raimundo Álvares da Costa, 400 - Central, Macapá - AP, 68900-074 / Horário de funcionamento: De segunda-feira a sexta-feira - 7h:30min às 14h:30min”.

5.3. O prazo de entrega de todos os itens (equipamentos) será de 90 dias corridos, contados a partir da assinatura do Contrato.

Características do Serviço

5.4. Para os serviços contínuos - Itens 7 e 12

5.4.1. Contratação de serviço contínuo que compreende o fornecimento, implantação, licenciamento, atualização e manutenção integrada de solução de segurança de rede — incluindo os equipamentos necessários e suas respectivas licenças — prestado de forma “as a Service”. Todo o conjunto (hardware e licenciamento) será disponibilizado ao CONTRATANTE como serviço gerenciado, e não como bem isolado.

5.4.2. O serviço deverá ser prestado de forma ininterrupta pelo prazo de 12 (doze) meses. Durante todo esse período, o contratado deverá assegurar a plena operação do hardware e das licenças, bem como sua substituição preventiva ou corretiva, atualizações de software/firmware e suporte técnico especializado.

5.4.3. Apesar de tratar-se de prestação de serviço contínuo, o valor deverá ser apresentado na proposta como montante global correspondente aos 12 (doze) meses de execução. Ou seja, a proposta deve apresentar um valor único total para o período integral contratado.

5.5. Para o item 12

5.5.1. Contratação de serviço contínuo que compreende o fornecimento, implantação, licenciamento, atualização e manutenção integrada de solução de segurança de rede — incluindo suas respectivas máquinas virtuais licenças — prestado de forma as a Service. Todo o conjunto (máquina virtual e licenciamento) será disponibilizado ao CONTRATANTE como serviço gerenciado, e não como bem isolado.

5.5.2. O serviço deverá ser prestado de forma ininterrupta pelo prazo de 12 (doze) meses. Durante todo esse período, o contratado deverá assegurar a plena operação da máquina virtual e das licenças, bem como sua substituição preventiva ou corretiva, atualizações de software/firmware e suporte técnico especializado.

5.5.3. Apesar de tratar-se de prestação de serviço contínuo, o valor deverá ser apresentado na proposta como montante global correspondente aos 12 (doze) meses de execução. Ou seja, a proposta deve apresentar um valor único total para o período integral contratado.

5.5.4. Para fins de faturamento, o pagamento será realizado mensalmente em parcelas correspondentes a 1/12 (um doze avos) do valor global contratado, garantindo a execução financeira conforme a prestação efetiva do serviço.

5.6. Quanto ao pagamento, deverá ser seguido o cronograma para o pagamento mensal abaixo:

5.6.1. Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;

5.6.2. Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;

5.6.3. Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;

5.6.4. O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

5.7. Para o item 16

5.7.1. A gerência deve ser disponibilizada em nuvem, sem usar qualquer recurso do cliente;

5.7.2. A solução SASE deve ser baseada em uma arquitetura em nuvem, permitindo a integração de funções de rede e segurança como serviço em uma única plataforma;

5.7.3. A solução SASE deve ser (SaaS) software baseado em serviço que permite aos clientes acessarem a Internet com segurança e proteção. Deve garantir a proteção de endpoints e usuários remotos off-net (fora da rede) com o mesmo nível de segurança de quando estão na rede, independentemente de sua localização;

5.7.4. A plataforma em nuvem da solução SASE deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semanas, com disponibilidade mensal de 99.999% para todos os serviços;

5.7.5. Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses.

5.8. Demais condições de execução, rotinas, materiais a serem disponibilizados constam no Anexo A do Estudo Técnico Preliminar - Especificações Técnicas

Informações relevantes para o dimensionamento da proposta

5.9. A demanda do órgão tem como base as seguintes características:

5.9.1. As especificações técnicas completas dos equipamentos e softwares ofertados neste certame, deverão ser confirmadas por meio de uma “matriz comprovatória” ou “ponto a ponto” anexada à proposta comercial, incluindo todos os PART NUMBERS relacionados, bem como a inserção de datasheets/folhetos técnicos oficiais do fabricante, sob pena de desclassificação.

5.9.2. Todos os equipamentos, módulos, fontes, transceivers, soluções de gerenciamento e plataformas ofertados neste certame, devem ser do mesmo fabricante.

5.9.3. O licitante deverá entregar declaração oficial de que os equipamentos, soluções de gerenciamento e plataformas estão em linha de produção e sem previsão de descontinuidade pelo fabricante, esta declaração deverá ser destinada ao Tribunal de Justiça do Estado do Amapá para este certame específico, com data atual.

5.9.4. Visando garantir e comprovar que a solução ofertada atenda as expectativas do CONTRATANTE, o licitante deverá apresentar com sua proposta uma planilha comprovando atender todas as linhas e exigências deste Documento. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.). Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem quaisquer ônus adicionais e independentemente da existência de contrato de manutenção.

5.9.5. Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta.

5.9.6. Para os ITENS 22 - "BANCO DE HORAS TÉCNICAS" e 23 - "UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON" : Visando garantir a qualidade e boa execução dos serviços de implementação do projeto, a licitante deverá apresentar em sua proposta os PARTNUMBER dos serviços do fabricante do produto que sejam compatíveis aos descritos neste Documento ou apresentar comprovação de entrega de qualidade de serviço por meio de documentos da qualificação técnico operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá

ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.

Especificação da garantia do serviço

5.10. O prazo de garantia, suporte técnico, atualização e/ou licenciamento observará o disposto no Anexo A – Especificações Técnicas Mínimas do Objeto, sendo de 60 meses para os itens 1 a 6, 8 a 10, 11, 13, 14, 15, 16 e 17, quando aplicável; de 12 meses para os itens 18, 19, 20 e 21; e pelo período de vigência contratual de 12 meses para os itens 7, 12, 22 e 23, sem prejuízo das obrigações específicas de suporte, atualização, substituição e manutenção previstas para cada item.

Transferência de conhecimento

5.11. A transferência do conhecimento deverá ser realizada observando-se o que segue:

5.11.1. Durante a execução do contrato, a contratada deverá assegurar transferência contínua de conhecimento técnico e operacional à equipe da SETIC, de modo a preservar a autonomia do Tribunal na gestão dos equipamentos e softwares, e na comunicação com o suporte do fabricante. As ações de transferência de conhecimento incluirão:

5.11.1.1. Disponibilização de relatórios técnicos e atualizações realizadas (eventual utilização de garantia de equipamentos e softwares);

5.11.1.2. Registro de lições aprendidas em cada ocorrência relevante (eventual utilização de garantia de equipamentos e softwares);

5.11.1.3. Reunião técnica semestral entre contratada e SETIC para alinhamento sobre padrões de atendimento e eventuais recomendações de melhoria (aplicação nos serviços de natureza continuada).

Procedimentos de transição e finalização do contrato

5.12. O contrato administrativo é a base para o funcionamento da máquina pública. A legislação norteadora dos contratos administrativos por entes públicos é a Lei n.º 14.133/2021.

5.13. Sendo assim, no caso de uma eventual interrupção contratual, que impeça o fornecimento dos serviços da CONTRATADA, é possível utilizar os dispositivos legais contidos nessa legislação, como por exemplo, rescisão contratual e contratação emergencial, bem como outros dispositivos previstos, a fim de restabelecimento dos serviços.

5.14. A transição contratual refere-se ao encerramento controlado da contratação, a ser executada nos meses finais de vigência, visando à continuidade dos serviços e à rastreabilidade das informações técnicas.

5.15. Ações previstas:

5.15.1. Consolidação dos relatórios de suporte e manutenção executados ao longo do contrato, incluindo histórico de chamados, peças substituídas, prazos de atendimento e confirmações de encerramento emitidas;

5.15.2. Validação técnica do estado dos equipamentos, assegurando ausência de pendências de garantia ou suporte;

5.15.3. Atualização do inventário patrimonial e técnico nos sistemas internos do TJAP;

5.15.4. Reunião de encerramento técnico entre a Contratada e a SETIC, para revisão dos serviços, identificação de lições aprendidas e recomendações para contratações futuras;

5.15.5. Elaboração e assinatura do termo de encerramento contratual, com atesto final da execução.

Ação	Unidade Responsável	Prazo Estimado
Consolidação de relatórios e históricos de suporte.	Contratada / SGLC	D-30 dias antes do encerramento
Validação técnica do estado dos equipamentos.	SETIC / CSDC	D-20 dias
Atualização do inventário e registros.	CSDC	D-15 dias
Reunião de encerramento técnico e elaboração de termo final.	SETIC / CGTI / Contratada	D-10 dias
Arquivamento do termo e encerramento processual.	SGLC / CGTI	D-5 dias

Formas de comunicação

5.16. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

5.16.1. Ofício;

5.16.2. E-mail;

5.16.3. Aplicativos de mensagens por smartphones, como Whatsapp ou Telegram;

5.16.4. Videoconferência através de aplicativo definido pelo Contratante.

Manutenção de sigilo e normas de segurança

5.17. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre a Administração e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. A Administração poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. A Administração poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo gestor do contrato, ou pelo seu respectivo substituto, o qual acumulará também as funções dos fiscais técnico e administrativo, cabendo, em especial:

6.6.1. informar à autoridade superior as ocorrências relacionadas à execução do contrato cujas medidas ultrapassem a sua competência, bem como as medidas adotadas, conforme registros realizados;

6.6.2. acompanhar a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e de pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

6.6.3. coordenar a rotina de acompanhamento e de fiscalização do contrato, cujo histórico de gerenciamento deverá conter todos os registros formais da execução, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, e elaborar relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

6.6.4. coordenar os atos preparatórios à instrução processual e ao envio da documentação pertinente ao setor de contratos para a formalização de procedimentos;

6.6.5. elaborar o relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração, conforme alínea "d" do inciso VI do § 3º do art. 174 da Lei nº 14.133, de 2021, com as informações obtidas durante a execução do contrato;

6.6.6. coordenar a atualização contínua do relatório de riscos durante a gestão do contrato;

6.6.7. emitir documento comprobatório da avaliação quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, a constarem do cadastro de atesto de cumprimento de obrigações conforme disposto em regulamento;

6.6.8. realizar o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências técnicas e administrativas;

6.6.9. realizar o recebimento definitivo do objeto do contrato, mediante termo detalhado que comprove o atendimento das exigências contratuais; e

6.6.10. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso.

Fiscalização técnica

6.7. Caberá ao gestor do contrato, no exercício da função de fiscalização técnica, em especial:

6.7.1. acompanhar a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

6.7.2. anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

6.7.3. emitir notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção; e

6.7.4. fiscalizar a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato para ratificação.

Fiscalização administrativa

6.8. Caberá ao gestor do contrato, no exercício da função de fiscalização administrativa, em especial:

6.8.1. verificar a manutenção das condições de habilitação da contratada e acompanhar o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;

6.8.2. examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias; e

6.8.3. atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. A avaliação da execução do objeto observará o disposto neste item:

7.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.1.1.1. não produzir os resultados acordados;

7.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

Recebimento dos serviços

7.2. Os serviços serão recebidos provisoriamente, no prazo de 05 (cinco) dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

7.3. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.4. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

7.5. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

7.6. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.7. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.7.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.7.2. O Contratado fica obrigado 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, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.7.3. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.7.4. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.7.5. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.8. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.9. Os serviços serão recebidos definitivamente no prazo de 05 (cinco) dias úteis, contados da entrega da nota fiscal, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.9.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

7.9.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

7.9.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

7.9.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização; e

7.9.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.10. 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.

7.11. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.12. 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.

Recebimento dos bens

7.13. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.14. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.15. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.15.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.16. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.17. 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.

7.18. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.19. 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.

Liquidação

7.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

7.21. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.22.1. o prazo de validade;

7.22.2. a data da emissão;

7.22.3. os dados do contrato e do órgão contratante;

7.22.4. o período respectivo de execução do contrato;

7.22.5. o valor a pagar; e

7.22.6. eventual destaque do valor de retenções tributárias cabíveis.

7.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

7.24. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

7.25. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.26. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.27. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.28. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.29. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.30. O pagamento observará os prazos e os marcos iniciais específicos previstos nos itens 7.34 e 7.35, conforme a natureza de cada item, após a regular liquidação da despesa.

7.31. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo da Tecnologia da Informação (ICTI).

Forma de pagamento

7.32. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

7.33. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.34. Para os itens 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20 e 21, o pagamento será efetuado no prazo de até 30 (trinta) dias corridos, contados do recebimento definitivo do objeto, mediante apresentação da respectiva Nota Fiscal/Fatura, em conformidade com a Nota de Empenho, devidamente conferida e atestada pelo fiscal do contrato ou servidor responsável pelo recebimento.

7.35. Para os itens 7, 12, 22 e 23, por se tratarem de itens vinculados à prestação de serviços, o pagamento será realizado mensalmente, conforme a efetiva prestação dos serviços e após a respectiva validação técnica pela Administração, observando-se o seguinte cronograma:

7.35.1. Validação técnica: até o dia 5 (cinco) de cada mês subsequente ao da prestação dos serviços, a CONTRATADA deverá apresentar relatório contendo a descrição dos serviços prestados no período;

7.35.2. Emissão da Nota Fiscal/Fatura: após a validação técnica, a CONTRATADA deverá emitir a Nota Fiscal/Fatura até o dia 10 (dez) do respectivo mês;

7.35.3. Processamento do pagamento: o CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) do respectivo mês, desde que a documentação apresentada esteja regular e os serviços tenham sido devidamente atestados;

7.35.4. O CONTRATANTE poderá solicitar a prorrogação do vencimento da fatura ou a sua correção quando verificar inconsistência, irregularidade ou necessidade de complementação documental, sem ônus para a Administração.

7.36. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.37. Independentemente do percentual de tributo informado em proposta, planilha ou documento equivalente, quando houver, serão retidos na fonte, por ocasião do pagamento, os percentuais estabelecidos na legislação vigente.

7.38. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá 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.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade pregão, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço por grupo.

Regime de execução

8.2. Para os itens 1 a 6 e 8 a 21, relativos ao fornecimento de bens, equipamentos, softwares, licenças e acessórios, o fornecimento será integral ou parcelado, conforme as quantidades efetivamente demandadas pela Administração.

8.3. Para os itens 7, 12, 22 e 23, caracterizados como serviços continuados, a execução ocorrerá de forma contínua durante a vigência contratual, observadas as respectivas unidades de medida e as condições de medição, ateste e pagamento previstas neste Termo de Referência.

Exigências de habilitação

8.4. A habilitação jurídica deve demonstrar a capacidade de o licitante exercer direitos e assumir obrigações, e a documentação a ser apresentada por ele limita-se à comprovação de existência jurídica da pessoa, cujo cumprimento ocorre mediante os seguintes documentos:

8.4.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

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

8.4.3. 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;

8.4.4. Sociedade empresária, sociedade limitada unipessoal – SLU: 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;

8.4.5. 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.

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

8.4.7. 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

8.4.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

Habilitação fiscal, social e trabalhista

8.6. A habilitação fiscal, social e trabalhista deve ser demonstrada mediante as seguintes provas:

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

8.6.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão 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, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.6.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.6.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.6.5. Prova de inscrição no cadastro de contribuintes municipal ou distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.6.6. Prova de regularidade com a fazenda municipal ou distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.6.7. Prova de inscrição no cadastro de contribuintes estadual ou distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.6.8. Prova de regularidade com a fazenda estadual ou distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.7. Caso o fornecedor seja considerado isento dos tributos municipais ou distritais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.8. 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.

Qualificação econômico-financeira

8.9. A qualificação econômico-financeira deve ser demonstrada mediante os seguintes documentos:

8.9.1. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do fornecedor, caso se trate de pessoa física, desde que admitida a sua contratação, ou de sociedade simples;

8.9.2. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

Qualificação técnica

8.10. A qualificação técnica será demonstrada mediante os seguintes documentos:

8.10.1. Comprovação de aptidão para execução de serviço em complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado.

8.10.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

a) Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de solução de "FIREWALLS" em quantidade não inferior à 50% do solicitado no edital, sendo permitido soma de atestados para atender ao solicitado. Deverá constar, pelo menos os seguintes itens: ITEM 1 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01 ou solução equivalente; ITEM 2 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02 ou solução equivalente.

b) Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de "BANCO DE HORAS TÉCNICAS" relacionado ao objeto, em quantidade não inferior à 50% do solicitado neste edital, sendo permitido soma de atestados para atender ao solicitado.

8.10.1.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

8.10.1.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

8.10.1.4. O 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.

9. ADEQUAÇÃO ORÇAMENTÁRIA

9.1. A indicação da disponibilidade de créditos orçamentários somente será exigida para a formalização do contrato ou de outro instrumento hábil.

10. CASOS OMISSOS

10.1. Os casos omissos serão decididos pela Administração, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais e estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

11. ALTERAÇÕES

11.1. Eventuais retificações neste termo de referência que não alterem a substância da contratação prescindem de nova autorização da Secretaria Geral do TJAP, bastando apenas a aprovação da Secretaria de Gestão de Licitações e Contratos.

Macapá/AP, 10 de julho de 2026

Elaborado por (*assinado eletronicamente)* **Elcio Pires de Souza Junior** Técnico Judiciário	Termo de referência aprovado por (*assinado eletronicamente)* **Marcio Pantoja Pacheco** Secretário de Gestão de Licitações e Contratos

ANEXO II - ESTUDO TÉCNICO PRELIMINAR

REGISTRO DE PREÇOS - AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO INCLUINDO FIREWALLS, SOLUÇÕES DE GERENCIAMENTO, CONTROLE DE ACESSO, ACESSÓRIOS NECESSÁRIOS E SERVIÇOS DE SUSTENTAÇÃO E SUPORTE

1. ESTUDO TÉCNICO PRELIMINAR

1.1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

O Tribunal de Justiça do Estado do Amapá (TJAP), no exercício de sua missão institucional de promover a justiça de forma célere, segura e eficiente, enfrenta desafios crescentes no que se refere à proteção dos ativos de informação, à segurança das comunicações digitais e à resiliência contra ameaças cibernéticas que comprometem a integridade, disponibilidade e confidencialidade dos seus sistemas judiciais e administrativos.

Considerando o vencimento das licenças atuais de softwares e equipamentos de segurança da informação em junho de 2026, há o risco iminente de interrupção da proteção cibernética do TJAP. E ainda, a infraestrutura atual é insuficiente para as novas ameaças e para o volume de tráfego criptografado moderno. Por fim, destaca-se que, atualmente, o TJAP está expandindo suas instalações administrativas e judiciais. Nas próximas obras previstas, cada nova construção ou reforma exigirá nova quantidade de dispositivos de Tecnologia da Informação e Comunicação (TIC).

Nesse sentido, com o avanço das conexões remotas, a ampliação de serviços digitais ao cidadão e a interdependência entre os sistemas internos e externos, tornou-se indispensável investir em uma infraestrutura robusta e integrada de segurança da informação, capaz de prevenir, detectar e responder a incidentes de forma eficaz e tempestiva.

Nesse contexto, destaca-se a necessidade da adoção de soluções tecnológicas que permitam ao TJAP ampliar sua capacidade de defesa cibernética por meio de mecanismos como firewall de próxima geração, autenticação multifator, controle de acesso, segmentação de tráfego, inteligência contra ameaças persistentes (APT), gerenciamento centralizado e integração com ambientes em nuvem.

O TJAP já possui seu ambiente consolidado com a plataforma Fortinet, que oferece um ecossistema de segurança unificada, integrado à estrutura lógica, física e organizacional existente. A escolha por essa plataforma vem ao encontro da política de continuidade dos serviços essenciais de TIC, da proteção de dados sensíveis e da eficiência na operação da segurança institucional.

Adicionalmente, destaca-se a necessidade de garantir redundância e alta disponibilidade da infraestrutura crítica de segurança, de forma a mitigar falhas pontuais e manter a operação ininterrupta dos sistemas mesmo em situações adversas. Para isso, torna-se necessária a aquisição célere de determinados equipamentos ou licenças, com o objetivo de possibilitar substituições emergenciais ou programadas, a fim de assegurar a continuidade dos serviços sem comprometer a proteção da informação e a disponibilidade dos sistemas judiciais.

A presente contratação está alinhada aos interesses institucionais do TJAP, em conformidade com os princípios constitucionais da administração pública, com os marcos normativos da segurança da informação e com os objetivos estratégicos definidos nas Resoluções CNJ n.º 325/2020 (Estratégia Nacional do Poder Judiciário), n.º 370/2021 (ENTIC-JUD) e n.º 396/2021, que institui a Política de Governança da Segurança da Informação no Âmbito do Poder Judiciário.

1.1.2. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

Para atender as necessidades de negócio, é necessário identificar as necessidades tecnológicas que promovam o atendimento dos objetivos institucionais.

Sendo assim, a principal necessidade atual é a de continuidade da padronização atual e expansão da infraestrutura tecnológica de segurança da informação do TJAP diante do crescimento exponencial das ameaças cibernéticas, do aumento da superfície de ataque resultante da transformação digital, da ampliação da estrutura física do Tribunal, bem como da ampliação do acesso remoto aos serviços e sistemas críticos da Justiça.

Para isso, é imprescindível a aquisição de novos ativos. E ainda, é necessário que as soluções a serem adquiridas sejam compatíveis com as soluções já existentes na infraestrutura de TIC atual. Essas ações fortalecem a base tecnológica do TJAP e contribuem diretamente para a melhoria da eficiência dos serviços entregues à sociedade

1.1.3. REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

Com base nas necessidades de negócio e tecnológicas, foram definidos como requisitos necessários e suficientes à escolha da solução de TIC, os seguintes requisitos técnicos e funcionais.

PADRONIZAÇÃO E INTEROPERABILIDADE DA INFRAESTRUTURA: A compatibilidade com a infraestrutura existente precisa ser garantida, pois simplifica a integração e a gestão centralizada. Esse alinhamento tecnológico evita problemas de interoperabilidade e facilita a manutenção e o treinamento da equipe interna. Sendo assim, a solução a ser adquirida deverá possuir integração nativa com os dispositivos e serviços Fortinet já existentes no ambiente do TJAP, incluindo FortiGate, FortiAnalyzer, FortiManager, FortiWeb. Além disso, deverá ser compatível com as versões atualmente em operação nos datacenters e redes do Tribunal, permitindo expansão sem necessidade de reconfiguração do ambiente preexistente. E ainda, deverá suportar o gerenciamento centralizado de políticas, logs, configurações e eventos de segurança via FortiManager e FortiAnalyzer.

MARCA/FABRICANTE: A solução deverá ser obrigatoriamente da marca Fortinet, visando manter a padronização adotada institucionalmente e a compatibilidade com os demais ativos do ecossistema de segurança do TJAP.

SOLUÇÃO INTEGRADA: A definição de uma solução integrada baseia-se na necessidade de expandir e otimizar a infraestrutura de segurança da informação do Tribunal de forma que todos os sistemas (hardwares e softwares) interoperem entre si, ou seja funcionem de maneira conjunta/integrada.

FERRAMENTA DE GESTÃO CENTRALIZADA: A gestão e o monitoramento centralizado, proporcionados pelas plataformas para gerenciamento, são essenciais para a administração do ambiente. Essas ferramentas permitem o acompanhamento em tempo real do desempenho, a configuração remota dos dispositivos e a emissão de alertas para ações corretivas, garantindo uma operação proativa.

DESEMPENHO, DISPONIBILIDADE E CAPACIDADE: Alto desempenho com suporte à operação em alta disponibilidade (HA), com *failover* automático e capacidade de suportar a carga de trabalho atual e futura estimada, com possibilidade de expansão por licenciamento modular.

ESCALABILIDADE: A escalabilidade é outro aspecto crítico, permitindo que a estrutura se expanda de forma horizontal e vertical conforme o aumento das demandas, sem prejudicar o desempenho ou a integridade dos dados. Tal característica possibilitará a incorporação de novos ativos e a atualização dos sistemas de maneira simples e eficaz.

GESTÃO, AUDITORIA E CONFORMIDADE: A solução deverá possibilitar: registro e análise de logs de eventos e acessos com geração de relatórios gerenciais e técnicos para fins de auditoria e conformidade com a Resolução CNJ nº 396/2021 (PGSI-JUD); capacidade de integração com ferramentas de SIEM existentes ou futuras; e funcionalidade de alertas em tempo real e *dashboards* personalizáveis para visualização de riscos e ocorrências.

SEGURANÇA DA INFORMAÇÃO: A solução deverá possibilitar: Implementação de políticas de segurança em múltiplas camadas, com prevenção de intrusão (IPS), filtragem de conteúdo, controle de aplicações e detecção de anomalias; suporte a autenticação multifator (MFA), integrada ao diretório corporativo (LDAP/Active Directory), com tokens físicos e virtuais; capacidade de realizar segmentação de rede (VLAN, Zonas de Segurança) e aplicação de políticas distintas por tipo de usuário, serviço ou dispositivo; e suporte a SD-WAN segura com balanceamento inteligente de links e definição de rotas por aplicação.

CAPACITAÇÃO DA EQUIPE TÉCNICA: A equipe técnica do TJAP possui formação e capacitação tendo em vista a infraestrutura atual, o que permite o uso imediato e eficiente da solução, evitando necessidade de requalificação ou reengenharia. Sendo assim, a solução a ser adquirida deverá ser da marca Fortinet.

SUPORTE TÉCNICO E GARANTIA: A garantia das soluções deverá ser fornecida para um período de 60 (sessenta) meses, incluindo atualizações, suporte e renovações automáticas, suporte “on-site” e "online", na modalidade 24x7 e possibilidade de substituição de *hardware* em regime N3BD (*Next Three Business Day*) e manutenção corretiva.

RESPONSABILIDADE AMBIENTAL: Além disso, a responsabilidade ambiental deve ser considerada, privilegiando soluções que apresentem alta eficiência energética e práticas de operação ambientalmente responsáveis, reduzindo o impacto ecológico da infraestrutura de TI.

INDEPENDÊNCIA CONTRATUAL: A independência contratual assegura que a Instituição não fique excessivamente vinculada a um único fornecedor ou tecnologia, permitindo liberdade para realizar ajustes, substituições ou expansões sem restrições impostas por cláusulas dubiamente exclusivas. Esse fator reduz riscos de dependência, facilita negociações mais vantajosas e garante maior poder de escolha em futuras aquisições, manutenções ou atualizações, promovendo sustentabilidade e autonomia na gestão da infraestrutura.

ESTADO DE EQUIPAMENTO “NOVO”: A aquisição de equipamentos novos garante maior vida útil, menor probabilidade de falhas e melhor desempenho operacional. Além disso, reduz a necessidade de manutenções corretivas frequentes, assegura compatibilidade com as tecnologias mais recentes e oferece cobertura integral de garantia do fabricante. Isso contribui para maior confiabilidade, previsibilidade de custos e melhor aproveitamento dos investimentos em infraestrutura.

1.1.4. REQUISITOS SOCIOAMBIENTAIS

O licitante deverá atender no que couber, os critérios de sustentabilidade ambiental devendo utilizar, quando disponíveis no mercado, materiais que sejam reciclados, reutilizados e biodegradáveis, bem como priorizar o emprego de mão-de-obra, materiais, tecnologias e matérias-primas de origem local para execução e operação do objeto, bem como respeitar as Normas Brasileiras (NBR) publicadas pela Associação Brasileira de Normas Técnicas (ABNT) sobre resíduos sólidos.

Deverá a contratada adotar boas práticas de sustentabilidade, baseadas na otimização e economia de recursos e na redução da poluição ambiental, quando da execução da confecção dos equipamentos contratados, tais como uso racional de água, economia de energia elétrica, economia de materiais, separação de resíduos e materiais recicláveis.

Dessa forma, considerando a necessidade de implantação de práticas de sustentabilidade, deve-se contratar empresas que sejam comprometidas com a sustentabilidade.

Visando um maior desenvolvimento nacional sustentável, a presente aquisição observará os princípios da economicidade, eficácia, eficiência para melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, inclusive com respeito a impactos ambientais, de forma a utilizar-se da menor quantidade possível de recursos que causem impactos negativos para a sociedade e para o meio ambiente.

Dessa forma, considerando a necessidade de implantação de práticas de sustentabilidade, deve-se priorizar contratar empresa fornecedora que seja comprometida com a sustentabilidade.

Todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias), deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, em especial a responsabilidade compartilhada pelo ciclo de vida do produto. A empresa vencedora deverá aplicar o disposto nos Artigos de nºs 31 a 33 da Lei nº 12.305 de 02 de agosto de 2010, no que diz respeito à Logística Reversa.

1.2. ANÁLISE DE SOLUÇÕES POSSÍVEIS

1.2.1. IDENTIFICAÇÃO DAS SOLUÇÕES

Solução 1
Proposta de continuidade da padronização atual e expansão da infraestrutura tecnológica de segurança da informação do TJAP, com soluções Fortinet, por meio da aquisição de novos *firewalls*, soluções de gerenciamento e controle, acessórios necessários e serviços de sustentação e suporte.

Solução 2
Como alternativa, propõe-se a adoção de um modelo onde o fornecedor/empresa oferecerá toda a solução (equipamentos, *softwares* e serviços) em formato de comodato, bem como utilizando o modelo de *Software-as-a-Service* (SaaS) e Infraestructure-*as-a-Service* (IaaS).

1.2.2. ANÁLISE COMPARATIVA DE SOLUÇÕES

REQUISITO	SOLUÇÃO 1	SOLUÇÃO 2
PADRONIZAÇÃO E INTEROPERABILIDADE DA INFRAESTRUTURA	ATENDE	ATENDE
MARCA/FABRICANTE	ATENDE	ATENDE
SOLUÇÃO INTEGRADA	ATENDE	ATENDE
FERRAMENTA DE GESTÃO CENTRALIZADA	ATENDE	ATENDE
DESEMPENHO, DISPONIBILIDADE E CAPACIDADE	ATENDE	NÃO ATENDE
ESCALABILIDADE	ATENDE	NÃO ATENDE

GESTÃO, AUDITORIA E CONFORMIDADE	ATENDE	ATENDE
SEGURANÇA DA INFORMAÇÃO	ATENDE	ATENDE
CAPACITAÇÃO DA EQUIPE TÉCNICA	ATENDE	ATENDE
SUPORTE TÉCNICO E GARANTIA	ATENDE	ATENDE
RESPONSABILIDADE AMBIENTAL	ATENDE	ATENDE
INDEPENDÊNCIA CONTRATUAL	ATENDE	NÃO ATENDE
ESTADO DE EQUIPAMENTO "NOVO"	ATENDE	Possui as duas possibilidades: "novo" / "usado".

1.2.3. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Durante a fase de análise de alternativas, foram avaliadas diferentes soluções que, embora apresentassem aderência parcial aos requisitos levantados, mostraram inviabilidades técnicas, operacionais, contratuais ou financeiras que impedem sua adoção pelo TJAP. O registro a seguir evidencia tais limitações:

Solução 2 - Alternativa em formato de comodato, bem como utilizando o modelo de *Software-as-a-Service* (SaaS) e *Infraestructure-as-a-Service* (IaaS):

Desempenho, disponibilidade e capacidade: Considerando que haverá um contrato com o fornecedor a ser cumprido, bem como um Acordo de Nível de Serviço, caso haja necessidade de elevação de desempenho, disponibilidade e capacidade, o contrato pode acabar limitando tal elevação.

Escalabilidade: Considerando que haverá um contrato com o fornecedor a ser cumprido, bem como um Acordo de Nível de Serviço, caso haja necessidade de elevação de escala, o contrato pode acabar limitando tal elevação.

Independência contratual: implica forte dependência de um único fornecedor (*vendor lock-in*), limitando a capacidade do TJAP de migrar ou ajustar contratos em situações emergenciais.

Estado do equipamento: possibilidade de utilização de equipamentos usados ou compartilhados, comprometendo a padronização e a confiabilidade dos ativos tecnológicos.

Assim, embora essa solução atenda a alguns requisitos técnicos, os riscos identificados em aspectos de desempenho, de capacidade, de escalabilidade e contratuais tornam sua adoção inviável para o TJAP, tendo em vista o atual momento.

1.2.4. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

1.2.4.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Considerando que a solução 2 apresenta-se inviável pelo exposto no item 1.2.3., não foi realizada análise comparativa dos custos TCO.

1.3. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Detalhado no anexo: "*ANEXO A – ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO OBJETO*".

1.3.1. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

a) Fortalecimento da segurança da informação no âmbito do TJAP, por meio da elevação do nível de proteção da infraestrutura tecnológica contra ameaças cibernéticas, vazamentos de dados, acessos indevidos e indisponibilidade de sistemas críticos.
b) Continuidade e integridade operacional, por meio da manutenção da padronização tecnológica com a plataforma *Fortinet* já implantada, evitando dificuldades operacionais e assegurando a interoperabilidade com ativos existentes.
c) Gestão centralizada e eficiente da segurança da informação, por meio da ampliação da capacidade de gerenciamento, monitoramento e resposta a incidentes de segurança de forma unificada, com uso de ferramentas nativas como *FortiManager* e *FortiAnalyzer*.
d) Eficiência administrativa e economia de recursos, por meio da redução de custos operacionais com capacitação, integração e suporte, por meio do aproveitamento da expertise já consolidada na equipe técnica interna do TJAP.
e) Conformidade com normas e diretrizes institucionais, por meio do atendimento às exigências da Política de Governança da Segurança da Informação (Resolução CNJ n.º 396/2021), da ENTIC-JUD (Resolução CNJ n.º 370/2021) e da Estratégia Nacional do Poder Judiciário (Resolução CNJ n.º 325/2020).
f) Melhoria da qualidade dos serviços ao cidadão, por meio da geração de impactos positivos na prestação jurisdicional, ao garantir maior confiabilidade, estabilidade e proteção dos sistemas judiciais e administrativos.

1.3.2. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

Não há contratações correlatas ou interdependentes.

1.3.3. PROVIDÊNCIAS A SEREM TOMADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Não há providências a serem adotadas.

1.3.4. DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO (ARP PARA ADESÃO)

Durante o processo de Estudo Técnico Preliminar não foi encontrada Ata de Registro de Preços (ARP) para adesão que atenda às necessidades identificadas pela SETIC/TJAP.

1.3.5. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

A Solução 1 (proposta de continuidade da padronização atual e expansão da infraestrutura tecnológica de segurança da informação do TJAP, com soluções Fortinet, por meio da aquisição de novos firewalls, soluções de gerenciamento e controle, acessórios necessários e serviços de sustentação e suporte) apresenta-se mais viável do que um modelo puramente baseado em comodato, bem como utilizando o modelo de Software-as-a-Service (SaaS) e Infraestructure-as-a-Service (IaaS).

Esta aquisição reduzirá custos operacionais, de manutenção e de instalação, otimizando investimentos prévios em infraestrutura e capacitação de pessoal. Além disso, a adoção de plataformas modernas fortalecerá os protocolos de proteção de dados, assegurando a integridade, confidencialidade e disponibilidade das informações. A eficiência energética dos novos equipamentos contribuirá para a redução do consumo de energia elétrica, alinhando-se às práticas sustentáveis da instituição.

Desse modo, a escolha pela Solução 1, assegura uniformidade de processos, padronização dos equipamentos/softwares, continuidade dos serviços sem interrupções, facilidade de manutenção, adequação à realidade orçamentária e independência contratual. A Solução 1 proposta é plenamente compatível com o parque tecnológico atualmente implantado no TJAP, evitando retrabalho, riscos de incompatibilidade e custos com reengenharia de sistemas.

Por fim, ressalta-se que a aquisição objeto deste Documento está em conformidade com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 2021-2026, especialmente nos objetivos de aumentar a satisfação dos usuários, promover a transformação digital, melhorar os serviços de infraestrutura, aprimorar a segurança da informação e fomentar a inovação colaborativa.

Conclui-se, portanto, que a aquisição de novos firewalls, soluções de gerenciamento e controle, acessórios necessários e serviços de sustentação e suporte (Fortinet) é viável e recomendável, pois atenderá às necessidades atuais da Instituição, promoverá melhorias significativas em áreas estratégicas e está alinhada com as diretrizes nacionais de TIC, contribuindo para a excelência na prestação dos serviços e para o fortalecimento institucional.

1.4. PESQUISA DE PREÇOS DE MERCADO

A Pesquisa de Preços e a Metodologia utilizada para seu desenvolvimento, estão detalhadas nos anexos: "*ANEXO - MAPA DE PREÇOS*" e "*ANEXO - JUSTIFICATIVA DE METODOLOGIA UTILIZADA NA COTAÇÃO DE PREÇOS*".

1.5. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

GRUPO ÚNICO						
ITEM	**DESCRIÇÃO**	**QTD.**	**UNIDADE DE MEDIDA**	**CATEGORIA DE PAGAMENTO**	**PREÇO UNITÁRIO ESTIMADO (R$)**	**PREÇO TOTAL ESTIMADO (R$)**
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	Unidade	PAGAMENTO ÚNICO	981.874,70	1.963.749,40
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	4	Unidade	PAGAMENTO ÚNICO	252.793,11	1.011.172,44
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	4	Unidade	PAGAMENTO ÚNICO	109.501,73	438.006,92
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	6	Unidade	PAGAMENTO ÚNICO	24.216,07	145.296,42

5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	20	Unidade	PAGAMENTO ÚNICO	19.548,56	390.971,20
6	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 06	4	Unidade	PAGAMENTO ÚNICO	105.206,58	420.826,32
7	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) COMO SERVIÇO - TIPO 02	240	Firewall por mês	PAGAMENTO MENSAL	5.927,44	1.422.585,60
8	LICENCIAMENTO UTP PARA NGFW - TIPO 03	2	Unidade	PAGAMENTO ÚNICO	71.830,97	143.661,94
9	LICENCIAMENTO UTP PARA NGFW - TIPO 04	4	Unidade	PAGAMENTO ÚNICO	17.584,07	70.336,28
10	LICENCIAMENTO UTP PARA NGFW - TIPO 05	22	Unidade	PAGAMENTO ÚNICO	13.385,09	294.471,98
11	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA - TIPO 01	10	Unidade	PAGAMENTO ÚNICO	50.918,74	509.187,40
12	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA COMO SERVIÇO - TIPO 01	600	Unidade	PAGAMENTO MENSAL	1.018,95	611.370,00
13	SOLUÇÃO DE GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO	6	Unidade	PAGAMENTO ÚNICO	14.213,89	85.283,34
14	SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC) PARA GRUPO DE 100 ENDPOINTS	50	Unidade	PAGAMENTO ÚNICO	26.917,83	1.345.891,50
15	SOLUÇÃO DE ACESSO À REDE DE CONFIANÇA ZERO (ZTNA)	20	Unidade	PAGAMENTO ÚNICO	31.347,41	626.948,20
16	SOLUÇÃO DE SERVIÇO DE ACESSO SEGURO DE BORDA (SASE)	1000	Unidade	PAGAMENTO ÚNICO	3.248,68	3.248.680,00
17	SOLUÇÃO DE TOKEN PARA MFA PARA GRUPO DE 50 USUÁRIOS	20	Unidade	PAGAMENTO ÚNICO	34.086,84	681.736,80

18	TRANSCEIVER SFP 1000Base-SX	40	Unidade	PAGAMENTO ÚNICO	634,90	25.396,00
19	TRANSCEIVER SFP+ 10GBase-SR	20	Unidade	PAGAMENTO ÚNICO	814,30	16.286,00
20	TRANSCEIVER SFP+ 10GBase-LR	10	Unidade	PAGAMENTO ÚNICO	1.400,76	14.007,60
21	TRANSCEIVER QSFP+ 40GBase-SR4	10	Unidade	PAGAMENTO ÚNICO	4.756,23	47.562,30
22	BANCO DE HORAS TÉCNICAS	1000	Horas Técnicas	PAGAMENTO MENSAL	712,70	712.700,00
23	UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON	500	UST	PAGAMENTO MENSAL	960,26	480.130,00
PREÇO GLOBAL ESTIMADO (R$)						**14.706.257,64**

A justificativa para os quantitativos definidos na tabela acima é apresentada no anexo: "*ANEXO - JUSTIFICATIVA PARA OS QUANTITATIVOS DEFINIDOS*".

1.6. PREVISÃO DE CONTRATAÇÃO NO PLANO ANUAL DE CONTRATAÇÕES DO TJAP

Há previsão no Plano Anual de Contratações 2026, por meio do DFD: 269/2025.

2. GESTÃO DO CONTRATO

2.1. CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE

A aceitação do objeto desta eventual aquisição estará condicionada aos critérios estabelecidos abaixo:

ATESTADO DE CAPACIDADE TÉCNICA

● Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de solução de "*FIREWALLS*" em quantidade não inferior à 50% do solicitado neste edital, sendo permitido soma de atestados para atender ao solicitado. Deverá constar, pelo menos os seguintes itens:

- ITEM 1 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01 ou solução equivalente;
- ITEM 2 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02 ou solução equivalente.

● Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de "*BANCO DE HORAS TÉCNICAS*" relacionado ao objeto, em quantidade não inferior à 50% do solicitado neste edital, sendo permitido soma de atestados para atender ao solicitado.

QUALIFICAÇÃO

● As especificações técnicas completas dos equipamentos e softwares ofertados neste certame, deverão ser confirmadas por meio de uma "matriz comprovatória" ou "ponto a ponto" anexada à proposta comercial, incluindo todos os PART NUMBERS relacionados, bem como a inserção de datasheets/folhetos técnicos oficiais do fabricante, sob pena de desclassificação.

●Todos os equipamentos, módulos, fontes, transceivers, soluções de gerenciamento e plataformas ofertados neste certame, devem ser do mesmo fabricante.

●O licitante deverá entregar declaração oficial de que os equipamentos, soluções de gerenciamento e plataformas estão em linha de produção e sem previsão de descontinuidade pelo fabricante, esta declaração deverá ser destinada ao Tribunal de Justiça do Estado do Amapá para este certame específico, com data atual.

●Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta.

●Sob risco de desclassificação, visando garantir e comprovar que a solução ofertada atenda as expectativas do CONTRATANTE, o licitante deverá apresentar com sua proposta uma planilha comprovando atender todas as linhas e exigências deste Documento. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.). Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem quaisquer ônus adicionais e independentemente da existência de contrato de manutenção.

●Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta.

LICENCIAMENTO E GARANTIA

● A licitante vencedora do certame deverá atender às definições relacionadas à licenciamento e garantia descritas para cada item no "*ANEXO A – ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO OBJETO*".

2.2. METODOLOGIA/FORMAS DE AVALIAÇÃO DA QUALIDADE E ADEQUAÇÃO DA SOLUÇÃO ÀS ESPECIFICAÇÕES FUNCIONAIS E TECNOLÓGICAS

Detalhado no anexo: "*ANEXO A – ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO OBJETO*".

2.3. PROCEDIMENTOS PARA EMISSÃO DE NOTA FISCAL

Para os itens 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, e 21:

O pagamento será efetuado por meio de ordem bancária, mediante depósito na conta corrente da CONTRATADA, no prazo de até 30 (trinta) dias consecutivos após o recebimento definitivo, acompanhado da respectiva Nota Fiscal/Fatura, emitida em, no mínimo, 02 (duas) vias, de acordo com a Nota de Empenho, a qual será conferida e atestada pelo Fiscal do Contrato ou servidor responsável pelo recebimento.

Para os itens 7, 12, 22 e 23, deverá ser seguido o cronograma para o pagamento mensal abaixo:
a) Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;
b) Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;
c) Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;
d) O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

2.4. EQUIPE DE GESTÃO DA CONTRATAÇÃO

FISCAL	NOME	MATRÍCULA	E-MAIL	UNIDADE
FISCAL TÉCNICO	Rayllan Leitão dos Santos	45701	rayllan.santos@tjap.jus.br	SETIC
FISCAL TÉCNICO SUBSTITUTO	Denis Santos da Cruz	45699	denis.cruz@tjap.jus.br	SETIC

3. PLANO DE SUSTENTAÇÃO, ESTRATÉGIA PARA CONTRATAÇÃO E CONTINUIDADE CONTRATUAL

3.1. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

3.1.1. RECURSOS MATERIAIS

Para a implementação e sustentação da solução, serão necessários os seguintes recursos materiais:

a) Ambiente com infraestrutura de tecnologia da informação, de segurança e de elétrica adequado.

3.1.1.1. DISPONIBILIDADE

A disponibilidade destes recursos materiais deve ser assegurada desde o início do projeto, considerando prazos de entrega e implementação que não impactem negativamente as operações correntes do TJAP. A contratada será responsável por garantir a entrega e a configuração dos recursos dentro dos prazos acordados, com planos de contingência para eventuais atrasos ou problemas.

3.1.1.2. QUANTIDADES / COMPETÊNCIAS

As quantidades e competências devem estar alinhadas aos quantitativos de Bens/Serviços previstos no “ITEM 1.5”.

3.1.2. RECURSOS HUMANOS

Em relação aos recursos humanos para sustentação do contrato, têm-se:

a) Secretaria de Estrutura de Tecnologia da Informação e Comunicação (SETIC);
b) Equipe da Coordenadoria de Segurança da Informação e Data Centers (CSDC);
c) Equipe da Coordenadoria de Gestão de Tecnologia da Informação (CGTI);
d) Equipe da Secretaria de Contratações e Convênios (SCC).

3.1.2.1. DISPONIBILIDADE

Há pessoal para desenvolvimento das atividades de planejamento e fiscalização da contratação.

3.1.2.2. QUANTIDADES / COMPETÊNCIAS

Há pessoal para desenvolvimento das atividades de planejamento e fiscalização da contratação.

3.2. ESTRATÉGIA PARA CONTRATAÇÃO

3.2.1. PARCELAMENTO DO OBJETO

A contratação deverá ser realizada em grupo único. Sendo assim, justifica-se o não parcelamento do objeto pelos seguintes motivos:
a) Coerência Técnica e Continuidade do Suporte: A unificação dos serviços sob um único contrato assegura a coerência técnica em toda a solução, garantindo que todos os processos, desde a ativação até a manutenção e o monitoramento, sejam realizados de forma integrada e padronizada. Além disso, a continuidade e uniformidade do suporte técnico é garantida por um único fornecedor, o que simplifica a responsabilização em caso de falhas.
b) Simplicidade e Eficiência Operacional: A centralização das aquisições em um único contrato não apenas simplifica a gestão e a administração logística e de manutenção, mas também permite a utilização de plataformas de gerenciamento centralizado, facilitando o monitoramento e o controle das operações de rede em tempo real e otimizando a atuação de uma equipe técnica reduzida.
c) Segurança: A adjudicação a um único fornecedor minimiza vulnerabilidades e reforça a proteção dos dados e da infraestrutura, garantindo abordagem uniforme para a segurança da informação.
Esses fatores justificam a escolha por grupo único e não parcelado, promovendo soluções mais integradas, seguras, eficientes e economicamente vantajosa para o projeto.

3.2.2. ADJUDICAÇÃO DO OBJETO

O objeto será adjudicado a um único fornecedor e como critério o de MENOR PREÇO.

3.2.3. MODALIDADE E TIPO DE LICITAÇÃO

A contratação dar-se-á por meio de procedimento licitatório através do Sistema de Registro de Preços (SRP), na modalidade PREGÃO, na forma ELETRÔNICA, em GRUPO ÚNICO, tendo como tipo MENOR PREÇO, em conformidade com a Resolução n.º 1594/2023-TJAP e subsidiariamente, no que couber pela Lei Federal n.º 14.133/2021 de acordo com a disponibilidade orçamentária e a necessidade da Administração.
Foi selecionado o Sistema de Registro de Preços com base no Art. 3º, incisos I e IV, da Resolução n.º 1594/2023-TJAP. Ou seja, poderá haver necessidade de contratações frequentes.

3.2.4. CLASSIFICAÇÃO, INDICAÇÃO E PREVISÃO ORÇAMENTÁRIA

A despesa será atendida com recursos do Orçamento do TJAP, prevista para o exercício (LOA/2026). Classifica-se, preliminarmente, no elemento 44.90.52 – Equipamentos e Material Permanente de TIC (e, se aplicável, 33.90.39 – Serviços de Terceiros – PJ). A dotação específica será indicada no consumo da ARP, conforme disponibilidade da LOA/2026.

3.2.5. VIGÊNCIA DO CONTRATO

Para todos os itens do objeto o contrato a ser firmado com a CONTRATADA terá vigência de 12 (doze) meses, a contar da data de assinatura do contrato.

3.2.6. NATUREZA DO OBJETO

Natureza do objeto: EQUIPAMENTO/PLATAFORMA (SISTEMA)/SERVIÇO CONTINUADO.

Fornecimento de bens comuns de TIC, compreendendo a aquisição de equipamentos de segurança da informação (*firewalls*), o licenciamento de plataformas de gerenciamento e controle de acesso incluindo suporte e garantia. E ainda, contratação de serviços de sustentação e suporte (banco de horas técnicas e unidades de serviços técnicos (USTs)), que se enquadram em serviços de natureza continuada.

Em resumo:

- Itens 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, e 21: Equipamentos e *softwares*;
- Itens 7, 12, 22 e 23: Serviços continuados.

Subcontratação do objeto: Durante o planejamento da contratação, foi avaliada a possibilidade de subcontratação parcial do objeto, considerando práticas usuais adotadas no mercado e o interesse público. No entanto, não foi identificada vantagem técnica e/ou economicamente viável para à Administração, do objeto ser subcontratado considerando os itens do objeto.

3.2.7. GARANTIA CONTRATUAL

Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei n.º 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

Justificativa: Considerando o tipo do objeto, justifica-se a solicitação de garantia para a contratação. Isso serve para garantir o fiel cumprimento das obrigações assumidas pela contratada.

3.3. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

3.3.1. AÇÕES DE CONTINUIDADE, SEUS RESPECTIVOS RESPONSÁVEIS E PRAZOS

O contrato administrativo é a base para o funcionamento da máquina pública. A legislação norteadora dos contratos administrativos por entes públicos é a Lei n.º 14.133/2021.

Sendo assim, no caso de uma eventual interrupção contratual, que impeça o fornecimento dos serviços da CONTRATADA, é possível utilizar os dispositivos legais contidos nessa legislação, como por exemplo, rescisão contratual e contratação emergencial, bem como outros dispositivos previstos, a fim de restabelecimento dos serviços.

Com o objetivo de assegurar a continuidade dos serviços de natureza continuada apresentados neste documento, evitando interrupção de serviços essenciais, serão adotadas as seguintes ações preventivas e de planejamento:

Ação	Unidade Responsável	Prazo Estimado
Avaliar o desempenho técnico e operacional do contrato vigente, considerando indicadores de atendimento e disponibilidade.	SETIC / CSDC	D-180 dias antes do encerramento
Definir, com base na avaliação, a necessidade de nova contratação, prorrogação ou substituição tecnológica.	CGTI / SGLC	D-120 dias
Iniciar a elaboração ou atualização do Estudo Técnico Preliminar (ETP) e do Termo de Referência.	CGTI / SETIC	D-90 dias
Encaminhar o processo licitatório completo (ETP, TR e minuta de edital) para tramitação interna e análise jurídica, garantindo tempo hábil à contratação subsequente.	SGLC / CGTI	D-60 dias
Iniciar ações de transição contratual.	SETIC / SGLC	D-30 dias

3.4. ESTRATÉGIA DE TRANSIÇÃO CONTRATUAL

3.4.1. AÇÕES DE TRANSIÇÃO CONTRATUAL, SEUS RESPECTIVOS RESPONSÁVEIS E PRAZOS

O contrato administrativo é a base para o funcionamento da máquina pública. A legislação norteadora dos contratos administrativos por entes públicos é a Lei n.º 14.133/2021.

Sendo assim, no caso de uma eventual interrupção contratual, que impeça o fornecimento dos serviços da CONTRATADA, é possível utilizar os dispositivos legais contidos nessa legislação, como por exemplo, rescisão contratual e contratação emergencial, bem como outros dispositivos previstos, a fim de restabelecimento dos serviços.

A transição contratual refere-se ao encerramento controlado da contratação, a ser executada nos meses finais de vigência, visando à continuidade dos serviços e à rastreabilidade das informações técnicas.

Ações previstas:
• Consolidação dos relatórios de suporte e manutenção executados ao longo do contrato, incluindo histórico de chamados, peças substituídas, prazos de atendimento e confirmações de encerramento emitidas;
• Validação técnica do estado dos equipamentos, assegurando ausência de pendências de garantia ou suporte;
• Atualização do inventário patrimonial e técnico nos sistemas internos do TJAP;
• Reunião de encerramento técnico entre a Contratada e a SETIC, para revisão dos serviços, identificação de lições aprendidas e recomendações para contratações futuras;
• Elaboração e assinatura do termo de encerramento contratual, com atesto final da execução.

Ação	Unidade Responsável	Prazo Estimado
Consolidação de relatórios e históricos de suporte.	Contratada / SGLC	D-30 dias antes do encerramento
Validação técnica do estado dos equipamentos.	SETIC / CSDC	D-20 dias
Atualização do inventário e registros.	CSDC	D-15 dias
Reunião de encerramento técnico e elaboração de termo final.	SETIC / CGTI / Contratada	D-10 dias
Arquivamento do termo e encerramento processual.	SGLC / CGTI	D-5 dias

3.5. ESTRATÉGIA DE INDEPENDÊNCIA

3.5.1. TRANSFERÊNCIA DE CONHECIMENTO

Durante a execução do contrato, a contratada deverá assegurar transferência contínua de conhecimento técnico e operacional à equipe da SETIC, de modo a preservar a autonomia do Tribunal na gestão dos equipamentos e *softwares*, e na comunicação com o suporte do fabricante.
As ações de transferência de conhecimento incluirão:
• Disponibilização de relatórios técnicos e atualizações realizadas (eventual utilização de garantia de equipamentos e *softwares*);
• Registro de lições aprendidas em cada ocorrência relevante (eventual utilização de garantia de equipamentos e *softwares*);
• Reunião técnica semestral entre contratada e SETIC para alinhamento sobre padrões de atendimento e eventuais recomendações de melhoria (aplicação nos serviços de natureza continuada).

3.5.2. DIREITOS DE PROPRIEDADE INTELECTUAL

A presente contratação não envolve o desenvolvimento de softwares, códigos-fonte, metodologias ou quaisquer ativos passíveis de geração de propriedade intelectual pelo fornecedor.

Todos os direitos de propriedade intelectual sobre os equipamentos e softwares permanecem sob titularidade do fabricante, cabendo ao TJAP apenas o direito de uso.

Assim, não há transferência ou cessão de direitos autorais ou de propriedade intelectual no âmbito desta contratação.

4. ANÁLISE DE RISCOS

A análise de riscos contém a descrição, a análise e o tratamento dos riscos e ameaças que possam vir a comprometer o sucesso de todo o Ciclo de Vida da Contratação. Esse, por sua vez, é conjunto de fases e etapas necessárias para se adquirir um bem e/ou contratar um serviço, contemplando o planejamento, a execução, a avaliação e o encerramento do contrato. Dessa forma, para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos potenciais, possíveis ações de mitigação e contingências, bem como a identificação de responsáveis por cada ação.

A Análise de Riscos está detalhada no anexo: "*ANEXO - ANÁLISE DE RISCOS*".

5. APROVAÇÃO E ASSINATURA

INTEGRANTE DEMANDANTE	INTEGRANTE ADMNISTRATIVO	INTEGRANTE TÉCNICO	INTEGRANTE TÉCNICO
Nome: Genner de Lima Moreira Matrícula: 20099	Nome: Yan Fernando Maciel de França Matrícula: 44340	Nome: Rayllan Leitão dos Santos Matrícula: 45701	Nome: Cadu Calixto de Carvalho dos Santos Matrícula: 44331

ANEXO III - ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO OBJETO

QUALIFICAÇÃO TÉCNICA DO LICITANTE – HABILITAÇÃO

GRUPO ÚNICO

FIREWALLS

Apresentar Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de solução de "*FIREWALLS*" em quantidade não inferior à 50% do solicitado neste edital, sendo permitido soma de atestados para atender ao solicitado. Deverá constar, pelo menos os seguintes itens:

- ITEM 1 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01 ou solução equivalente;
- ITEM 2 - FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02 ou solução equivalente.

BANCO DE HORAS TÉCNICAS

Apresentar Atestado de Capacidade Técnica, fornecido por empresa pública ou privada, demostrando aptidão do LICITANTE para o fornecimento de "*BANCO DE HORAS TÉCNICAS*" relacionado ao objeto, em quantidade não inferior à 50% do solicitado neste edital, sendo permitido soma de atestados para atender ao solicitado.

QUALIFICAÇÃO

- As especificações técnicas completas dos equipamentos e softwares ofertados neste certame, deverão ser

confirmadas por meio de uma “matriz comprovatória” ou “ponto a ponto” anexada à proposta comercial, incluindo todos os PART NUMBERS relacionados, bem como a inserção de datasheets/folhetos técnicos oficiais do fabricante, sob pena de desclassificação.

- Todos os equipamentos, módulos, fontes, *transceivers*, soluções de gerenciamento e plataformas ofertados neste certame, devem ser do mesmo fabricante.
- O licitante deverá entregar declaração oficial de que os equipamentos, soluções de gerenciamento e plataformas estão em linha de produção e sem previsão de descontinuidade pelo fabricante, esta declaração deverá ser destinada ao Tribunal de Justiça do Estado do Amapá para este certame específico, com data atual.
- Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de “COPIAR” e “COLAR” o descritivo contido no edital não será caracterizado como descritivo da proposta.
- Sob risco de desclassificação, visando garantir e comprovar que a solução ofertada atenda as expectativas do CONTRATANTE, o licitante deverá apresentar com sua proposta uma planilha comprovando atender todas as linhas e exigências deste Documento. Todos os equipamentos devem ser fornecidos completos do ponto de vista da funcionalidade em rede e incluir todos os adicionais necessários (de qualquer espécie: licenças de software, cabos, manuais, etc.). Todos os equipamentos devem ser entregues com o firmware mais atual disponibilizado pelo fabricante e ser legalmente disponibilizado para a instalação pela CONTRATANTE, sem quaisquer ônus adicionais e independentemente da existência de contrato de manutenção.
- Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta.

REFERÊNCIA TECNOLÓGICA

- Os modelos indicados nas especificações técnicas são apresentados como referência tecnológica, em razão da padronização adotada pela Administração. Será admitido o fornecimento de outros modelos do mesmo fabricante, desde que comprovadamente equivalentes em termos técnicos, funcionais e operacionais e compatíveis com a infraestrutura existente, cuja equivalência será analisada e validada pela Secretaria de Tecnologia da Informação e Comunicação (SETIC).

CONTROLE DE QUALIDADE DOS SERVIÇOS

- Para os ITENS 22 - "BANCO DE HORAS TÉCNICAS" e 23 - "UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON" : Visando garantir a qualidade e boa execução dos serviços de implementação do projeto, a licitante deverá apresentar em sua proposta os PARTNUMBER dos serviços do fabricante do produto que sejam compatíveis aos descritos neste Documento ou apresentar comprovação de entrega de qualidade de serviço por meio de documentos da qualificação técnico operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.
- Os documentos e comprovações solicitadas, visando "CONTROLE DE QUALIDADE DOS SERVIÇOS", deverão ser fornecidas durante a execução contratual.

REQUISITOS DE ENTREGA DA SOLUÇÃO

- Todos os itens (equipamentos) deverão ser entregues nas dependências do CONTRATANTE, pela CONTRATADA.
- Endereço de entrega: “Prédio Anexo da Sede do TJAP (Anexo Desembargador Eduardo Contreras – SITE A) / Av. Raimundo Álvares da Costa, 400 - Central, Macapá - AP, 68900-074 / Horário de funcionamento: De segunda-feira a sexta-feira - 7h:30min às 14h:30min”.
- O prazo de entrega de todos os itens (equipamentos) será de 90 dias corridos, contados a partir da assinatura do Contrato.

REQUISITOS DE SUPORTE TÉCNICO PARA TODOS OS ITENS DESTE DOCUMENTO

- Cobertura 24x07 (24 horas por dia x 07 dias por semana).
- A CONTRATADA deve possuir suporte técnico remoto para a solução de problemas comuns de suporte.
- A CONTRATADA deve realizar atendimento *on-site* em até 05 (cinco) dias úteis, com tempo de atendimento contado a partir da abertura do chamado.
- O FABRICANTE deverá possuir Central de Atendimento online para abertura dos chamados de garantia, comprometendo-se a manter estes registros constando a descrição do problema.
- Todos os itens de *software* que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do FABRICANTE.
- O serviço de suporte deverá ser do FABRICANTE do equipamento ou por assistência técnica qualificada e indicada por este por meio de declaração.

GRUPO ÚNICO

CARACTERÍSTICAS COMUNS PARA *FIREWALLS* DE PRÓXIMA GERAÇÃO (ITENS 1 A 6)

A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em *appliance* com funcionalidades de *Next Generation Firewall* (NGFW), console de gerência e monitoração;

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *end-of-life* e *end-of-sale;*

Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos *appliances* desde que atendam a todos os requisitos desta especificação;

Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com as seguintes funcionalidades: *Firewall*, *Traffic Shapping* e QoS, Filtro de Conteúdo Web, Antivírus, *AntiSpam*, Detecção e Prevenção de Intrusos (IPS), VPN IPSec ou SSL, Controle de Aplicações e Virtualização.

FUNCIONALIDADES DE REDE E *FIREWALL*

O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

Os dispositivos de proteção de rede devem possuir suporte a Vlans;

Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, *Server* e *Relay*;

Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (*Network Address Translation*), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Deverá suportar sFlow ou Netflow;

Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

Deve suportar o protocolo padrão da indústria VXLAN;

Deve implementar o protocolo ECMP;

Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

Enviar log para sistemas de monitoração externos;

Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

Deve possui mecanismos de proteção anti-spoofing;

Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

Suportar OSPF graceful restart;

Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

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 Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

Deverá suportar controle por zonas de segurança;

Deverá suportar controles de políticas por porta e protocolo;

Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

Suporte a objetos e regras IPV6;

Suporte a objetos e regras multicast;

Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

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 rede Tor;

Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

Deve 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. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

Identificar o uso de táticas evasivas via comunicações criptografadas;

Atualizar a base de assinaturas de aplicações automaticamente;

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao

Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

Deve alertar o usuário quando uma aplicação for bloqueada;

Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para os mesmos;

Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.);

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

Deve permitir forçar o uso de portas específicas para determinadas aplicações.

FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

Deve 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;

Deve permitir o bloqueio de vulnerabilidades;

Deve permitir o bloqueio de exploits conhecidos;

Deve incluir proteção contra-ataques de negação de serviços;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.;

Detectar e bloquear a origem de portscans;

Bloquear ataques efetuados por worms conhecidos;

Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

Possuir assinaturas para bloqueio de ataques de buffer overflow;

Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

Identificar e bloquear comunicação com botnets;

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;

Os eventos devem identificar o país de onde partiu a ameaça;

Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

Deve permitir que na captura de pacotes por assinaturas de IPS 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.

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

Possuir pelo menos 70 (setenta) categorias de URLs;

Deve possuir a função de exclusão de URLs do bloqueio;

Permitir a customização de página de bloqueio;

Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado.

FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

Deve 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, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

Deve possuir integração com 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;

Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

Deve suportar o envio e recebimento de credenciais via RADIUS;

Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

FUNCIONALIDADE DE FILTRO DE DADOS

Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP);

Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

FUNCIONALIDADE DE GEOLOCALIZAÇÃO

Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

FUNCIONALIDADE DE VPN

Suportar VPN Site-to-Site e Client-To-Site;

Suportar IPSec VPN;

A VPN IPSEc deve suportar 3DES;

A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

Deve 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;

Atribuição de DNS nos clientes remotos de VPN;

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN IPSEC;

Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

Suportar leitura e verificação de CRL (Certificate Revocation List);

Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis IPSEC;

Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

Deverá manter uma conexão segura com o portal durante a sessão;

O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

Endereço de origem;

Endereço de destino;

Usuário e grupo;

Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

Por porta;

O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

O QoS deve possibilitar a definição de fila de prioridade;

Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

Suportar marcação de pacotes Diffserv, inclusive por aplicação;

Suportar modificação de valores DSCP para o Diffserv;

Suportar priorização de tráfego usando informação de ToS (Type of Service);

Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

Deve possibilitar a definição de bandas distintas para download e upload.

FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

A solução deve ser capaz de agregar vários links em uma interface virtual;

A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc.);

A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover);

A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente;

Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc.);

Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

A solução deve suportar nativamente conectores com clouds públicas;

Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

Deve implementar balanceamento de link por hash do IP de origem;

Deve implementar balanceamento de link por hash do IP de origem e destino;

Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

ITEM 1 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO *FIREWALL* DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01:

Deve suportar, no mínimo, 140 (cento e quarenta) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 15 (quinze) milhões de conexões simultâneas;

Deve suportar, no mínimo, 650.000 (seiscentos e cinquenta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 52 (cinquenta e dois) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.800 (mil e oitocentos) túneis de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 45.000 (quarenta e cinco mil) túneis de clientes VPN IPSEC simultâneos;

Deve suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput de IPS;

Deve suportar, no mínimo, 8 (oito) Gbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve possuir, pelo menos, 16 (dezesseis) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;

Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet e SFP de 1 Gigabit Ethernet;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;

Deve possuir unidade do tipo SSD com no mínimo 480 (quatrocentos e oitenta) GB para armazenamento de informações locais;

Deve possuir fonte de alimentação AC redundante;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 2 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02:

Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 10 (dez) milhões de conexões simultâneas;

Deve suportar, no mínimo, 400.000 (quatrocentas mil) novas conexões por segundo;

Deve suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput VPN IPSec;

Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSec Site-to-Site simultâneos;

Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes VPN IPSec simultâneos;

Deve suportar, no mínimo, 8 (oito) Gbps de throughput de IPS;

Deve suportar, no mínimo, 6 (seis) Gbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 5 (cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e antimalware;

Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;

Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores RJ45;

Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

Deve possuir, pelo menos, 1 (uma) interface RJ45 ou SFP/SFP+ dedicada para alta disponibilidade (HA);

Deve estar licenciado para gerenciar até 256 (duzentos e cinquenta e seis) pontos de acesso sem fio e 64 (sessenta e quatro) switches simultaneamente em um único appliance;

Deve possuir unidade do tipo SSD com no mínimo 480 (quatrocentos e oitenta) GB para armazenamento de informações locais;

Deve possuir fonte de alimentação AC redundante e hot swap;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (contextos) por appliance.

ITEM 3 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO *FIREWALL* DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03:

Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 1.5 Milhão (um milhão e quinhentas mil) conexões simultâneas;

Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo;

Deve Suportar, no mínimo, 10 (dez) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de VPN SSL;

Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;

Deve suportar, no mínimo, 02 (dois) Gbps de throughput de IPS;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 01 (um) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve possuir, pelo menos, 08 (oito) interfaces Gigabit Ethernet com conectores SFP;

Deve possuir, pelo menos, 02 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+;

Deve possuir unidade do tipo SSD com no mínimo 480 (quatrocentos e oitenta) GB para armazenamento de informações locais;

Deve estar licenciado para gerenciar até 30 (trinta) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;

Deve possuir fonte de alimentação AC redundante;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 4 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04:

Deve suportar, no mínimo, 05 (cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 700.000 (setecentos mil) conexões simultâneas;

Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;

Deve Suportar, no mínimo, 06 (seis) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 400 (quatrocentos) túneis de clientes VPN IPSEC simultâneos;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;

Deve suportar, no mínimo, 600 (seiscentos) Mbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 700 (setecentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve estar licenciado para gerenciar até 30 (trinta) pontos de acesso sem fio e 20 (vinte) switches simultaneamente em um único appliance;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 5 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO *FIREWALL* DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05:

Deve suportar, no mínimo, 05 (cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 700.000 (setecentos mil) conexões simultâneas;

Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;

Deve Suportar, no mínimo, 04 (quatro) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de clientes VPN IPSEC simultâneos;

Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;

Deve suportar, no mínimo, 400 (quatrocentos) Mbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 600 (seiscentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

Deve possuir, pelo menos, 5 (cinco) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve estar licenciado para gerenciar até 8 (oito) pontos de acesso sem fio e 8 (oito) switches simultaneamente em um único appliance;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 6 – CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO *FIREWALL* DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 06:

Deve suportar, no mínimo, 27 (vinte e sete) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 1,5 (um vírgula cinco) milhões de conexões simultâneas;

Deve suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo;

Deve Suportar, no mínimo, 24 (vinte e quatro) Gbps de throughput VPN IPSec;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de clientes VPN IPSEC simultâneos;

Deve suportar, no mínimo, 1,4 (um vírgula quatro) Gbps de throughput de VPN SSL;

Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;

Deve suportar, no mínimo, 4,4 (quatro vírgula quatro) Gbps de throughput de IPS;

Deve suportar, no mínimo, 700 (setecentos) Mbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 2,2 (dois vírgula dois) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

Deve possuir, pelo menos, 2 (duas) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet;

Deve possuir unidade do tipo SSD com no mínimo 120 (cento e vinte) GB para armazenamento de informações locais;

Deve estar licenciado para gerenciar até 40 (quarenta) pontos de acesso sem fio e 20 (vinte) switches simultaneamente em um único appliance;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 7 – *FIREWALL* DE PRÓXIMA GERAÇÃO (NGFW) COMO SERVIÇO - TIPO 02:

CARACTERÍSTICAS DO SERVIÇO

Contratação de serviço contínuo que compreende o fornecimento, implantação, licenciamento, atualização e manutenção integrada de solução de segurança de rede — incluindo os equipamentos necessários e suas respectivas licenças — prestado de forma "*as a Service"*. Todo o conjunto (hardware e licenciamento) será disponibilizado ao CONTRATANTE como serviço gerenciado, e não como bem isolado.

O serviço deverá ser prestado de forma ininterrupta pelo prazo de 12 (doze) meses. Durante todo esse período, o contratado deverá assegurar a plena operação do hardware e das licenças, bem como sua substituição preventiva ou corretiva, atualizações de software/firmware e suporte técnico especializado.

Apesar de tratar-se de prestação de serviço contínuo, o valor deverá ser apresentado na proposta como montante global correspondente aos 12 (doze) meses de execução. Ou seja, a proposta deve apresentar um valor único total para o período integral contratado.

Entretanto, para fins de faturamento, o pagamento será realizado mensalmente em parcelas correspondentes a 1/12 (um doze avos) do valor global contratado, garantindo a execução financeira conforme a prestação efetiva do serviço.

Quanto ao pagamento, deverá ser seguido o cronograma para o pagamento mensal abaixo:

a) Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;

b) Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;

c) Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;

d) O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

Durante todo o período de vigência, a solução contratada deverá possuir e manter atualizadas, no mínimo, as seguintes funcionalidades integradas: Firewall de Próxima Geração; Traffic Shaping e QoS (Quality of Service); Filtro de Conteúdo Web; Antivírus; Antispam; Sistema de Detecção e Prevenção de Intrusos (IPS); VPN IPSec ou SSL; Controle de Aplicações; Recursos de Virtualização.

Em caso de falha de hardware que comprometa parcial ou totalmente a operação do serviço de firewall, a contratada deverá realizar a **substituição do equipamento ou dos componentes afetados** em até **03 (três) dias úteis (*Next 3 Business Days* - N3BD)**, contados a partir da **abertura oficial do chamado técnico** pela equipe do TJAP.

A substituição deverá ser realizada sem ônus adicional para a Administração e garantir a continuidade do serviço com as mesmas características técnicas e funcionais previstas neste Termo.

Caso a contratada não disponha de unidade de backup idêntica, será admitido o uso de modelo equivalente ou superior, desde que compatível com o ambiente Fortinet em operação.

CARACTERÍSTICAS DO *FIREWALL* "*AS A SERVICE*"

Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

Deve suportar, no mínimo, 10 (dez) milhões de conexões simultâneas;

Deve suportar, no mínimo, 400.000 (quatrocentas mil) novas conexões por segundo;

Deve suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput VPN IPSec;

Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSec Site-to-Site simultâneos;

Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes VPN IPSec simultâneos;

Deve suportar, no mínimo, 8 (oito) Gbps de throughput de IPS;

Deve suportar, no mínimo, 6 (seis) Gbps de throughput de Inspeção SSL;

Deve suportar, no mínimo, 5 (cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e antimalware;

Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;

Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores RJ45;

Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet;

Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

Deve possuir, pelo menos, 1 (uma) interface RJ45 ou SFP/SFP+ dedicada para alta disponibilidade (HA);

Deve estar licenciado para gerenciar até 256 (duzentos e cinquenta e seis) pontos de acesso sem fio e 64 (sessenta e quatro) switches simultaneamente em um único appliance;

Deve possuir unidade do tipo SSD com no mínimo 480 (quatrocentos e oitenta) GB para armazenamento de informações locais;

Deve possuir fonte de alimentação AC redundante e hot swap;

Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (contextos) por appliance.

ITEM 8 – LICENCIAMENTO UTP PARA NGFW - TIPO 03:

Contratação de licenciamento integrado para solução de Firewall de Próxima Geração para o Fortinet FG-101F, com vigência de 60 (sessenta) meses contínuos, garantindo acesso pleno a todas as funcionalidades avançadas de segurança cibernética e suporte premium da fabricante.

O licenciamento deverá contemplar o pacote Unified Threat Protection (UTP), compreendendo obrigatoriamente:

Intrusion Prevention System (IPS) – Sistema de detecção e prevenção de intrusões em rede, baseado em assinaturas e análises comportamentais, para bloquear ataques conhecidos e zero-day;

Advanced Malware Protection (AMP) – Proteção contra malware avançado, inclusive ransomware, spyware e ameaças persistentes avançadas (APT);

Application Control – Controle de aplicações em nível granular, permitindo políticas por aplicação, categoria ou assinatura;

URL Filtering – Filtragem de URLs baseada em categorias, reputação e listas dinâmicas para bloqueio de sites maliciosos ou não autorizados;

DNS Filtering – Filtragem DNS para bloquear domínios perigosos e prevenir ataques baseados em manipulação de DNS;

Video Filtering – Controle sobre streaming e vídeos em plataformas específicas para adequação ao uso corporativo e à largura de banda;

Antispam Service – Serviço antispam integrado, mitigando phishing e spam antes de chegar à rede interna;

FortiCare Premium – Suporte técnico especializado 24x7, acesso a firmware, atualizações, patches e atendimento prioritário pela Fortinet;

O licenciamento deve ser entregue de forma integrada com o equipamento ou serviço (hardware + licença) para garantir conformidade do SLA e evitar descontinuidade de proteção.

ITEM 9 – LICENCIAMENTO UTP PARA NGFW - TIPO 04:

Contratação de licenciamento integrado para solução de Firewall de Próxima Geração para o Fortinet FG-101F, com vigência de 60 (sessenta) meses contínuos, garantindo acesso pleno a todas as funcionalidades avançadas de segurança cibernética e suporte premium da fabricante.

O licenciamento deverá contemplar o pacote Unified Threat Protection (UTP), compreendendo obrigatoriamente:

Intrusion Prevention System (IPS) – Sistema de detecção e prevenção de intrusões em rede, baseado em assinaturas e análises comportamentais, para bloquear ataques conhecidos e zero-day;

Advanced Malware Protection (AMP) – Proteção contra malware avançado, inclusive ransomware, spyware e ameaças persistentes avançadas (APT);

Application Control – Controle de aplicações em nível granular, permitindo políticas por aplicação, categoria ou assinatura;

URL Filtering – Filtragem de URLs baseada em categorias, reputação e listas dinâmicas para bloqueio de sites maliciosos ou não autorizados;

DNS Filtering – Filtragem DNS para bloquear domínios perigosos e prevenir ataques baseados em manipulação de DNS;

Video Filtering – Controle sobre streaming e vídeos em plataformas específicas para adequação ao uso corporativo e à largura de banda;

Antispam Service – Serviço antispam integrado, mitigando phishing e spam antes de chegar à rede interna;

FortiCare Premium – Suporte técnico especializado 24x7, acesso a firmware, atualizações, patches e atendimento prioritário pela Fortinet;

O licenciamento deve ser entregue de forma integrada com o equipamento ou serviço (hardware + licença) para garantir conformidade do SLA e evitar descontinuidade de proteção.

ITEM 10 – LICENCIAMENTO UTP PARA NGFW - TIPO 05:

Contratação de licenciamento integrado para solução de Firewall de Próxima Geração para o Fortinet FG-40F, com vigência de 60 (sessenta) meses contínuos, garantindo acesso pleno a todas as funcionalidades avançadas de segurança cibernética e suporte premium da fabricante.

O licenciamento deverá contemplar o pacote Unified Threat Protection (UTP), compreendendo obrigatoriamente:

Intrusion Prevention System (IPS) – Sistema de detecção e prevenção de intrusões em rede, baseado em assinaturas e análises comportamentais, para bloquear ataques conhecidos e zero-day;

Advanced Malware Protection (AMP) – Proteção contra malware avançado, inclusive ransomware, spyware e ameaças persistentes avançadas (APT);

Application Control – Controle de aplicações em nível granular, permitindo políticas por aplicação, categoria ou assinatura;

URL Filtering – Filtragem de URLs baseada em categorias, reputação e listas dinâmicas para bloqueio de sites maliciosos ou não autorizados;

DNS Filtering – Filtragem DNS para bloquear domínios perigosos e prevenir ataques baseados em manipulação de DNS;

Video Filtering – Controle sobre streaming e vídeos em plataformas específicas para adequação ao uso corporativo e à largura de banda;

Antispam Service – Serviço antispam integrado, mitigando phishing e spam antes de chegar à rede interna;

FortiCare Premium – Suporte técnico especializado 24x7, acesso a firmware, atualizações, patches e atendimento prioritário pela Fortinet;

O licenciamento deve ser entregue de forma integrada com o equipamento ou serviço (hardware + licença) para garantir conformidade do SLA e evitar descontinuidade de proteção.

ITEM 11 – SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA - TIPO 01:

Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

A solução deve suportar receber, no mínimo, 25 (vinte e cinco) GB de logs diários;

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses.

A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2016/ 2019 / 2022 e KVM no Redhat 9.1;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com as seguintes nuvens públicas: Amazon (Web Service AMI, EC2, EBS), Alibaba Cloud, Google Cloud Platform, IBM Cloud, Microsoft Azure e Oracle Cloud Infrastructure;

Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

Possuir suporte para SNMP versão 2 e 3;

Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

Deve permitir gerar alertas de eventos a partir de logs recebidos;

A solução deve ter relatórios predefinidos;

Permitir importação e exportação de relatórios;

Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

Deve possuir mecanismos de remoção automática para logs antigos;

Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

Permitir o envio por e-mail relatórios automaticamente;

Deve permitir que o relatório seja enviado por Email para o destinatário específico;

Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

Deve permitir o uso de filtros nos relatórios;

Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

Permitir especificar o idioma dos relatórios criados;

Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

Deve permitir exportar os logs no formato CSV;

Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

Deve permitir visualizar em tempo real os logs recebidos;

Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória);

Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

Deve possuir relatório de uso de aplicações e mídias sociais;

Deve possuir relatório de prevenção de perda de dados (DLP);

Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

Deve possuir relatório diário resumido de eventos e incidentes de segurança;

Deve possuir um relatório de tráfego DNS e e-mail;

Deve possuir relatório das 10 principais aplicações utilizadas na rede;

Deve possuir relatório dos 10 principais sites web utilizados na rede;

Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

Deve suportar recursos de automação (*playbooks*) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança.

ITEM 12 – SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA COMO SERVIÇO - TIPO 01:

CARACTERÍSTICAS DO SERVIÇO

Contratação de serviço contínuo que compreende o fornecimento, implantação, licenciamento, atualização e manutenção integrada de solução de segurança de rede — incluindo suas respectivas máquinas virtuais licenças — prestado de forma as a Service. Todo o conjunto (máquina virtual e licenciamento) será disponibilizado ao CONTRATANTE como serviço gerenciado, e não como bem isolado.

O serviço deverá ser prestado de forma ininterrupta pelo prazo de 12 (doze) meses. Durante todo esse período, o contratado deverá assegurar a plena operação da máquina virtual e das licenças, bem como sua substituição preventiva ou corretiva, atualizações de software/firmware e suporte técnico especializado.

Apesar de tratar-se de prestação de serviço contínuo, o valor deverá ser apresentado na proposta como montante global correspondente aos 12 (doze) meses de execução. Ou seja, a proposta deve apresentar um valor único total para o período integral contratado.

Para fins de faturamento, o pagamento será realizado mensalmente em parcelas correspondentes a 1/12 (um doze avos) do valor global contratado, garantindo a execução financeira conforme a prestação efetiva do serviço.

Quanto ao pagamento, deverá ser seguido o cronograma para o pagamento mensal abaixo:

a) Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;

b) Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;

c) Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;

d) O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

CARACTERÍSTICAS DO GERENCIAMENTO DE LOGS E RELATORIA "*AS A SERVICE*"

Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

A solução deve suportar receber, no mínimo, 25 (vinte e cinco) GB de logs diários;

A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2016/ 2019 / 2022 e KVM no Redhat 9.1;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com as seguintes nuvens públicas: Amazon (Web Service AMI, EC2, EBS), Alibaba Cloud, Google Cloud Platform, IBM Cloud, Microsoft Azure e Oracle Cloud Infrastructure;

Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

Possuir suporte para SNMP versão 2 e 3;

Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

Deve permitir gerar alertas de eventos a partir de logs recebidos;

A solução deve ter relatórios predefinidos;

Permitir importação e exportação de relatórios;

Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

Deve possuir mecanismos de remoção automática para logs antigos;

Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

Permitir o envio por e-mail relatórios automaticamente;

Deve permitir que o relatório seja enviado por Email para o destinatário específico;

Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

Deve permitir o uso de filtros nos relatórios;

Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

Permitir especificar o idioma dos relatórios criados;

Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

Deve permitir exportar os logs no formato CSV;

Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

Deve permitir visualizar em tempo real os logs recebidos;

Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

Deve possuir relatório de uso de aplicações e mídias sociais;

Deve possuir relatório de prevenção de perda de dados (DLP);

Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

Deve possuir relatório diário resumido de eventos e incidentes de segurança;

Deve possuir um relatório de tráfego DNS e e-mail;

Deve possuir relatório das 10 principais aplicações utilizadas na rede;

Deve possuir relatório dos 10 principais sites web utilizados na rede;

Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

Deve suportar recursos de automação (*playbooks*) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança.

ITEM 13 – SOLUÇÃO DE GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO:

Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses;

A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2016/2019/2022, KVM no Redhat 9.1, Nutanix AHV (AOS 6.5);

Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);

Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução;

A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

Deverá 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;

Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

Permitir usar palavras chaves ou cores para facilitar identificação de regras;

Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

Permitir criação de regras que fiquem ativas em horário definido;

Permitir criação de regras com data de expiração;

Realizar o backup das configurações para permitir o retorno de uma configuração salva;

Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso;

Gerar alertas automáticos via Email, SNMP e Syslog;

Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.

Permitir backup das configurações e rollback de configuração para a última configuração salva;

Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;

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;

Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;

Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI;

A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;

A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

Deve suportar o gerenciamento de pontos de acesso de forma centralizada;

Deve suportar o gerenciamento centralizado de switches.

ITEM 14 – SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC) PARA GRUPO DE 100 ENDPOINTS:

Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses;

Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do Órgão;

Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;

A solução deve suportar capacidade de expansão para até 4.000 (dois mil) endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;

A solução deve estar licenciada para operação com, pelo menos, 100 (cem) endpoints conectados simultaneamente;

A solução deve ser entregue em alta disponibilidade;

A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

Para estações de trabalho, deve suportar verificação de compliance em VPN;

A licença contemplada deverá suportar todas as características exigidas neste Documento;

A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;

Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

Consultas em DHCP Fingerprint;

Consultas via protocolos HTTP/HTTPS;

Consultas via protocolo SNMP;

Consultas via protocolo SSH;

Consultas via protocolo Telnet;

Consultas de portas TCP;

Consultas de portas UDP;

MAC OUI;

Consultas via protocolo WMI;

Protocolo ONVIF;

Protocolo NetFlow;

Base assinaturas pré-definidas;

A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

Endereço MAC;

Endereço IP;

Sistema operacional;

Nome do host;

Horário de conexão;

Usuário conectado;

Localização.

A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

Android;

Apple iOS para iPhone, iPod e iPad;

Chrome OS;

Linux;

MacOS X;

Windows 7, 8 e 10;

Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;

Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;

Deve permitir a recategorização periódica de dispositivos;

Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;

A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;

A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;

A solução deve suportar RADIUS Change of Authorization;

A solução deve suportar MAC Address Bypass;

A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;

Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;

Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, e-mail, telefone), características da máquina (asset tag, hostname), localidade e horário;

A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;

A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

Deve permitir a definição de complexidade da senha dos usuários visitantes;

Deve ser possível definir um período de validade para as contas de usuários visitantes;

Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

A solução deve vincular o login do visitante à máquina utilizada no acesso;

Deve suportar a validação de credenciais:

Em base local interna à ferramenta;

Em servidores RADIUS;

Em servidores LDAP.

A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;

A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;

Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se re-autenticar;

Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;

A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;

Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;

A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;

Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;

Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;

Se um dispositivo não passar os testes de conformidade, deve ser possível:

Não forçar a remediação;

Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;

Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

Windows 7;

Windows 8;

Windows 10;

MacOS;

Linux.

Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

Presença de software de antivírus instalado e em execução;

Versão do sistema operacional;

Nome de domínio do Active Directory ao qual a estação Windows pertença;

Serviços em execução para estações Windows;

Informações sobre um determinado certificado digital em estações Windows;

Registros ou chaves de registro para estações Windows;

Processos em execução para estações Windows, Linux e MacOS;

Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;

Pacotes instalados em estações Linux e MacOS.

A solução deve ser capaz de monitorar quando um serviço requirido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

Programas de gerenciamento e distribuição de software;

GPO do Active Directory;

Captive Portal;

Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de e-mail e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

Deve suportar integração com soluções de patching;

Deve suportar integração com soluções de análise de vulnerabilidades;

A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

A solução deve armazenar os eventos internamente e permitir que sejam exportados;

A solução deve permitir a exportação dos eventos através de syslog;

Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;

A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc., para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;

Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

Caso o CONTRATANTE não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor inclui-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;

Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues.

ITEM 15 – SOLUÇÃO DE ACESSO À REDE DE CONFIANÇA ZERO (ZTNA):

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;

A solução de ZTNA deve estar dimensionada para suportar a gestão de, pelo menos, 2.000 máquinas, simultaneamente;

Deve estar licenciado para proteger 25 (vinte e cinco) dispositivos por 60 (sessenta) meses, atendendo aos requisitos desse item;

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses;

A solução ofertada não deve fazer uso de nenhum elemento na infraestrutura da CONTRATANTE, com exceção dos agentes nas estações e servidores gerenciados;

A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;

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;

A solução de ZTNA deve ser do mesmo fabricante de “Firewalls de Próxima Geração (NGFW)” fornecidos, a fim de garantir compatibilidade e integração nativa;

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;

Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;

A solução deve ser escalável até 50.000 agentes;

O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;

Deve ser compatível com pelo menos, os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;

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;

A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3.;

Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;

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 por agente e deverá ainda ser compartilhado com o proxy de acesso;

Deve ser possível revogar o certificado de um agente por meio da console central;

O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;

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 diferente, o acesso deverá ser bloqueado por padrão;

Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;

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;

Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;

Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;

Deve ser possível exportar os logs diretamente a nível de agente;

Deve ser possível exigir uma senha para desconectar o agente da console central;

Deve existir a possibilidade de restringir o usuário de realizar back up da configuração do agente;

Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;

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;

Deve ser possível configurar o agente para usar Proxy;

O agente deve permitir a configuração local via XML (eXtensible Markup Language);

Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;

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;

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;

Deve ser possível especificar a validade do código de registro;

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;

A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;

Deve ser possível agrupar agentes em grupos;

Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;

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;

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 WiFi, 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 de 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;

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;

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;

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;

Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;

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;

Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso a recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;

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;

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;

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;

A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;

Deve ser possível verificar quais endpoints estão associadas com cada tag;

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;

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;

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;

Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;

Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;

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;

Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;

Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;

Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;

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;

Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;

O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário;

Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;

Deve suportar a criação de várias versões de pacotes de instalação;

As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;

Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de

aplicar a remediação imediatamente;

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;

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;

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;

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;

Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;

Deve ser possível determinar quando o filtro web entrará em ação no agente, se o mesmo deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;

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;

O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.

ITEM 16 – SOLUÇÃO DE SERVIÇO DE ACESSO SEGURO DE BORDA (SASE):

CARACTERÍSTICAS GERAIS

A gerência deve ser disponibilizada em nuvem, sem usar qualquer recurso do cliente;

A solução SASE deve ser baseada em uma arquitetura em nuvem, permitindo a integração de funções de rede e segurança como serviço em uma única plataforma;

O acesso a console de administração da solução SASE deve feito via navegador web e ter a possibilidade de se integrar com IdP para autenticação SSO dos usuários administrativos;

A solução SASE deve garantir o acesso seguro à web, serviços em nuvem e aplicações privadas, independentemente da localização do usuário ou de onde essas aplicações estão hospedadas;

A solução SASE deve ser (SaaS) software baseado em serviço que permite aos clientes acessarem a Internet com segurança e proteção. Deve garantir a proteção de endpoints e usuários remotos off-net (fora da rede) com o mesmo nível de segurança de quando estão na rede, independentemente de sua localização;

A solução SASE deve ser composta por, no mínimo:

FWaaS (Firewall as a Service);

SWG (Secure Web Gateway);

CASB (Cloud Access Security Broker);

ZTNA (Zero Trust Network Access);

SD-WAN (Software-Defined Wide-Area Network);

DLP (Data Loss Prevention);

Todos os componentes da solução SASE devem ser de um único fabricante, ou seja, deve ser uma solução Single-Vendor SASE (conforme definição cunhada pelo Gartner);

A solução SASE deve ter cobertura mundial, com possibilidade de provisionamento nos seguintes continentes: Américas, Europa, África, Ásia e Oceania;

A solução SASE deve permitir e estar licenciado para provisionamento em, no mínimo, 4 (quatro) pontos de presença (POP).

Ao menos um ponto de presença deve estar disponível obrigatoriamente no Brasil;

Os 4 (quatro) pontos de presença incluídos na solução SASE devem permitir a configuração de, no mínimo, 1 (um) endereço de IP fixo para cada. Caso a solução exija licenciamento adicional, este deve ser entregue para todos os POPs;

A solução SASE deve possuir, além da redundância geográfica, a possibilidade de o usuário escolher em qual POP os logs serão armazenados para estar em compliance com legislações locais;

A plataforma em nuvem da solução SASE deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semanas, com disponibilidade mensal de 99.999% para todos os serviços;

Quando um tráfego for direcionado a um POP da solução SASE, todo o processamento das funcionalidades de segurança deve acontecer dentro desse mesmo POP, sem que o tráfego seja direcionado para processamento, em cadeia, em diferentes datacenters;

A comunicação entre agentes (clientes) e outras soluções de infraestrutura SASE devem sempre usar comunicação segura criptografada;

A solução SASE deve permitir a integração com ambiente corporativo, escritórios, sites remotos através de SD-WAN Seguro;

A solução SASE deve suportar os acessos:

Acesso seguro à Internet (SIA) - com ou sem Agente;

Acesso Privado Seguro (SPA) – integração com outras arquiteturas que permitam o acesso privado seguro através de soluções como ZTNA, SD-WAN e NGFW para garantir eficiência e conectividade aos recursos locais. As integrações com soluções NGFW devem ser feitas por comunicação criptografada e preferencialmente por túneis IPSec;

Acesso seguro a aplicações SaaS - Através da integração de API com provedores de nuvem, CASB deve adicionar controle e visibilidade aos dados e aplicações sancionados;

A solução SASE deve permitir o acesso remoto seguro às aplicações hospedadas localmente (on-Premisse) através da integração de uma arquitetura SASE e ZTNA;

A solução SASE deve permitir acesso seguro para aplicações em nuvem com CASB, adicionando mais controle, visibilidade das aplicações permitidas e dados de tráfego através de uma integração com a API do provedor;

A solução SASE em conjunto com a arquitetura ZTNA deve permitir controle e análise profunda de postura do endpoint, permitindo o acesso apenas a partir de dispositivos seguros e as características específicas de cada acesso.

A solução SASE, deve ter componente de Web Gateway Seguro com base de informações, inteligência, pesquisa e desenvolvimento de proteções com suporte a:

Inspeção SSL;

Antivírus;

IPS;

Filtro Web baseado em categorias;

Proteção contra domínios de C&C;

Inline CASB;

Filtro de canais de Youtube;

A solução SASE deve permitir o redirecionamento do tráfego web para uma solução de isolamento remoto de navegador (RBI), a partir de políticas de segurança que leve em consideração parâmetros tais como a categoria do site visitado e o usuário ou o seu grupo;

Caso a solução SASE não possua nativamente uma solução de isolamento remoto de navegador (RBI), o licenciamento de uma solução do mesmo fabricante será permitido, desde que inclua o quantitativo de licenças para atender todos os clientes da solução SASE;

O componente de isolamento remoto de navegador (RBI) deve possuir controle granular para bloquear ou permitir: clicar com o botão direito; imprimir para PDF; fazer o upload e/ou download de arquivos executáveis, de imagem, de texto e do Microsoft Office; copiar e colar textos.

Para acessos no formato SWG, sem cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, Radius ou SAML;

A solução SASE deve reconhecer o tráfego de rede gerado por um grande número de aplicações. O controle de aplicação com Inline-CASB deve usar decodificadores de protocolo que podem analisar o tráfego de rede para detectar o tráfego de aplicação, mesmo que o tráfego use portas ou protocolos não padrão. O Controle de Aplicação com Inline-CASB deve suportar a detecção de tráfego usando o protocolo HTTP (versões 1.0, 1.1 e 2.0);

A solução SASE deve permitir a configuração e adição do Inline-CASB sob demanda, suportar o controle de aplicações SaaS através de inclusão de headers http e restrição de tenant tanto no uso com cliente quanto no uso sem cliente;

A solução SASE deve suportar e estar licenciada para controlar, no mínimo, as seguintes aplicações SaaS:

Microsoft Office 365;

Microsoft OneDrive;

Microsoft Teams;

Outlook ou Hotmail;

ChatGPT;

Gmail;

Google Workspace (Calendar, Docs, Drive, Meet);

Meta (Facebook, Instagram);

YouTube;

DocuSign;

GitHub;

LinkedIn;

Zoom;

A solução SASE deve permitir a geração de relatórios e visualização de logs. Os relatórios e logs deverão informar sobre atividades de rede, detecção de vírus, visita a sites inválidos, intrusões, tentativas de falha de login, etc.

A solução SASE deve permitir gerar relatórios de dados a partir de logs. Deve permitir executar regularmente relatórios em intervalos programados e executar relatórios manualmente quando desejado;

A solução SASE deve possuir módulo de logs para informações estatísticas e de segurança;

A solução SASE deve permitir o encaminhamento de forma segura de logs para um servidor externo no formato Syslog ou CEF;

Para acessos através de cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, RADIUS ou SAML;

A solução SASE deve gerar certificados que serão utilizados pelos Agentes para registro. Apenas certificados gerados pela solução deverão ser aceitos para validação;

A solução SASE deve utilizar apenas 01 (um) Agente (Cliente) para a comunicação com a plataforma SASE, ZTNA e outros benefícios como Sandbox, AntiMalware, Varredura de Vulnerabilidades, Inventário de Software, Filtro Web, entre outros;

A solução SASE deve permitir que sejam aplicadas políticas de segurança de forma granular para o acesso seguro à Internet e para o acesso a aplicações internas em conjunto com o ZTNA ou Acesso Privado Seguro (SPA), com controle baseado em IP, Aplicação, Usuário ou Grupo de Usuários;

O Agente da solução SASE deve ser compatível com os seguintes Sistemas Operacionais: Windows, macOS, Linux, Android e iOS;

A solução SASE deve ter integração através do SAML com IdP's como Azure AD e Okta, facilitando a autenticação dos usuários para se conectarem ao ambiente SASE;

O Agente da solução SASE deve ser implementado manualmente através do download e inclusão do "Código de Convite" para ativar as funcionalidades;

Após o registro do Agente na solução SASE, deve ser possível usar diferentes usuários (um de cada vez) para estabelecer o túnel e enviar tráfego para o SASE;

A solução SASE deve possuir o suporte à configuração de uma conexão sempre ativa. A configuração sempre ativa é opcional e customizada pelo administrador da solução;

A solução SASE deve suportar a configuração do Acesso à Rede de Confiança Zero (ZTNA) sem instalação de Agente adicional (agentless ZTNA).

O acesso a aplicações via ZTNA sem agente deve suportar a configuração de aplicações privadas, que serão roteadas através do recurso Acesso Privado Seguro (SPA);

A solução SASE deve ter disponibilidade de pelo menos 1.0 Mbps de tráfego por usuário;

A solução SASE deve permitir o controle de mídias removíveis USB nos dispositivos finais;

A solução SASE deve permitir o acesso de aplicações privadas através de Proxy ZTNA em um NGFW;

O cliente deve possuir funcionalidades de antivírus e envio de arquivos para análise de sandbox para proteção da estação caso o acesso à internet deixe de ser realizado de forma segura via SASE;

A solução SASE deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso, impedindo que um cliente não conforme possa se conectar a recursos;

A postura deve ser monitorada continuamente para que, caso ocorra alguma alteração de conformidade, o acesso aos recursos possa ser bloqueado;

A solução SASE deve permitir a desativação ou ativação da análise de postura dos endpoints;

Quando necessária a autenticação WEB para a solução SASE, as informações de login devem ser transmitidas por SSL e mantidas de forma segura;

A solução de SASE deve ter console com módulos:

Painéis de monitoramento;

Configurações de Rede;

Configurações SASE;

Configurações do Sistema;

Analytics que pode ser usado para análise em tempo real e elaboração de relatórios;

A solução de SASE deve permitir criar e modificar o Dashboard (painel web) com matriz personalizável de widgets.

A solução SASE deve incluir Dashboards (painéis) para monitorar o inventário de dispositivos, ameaças de segurança, tráfego e saúde da rede. Deve incluir os seguintes painéis:

Status: Fornece uma visão geral do seu ambiente SASE atual e do status do endpoint;

Mapa de Ativos: Exibe a localização geográfica dos ativos, incluindo servidores, em um mapa global. Também indica qual servidor tem o registro ativado;

Visão Única: Sistema abrangente de monitoramento para sua rede que integra dados em tempo real e históricos em uma única visualização. Deve permitir usá-lo para registrar e monitorar ameaças às redes, filtrar dados em vários níveis e acompanhar a atividade administrativa.

A solução SASE deve disponibilizar os seguintes monitores:

Fontes: Exibe fontes por volume de tráfego e detalhamento por fonte;

Thin-Edge: Exibe dispositivos Thin-Edge por volume de tráfego e detalhamento por dispositivo;

Destinos: Exibe destinos por volume de tráfego e detalhamento por destino;

Aplicações: Exibe aplicações por volume de tráfego e detalhamento por aplicação;

Aplicações em Nuvem: Exibe aplicações em nuvem e detalhamento por aplicação;

Sites da Web: Exibe sites por contagem de sessão e detalhamento por domínio;

Políticas: Exibe políticas por volume de tráfego e detalhamento por número de política;

Sessões: Exibe sessões por fonte de tráfego;

VPN: Exibe conexões VPN por usuário;

Ameaças: Exibe ameaças e detalhamento por ameaça.

A solução SASE deve permitir visualizar os endpoints gerenciados através do widget de status correspondente ou do monitor de status. Tanto o widget quanto o monitor devem exibir gráficos que mostram informações do endpoint, incluindo o status e a plataforma. Deve permitir o cancelamento do registro de um endpoint a partir do widget ou monitor;

Para auxiliar os administradores no diagnóstico de problemas de conectividade e de performance de rede dos usuários remotos, a solução SASE deve incluir recursos de monitoramento fim-a-fim, desde o cliente da solução, passando pelo POP e até as aplicações de destino;

A solução SASE deve permitir que monitoramentos sejam executados em tempo real e exibam as informações de consumo de CPU, memória e disco da estação cliente, além dos dados de performance de acesso (perda de pacotes e tempo de ida-volta (RTT)) à aplicação SaaS escolhida;

A solução SASE deve permitir perfis administrativos específicos para administradores de leitura ou escrita;

A solução SASE deve ter gerenciamento de implantação pela console da solução. Assim, implantações e atualizações de quaisquer soluções complementares podem ser obtidas através da nuvem;

A solução SASE deve possuir suporte a segurança e filtros de DNS para os acessos via agente de forma a impedir ataques e acessos inseguros na camada de DNS;

A solução SASE deve ter componente FWaaS (Firewall como Serviço) para aplicar políticas com Perfis que incluem Filtro Web, Antimalware, DLP, Filtro DNS, Filtro de Arquivos, IPS, Controle de APP e Inspeção SSL;

A solução SASE deve ter mecanismo de prevenção de vazamento de dados para impedir que dados sensíveis saiam e entrem nos dispositivos protegidos;

A solução SASE deve trazer dicionários de informações sensíveis, pré-definidos e atualizados automaticamente pelo fabricante, contendo no mínimo: números de cartões de crédito, códigos fonte Python, Java, Powershell e C, arquivos de configuração de equipamentos Cisco, CPF (Cadastro de Pessoa Física), CNPJ (Cadastro Nacional de Pessoa Jurídica) e CNH (Carteira Nacional de Habilitação);

A solução SASE deve permitir a criação de dicionários personalizados de informações sensíveis, utilizando palavras chaves, expressões regulares e lógica booleana;

A solução de SASE deve permitir a personalização de páginas HTML de bloqueio que são exibidas nos endpoints em certas situações com base nas configurações do Controle de Aplicação;

A solução SASE deve permitir o login de usuários e aplicar políticas IAM para controle do acesso administrativo;

A solução SASE deve implementar MFA para autenticação de usuários administrativos;

A solução SASE deve manter em sua plataforma em nuvem as regras de segurança, seja para acesso à plataforma ou as políticas impostas pelo SASE, para controlar os usuários remotos. A plataforma de gerenciamento e configuração de políticas de segurança não deve ficar restrita a apenas um PoP e deve ser altamente disponível, replicando os perfis de segurança para todos os PoPs de segurança do cliente;

A solução SASE deve inspecionar a camada SSL/TLS durante a inspeção de certificados e as camadas superiores durante a inspeção profunda. A solução SASE deve filtrar e proteger o tráfego seguro que os vários perfis de segurança processaram. A inspeção SSL deve proteger, além do tráfego HTTPS, outros protocolos criptografados comumente usados, como SMTPS, POP3S, IMAPS e FTPS;

A configuração do Secure Web Gateway da solução SASE deve ser feita sem a necessidade de um agente no endpoint para acesso HTTP e HTTPS, permitindo que políticas de segurança sejam aplicadas para proteger o acesso;

O controle do CASB pode ser efetuado em console separada permitindo maior controle e segmentação de acesso através de perfis de IAM;

O módulo CASB deve ter visibilidade de conteúdos do S3 Bucket da AWS, Storage do Azure e GCP, além das integrações do Microsoft e Google Workspace.

CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO SERVIÇO

Deve estar licenciada para no mínimo 500 (quinhentos) usuários;

Cada usuário deve ter direito de uso da solução em no mínimo 3 (três) dispositivos simultâneos.

Caso o licenciamento da solução seja feito por dispositivo e não por usuário, a solução deve ser entregue licenciada para suportar no mínimo 1.500 (mil e quinhentos) dispositivos.

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses.

ITEM 17 – SOLUÇÃO DE TOKEN PARA MFA PARA GRUPO DE 50 USUÁRIOS:

CARACTERÍSITCAS GERAIS PARA TOKEN MFA

Deve permitir o download gratuito nas lojas de aplicativos separado do seu provisionamento;

O aplicativo deve suportar a inclusão e exclusão de novos tokens;

Deve ser instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo que tenha a necessidade de gerenciar remotamente o dispositivo do usuário;

Deve garantir a privacidade do dispositivo móvel, ou seja, não deve ser capaz de consultar histórico de navegação;

Deve requerer a permissão proprietário para envio de notificações ou qualquer tipo de alteração nas configurações;

Deve suportar as principais plataformas de mobile do mercado (iOS, iPadOS, Android, Windows Phone 8 e 8.1,), além de ser suportado em sistemas operacionais desktops Windows 10 e superiores;

Deve suportar a geração dinâmica das sementes de token, minimizando a exposição online;

Deve suportar ativação através da utilização de QR Codes e manual;

Deve criptografar o armazenamento de sementes utilizadas na geração do token;

Deve ser capaz de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH;

Deve suportar a ocultação do token para tokens baseados em tempo (TOTP);

Deve capaz de proteger abertura do aplicativo através de PIN ou Impressão Digital ou Face Security;

Deve exibir o intervalo de tempo OTP;

Deve exibir do número de série do token;

Deve ser compatível com o relógio da Apple;

Deve suportar que a senha gerada possa ser copiada para a área de transferência;

Deve suportar detalhes de login enviados ao telefone para aprovação com um toque;

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;

Deve ser compatível e integrável com as soluções dos itens de Firewall de Próxima Geração (NGFW);

Deve estar de acordo com as seguintes RFCs para especificações OTP: RFC6238 e RFC4226;

Deve ser capaz de realizar vinculação com o dispositivo móvel;

Deve suportar à sua utilização como segundo fator de autenticação para acesso VPN, sem a necessidade de utilização de um servidor Radius;

Deve ser compatível com Google, Dropbox, Amazon e outros tokens TOTP (Time-based One-Time Password) compatíveis com OAT;

PACOTE DE USUÁRIOS

Deve permitir ser associado a até 50 (cinquenta) usuários;

Deve ter a flexibilidade de ser desmembrado, com ou sem ajuda do suporte técnico do fabricante, em pacotes menores para permitir a associação independente nas soluções dos itens Firewall de Próxima Geração (NGFW).

Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo pelo período de 60 (sessenta) meses.

ITEM 18 – TRANSCEIVER SFP 1000BASE-SX:

Transceiver SFP para conexão de fibras ópticas multimodo de até 500m em fibras 50/125 µm e até 200m em fibras 62.5/125 µm;

Deve ser compatível com o padrão IEEE 802.3z (1000Base-SX);

Deve ter velocidade de 1GbE;

Deve suportar a inserção a quente (Hot Plug);

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

Deve possuir garantia do fabricante pelo período de 12 (doze) meses.

ITEM 19 – TRANSCEIVER SFP+ 10GBASE-SR:

Transceiver SFP+ para conexão de fibras ópticas multimodo de até 400m em fibras OM4 e até 300m em fibras OM3;

Deve ser compatível com o padrão IEEE 802.3ae (10GBase-SR);

Deve ter velocidade de 10GbE;

Deve suportar a inserção a quente (Hot Plug);

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

Deve possuir garantia do fabricante pelo período de 12 (doze) meses.

ITEM 20 – TRANSCEIVER SFP+ 10GBASE-LR:

Transceiver SFP+ para conexão de fibras ópticas monomodo de até 10Km;

Deve ser compatível com o padrão IEEE 802.3ae (10GBase-LR);

Deve ter velocidade de 10GbE;

Deve suportar a inserção a quente (Hot Plug);

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

Deve possuir garantia do fabricante pelo período de 12 (doze) meses.

ITEM 21 – TRANSCEIVER QSFP+ 40GBASE-SR4:

Transceiver QSFP+ para conexão de fibras ópticas multimodo de até 150m em fibras OM4 e até 100m em fibras OM3;

Deve ser compatível com o padrão IEEE 802.3ba (40GBase-SR4);

Deve ter velocidades de 40GbE;

Deve suportar a inserção a quente (Hot Plug);

Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

Deve possuir garantia do fabricante pelo período de 12 (doze) meses.

ITEM 22 – BANCO DE HORAS TÉCNICAS:

SERVIÇOS ESPECIALIZADOS PARA NOVAS DEMANDAS OU CORREÇÃO DE PROBLEMAS NÃO PREVISTOS CONTENDO NO MÍNIMO, OS SEGUINTES REQUISITOS:

Visando garantir o perfeito funcionamento da solução após implementação, levando em consideração de ser uma solução nova para o time técnico da CONTRATANTE, mesmo após treinamento sobre as funcionalidades e operação assistida, deverá ser ofertado serviço de banco de horas técnica em caso de intercorrências que prejudiquem o bom funcionamento e que necessitem de intervenção no ambiente da CONTRATANTE por time técnico qualificado para tal resolução por parte da CONTRATADA.

O serviço deverá ser prestado preferencialmente de forma remota, com prazo de uso durante o período contratado de 12 (doze) meses.

O serviço especializado será demandado através de Ordens de Serviço (OS) prevendo o quantitativo a serem consumidos, o período de execução e a descrição dos serviços a serem executados.

Qualquer alteração na quantidade de horas deverá ser justificada e previamente aprovada pela CONTRATANTE.

Os serviços proporcionais de gerenciamento de projetos e liderança técnica deverão estar incluídos dentro do valor da hora.

O serviço especializado abrange as seguintes atividades, podendo por meio de livre acordo entre as partes através de comunicação formal abrangerem itens não contemplados neste Documento:

Resolução de problemas críticos na infraestrutura de processamento, armazenamento, backup, *firewall*, virtualização e redes;

Revisões e/ou Alterações de configurações, novas instalações, atualização de versões de softwares ou firmwares;

Execução de testes programados de recuperação de desastres visando validar o plano de continuidade de negócios;

Treinamento para conscientização sobre ameaças cibernéticas;

Serviços consultivos, para apoiar a avaliar, melhorar e testar processos de resposta a incidentes críticos de segurança;

Serviço de consolidação em dashboard com inúmeros fatores de riscos externos, como: serviços e portas divulgados publicamente, credenciais vazadas, identificação de páginas web, domínios e perfis de redes sociais que tentem se passar pela CONTRATANTE;

Serviço de Implantação e Configuração para Solução De Segurança e Gerência De Redes;

Serviço de Implantação e Configuração para Unidade Centralizada de Armazenamento de Logs e Relatoria;

Serviços Profissionais de Implantação e Configuração Unidade de Gerência Centralizada de Equipamentos;

Instalação e configuração de Solução de Segurança;

Treinamentos especializados;

Migrações de dados;

Diagnóstico de problemas de desempenho e planejamento de capacidade;

Recuperação de dados através de Software de Backup e Replicação;

Recuperação de solução de segurança de dados em ambiente VIRTUALIZADO;

Implementação de regras de segurança;

Configurações em ativos de rede;

Elaboração de documentação técnica e de usuário;

Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE;

Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas;

Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;

Realização de operação assistida e monitoramento de ambientes entregues com a solução;

Orientar na utilização dos softwares instalados no CONTRATANTE com a utilização das melhores práticas e orientações dos fabricantes;

Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no CONTRATANTE minimizando impactos;

Apoiar na configuração/parametrização do sistema em novas máquinas;

Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do CONTRATANTE;

Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;

Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;

Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistemas e produtos foram instalados;

Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE;

Esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE;

Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;

Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;

Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;

Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente.

A licitante deverá possuir uma ferramenta de SERVICE DESK on-line e que siga as melhores práticas da certificação ITIL para a abertura e gerenciamento de chamados na utilização dos bancos de horas, a fim de acompanhar o tempo de resolução para cada atividade (SLA), bem como disponibilizá-los em filas de priorizações para cada ocorrência, serviço e/ou incidente.

A ferramenta mencionada deverá permitir que a CONTRATANTE realize abertura de chamados através de e-mail, portal na Internet e/ou aplicativo de celular, sendo que cada chamado deverá possuir um código de identificação único que permita a sua rápida identificação.

O sistema deverá permitir o acompanhamento em tempo real pela CONTRATANTE dos chamados abertos e seus respectivos status, além de permitir a visualização do histórico de todos os chamados finalizados.

Para melhor gerenciamento dos chamados pela CONTRATADA, o sistema deverá possuir um painel (dashboard) que possua gráficos e outros tipos de visualizadores, além de permitir a geração de relatórios conforme necessidade e solicitação da CONTRATANTE.

Para fins de comprovação, o licitante deverá informar o nome da ferramenta de service desk utilizada, sob pena de desclassificação.

Todo processo do serviço realizado deverá ser demonstrado em relatórios com todos os seus detalhes da sua execução.

Após a abertura de um chamado no sistema, o primeiro atendimento deverá ocorrer de forma remota para melhor entendimento do cenário e sua possível solução. Todavia, caso o atendimento remoto não seja suficiente para conclusão do chamado, então o atendimento deverá ser realizado de forma on-site, ou seja, de forma presencial no endereço da CONTRATANTE.

Quanto remoto, o atendimento será feito por ferramenta que contabilizará o tempo de acesso e trabalho, a fim de validar a consumação do banco de horas.

O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculado ao item da Ordem de Serviço (*ANEXO - MODELO DE ORDEM DE SERVIÇO (OS)*).

Quanto ao pagamento, deverá ser seguido o cronograma para o pagamento mensal abaixo:

a) Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;

b) Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;

c) Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;

d) O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

ITEM 23 – UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON:

O quantitativo de Unidade de Serviço Técnico (UST) será determinado de acordo com a atividade a ser realizada, nos termos definidos na presente especificação técnica.

Visando simplificar a visualização das necessidades de UST para implantação, abaixo consta quadro resumo de utilização de USTs, por tipo de Serviço de Implantação:

ATIVIDADES	NÚMERO DE UST
Planejamento de Implantação e do Hands On	30
Instalação de Ativos e Serviços de Segurança	5
Instalação de Solução de Controle de Acesso à Rede (NAC) ou Solução de Serviço de Acesso Seguro de Borda (SASE)	35

PLANEJAMENTO DE IMPLANTAÇÃO E HANDS ON

O Planejamento de Implantação e Hands On deverá, pela sua complexidade, utilizará 30 USTs.

O Planejamento de Implantação compreende, entre outros, os seguintes procedimentos:

Análise de topologia e arquitetura da rede, considerando os firewalls, switches, access points, VLANs e outros componentes relevantes da infraestrutura da CONTRATANTE;

Análise de acesso à Internet, sites remotos, serviços de rede oferecidos aos usuários internos e externos;

Análise das regras de firewall existentes e aplicadas à solução ofertada e avaliação de melhores práticas, para implementação da solução;

Apresentação de plano de implantação, com descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

Geração de relatório e entrega de documentação da instalação, com as configurações efetuadas e as decisões tomadas, diagramas e topologias, em formato legível e tecnicamente fundamentado;

Deslocamentos, hospedagens, alimentação e outros itens que se julgarem necessários para que a instalação seja local. A configuração pode ser remota.

A CONTRATADA deverá realizar repasse de conhecimento, do tipo "Hands On" sobre a solução de Firewall, NAC e SASE, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento.

O repasse de conhecimento será ministrado para um total de 4 (quatro) participantes da CONTRATANTE, podendo ser remoto.

A CONTRATADA deverá fornecer todo material audiovisual, didático.

Deverá ter caráter prático e se baseará no sistema contratado e instalado na CONTRATANTE.

Os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.

Após a implementação, deverá ser fornecido documento "*as-built*", que descreve os principais elementos de implementação da configuração implantada e os resultados da verificação do sistema de base.

INSTALAÇÃO DE ATIVOS E SERVIÇOS DE SEGURANÇA

Os ativos de segurança abrangem a instalação e configuração de: firewalls, solução de gerenciamento de logs e relatoria, proteção de aplicações de Web e API, solução de gerenciamento de configuração centralizado, solução de ZTNA.

Serão utilizados 5 (cinco) UST para cada equipamento ou solução indicado no item anterior instalado pela CONTRATADA.

Não necessariamente serão utilizadas as 5 (cinco) UST para cada equipamento ou solução adquirido, somente serão utilizadas as UST para os equipamentos ou soluções que a CONTRATADA realizar o serviço de instalação e configuração.

Os serviços de instalação e configuração compreendem, entre outros, os procedimentos, quando aplicável:

Teste de energização;

Atualização de firmware;

Configuração de IP LAN;

Configuração de IP WAN;

Instalação das licenças;

Troca de senha de Administrador;

Demais configurações necessárias para o perfeito funcionamento do equipamento ou solução.

INSTALAÇÃO DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (NAC) OU SOLUÇÃO DE SERVIÇO DE ACESSO SEGURO DE BORDA (SASE)

Ao adquirir uma unidade do item "*Instalação de Solução de Controle de Acesso à Rede (NAC) ou Solução de Serviço de Acesso Seguro de Borda (SASE)*", para sua implantação, será necessário o uso de 35 USTs para cada unidade.

Os serviços de instalação e configuração dessas Soluções, entre outros, os seguintes procedimentos:

Configuração do sistema, de acordo com as exigências levantadas, com as devidas atualizações necessárias;

Implantação integral, com todas as funcionalidades disponíveis, de acordo com a quantidade contratada;

Devem ser realizados testes iniciais no sistema de produção, para isso, deve-se incluir verificações básicas de saúde do ambiente, verificações de alta disponibilidade e verificações funcionais antes de colocar a solução em operação;

A contratada deverá fornecer suporte durante a implantação. Revisões menores ou ajustes finos podem ser feitos, se necessário para garantir o bom funcionamento;

Para o caso do SASE, serão necessários incluir 5 dias de serviços de implantação do Fabricante, como medida de robustez na implantação da solução. A comprovação deverá ser feita pela apresentação na proposta comercial do part number do Fabricante para este tipo de serviços;

É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material didático e, caso necessário, outros equipamentos eletrônicos para a realização dos repasses de conhecimento;

O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculado ao item da Ordem de Serviço (*ANEXO - MODELO DE ORDEM DE SERVIÇO (OS)*).

Quanto ao pagamento, deverá ser seguido o cronograma para o pagamento mensal abaixo:

a) Validação técnica: até o dia 5 (cinco) de cada mês subsequente da prestação dos serviços, a CONTRATADA deverá apresentar relatório considerando os serviços prestados;

b) Emissão da Fatura/Nota Fiscal: A CONTRATADA deverá emitir a fatura/nota fiscal até o dia 10 (dez) de cada mês, após a validação técnica;

c) Processo de pagamento: O CONTRATANTE realizará o pagamento até o dia 25 (vinte e cinco) de cada mês;

d) O CONTRATANTE poderá solicitar a prorrogação de vencimento da fatura quando verificar inconsistência na mesma, sem ônus para o CONTRATANTE.

ANEXO IV - JUSTIFICATIVA TÉCNICA PARA INDICAÇÃO DE MARCA – FORTINET

No contexto do presente processo licitatório destinado à contratação de soluções de segurança cibernética, incluindo equipamentos, licenças, softwares e serviços especializados para proteção da infraestrutura tecnológica do Tribunal de Justiça do Estado do Amapá (TJAP), o presente documento tem por finalidade apresentar a fundamentação técnica que justifica a indicação da marca FORTINET como padrão tecnológico a ser adotado.

A presente indicação baseia-se em critérios técnicos, operacionais, econômicos e estratégicos, observando-se os princípios estabelecidos pela Lei n.º 14.133/2021, especialmente no que se refere ao princípio da padronização previsto no art. 40, inciso V, alínea "a", que dispõe que as especificações dos objetos devem considerar a padronização, sempre que tecnicamente justificável.

De acordo com a referida legislação, a padronização visa garantir maior eficiência administrativa, segurança operacional e economicidade nas contratações públicas, permitindo que a Administração estabeleça critérios técnicos que assegurem

a compatibilidade entre as soluções já existentes e as novas aquisições.

1. PADRONIZAÇÃO TECNOLÓGICA DO PARQUE DE SEGURANÇA CIBERNÉTICA:

Desde o ano de 2021, o Tribunal de Justiça do Estado do Amapá vem adotando de forma progressiva soluções de segurança cibernética do fabricante Fortinet, consolidando um ecossistema tecnológico integrado para proteção da infraestrutura institucional. Nesse período, foram realizados diversos processos de aquisições/contratações para implantação dessas soluções, os quais resultaram nos seguintes contratos:

- PA 029891/2020 – Contrato nº 012/2021;
- PA 011856/2022 – Contrato nº 005/2022;
- PA 063176/2021 – Contrato nº 0071/2022;
- PA 018392/2022 – Contrato nº 0023/2021.

Essas aquisições/contratações permitiram a implementação de soluções estratégicas de segurança da informação, incluindo:

- Firewalls de próxima geração (Next Generation Firewall – NGFW);
- Sistemas de autenticação segura;
- Soluções de controle de acesso à rede;
- Ferramentas de monitoramento e análise de eventos de segurança;
- Plataformas de gerenciamento centralizado da segurança.

Com isso, consolidou-se no TJAP um ambiente de segurança baseado na arquitetura *Fortinet Security Fabric*, que integra diferentes componentes de proteção em uma única plataforma de gerenciamento e análise.

A introdução de soluções de fabricantes distintos poderia comprometer essa integração, gerar aumento da complexidade operacional e de custos, bem como reduzir a eficiência dos mecanismos de defesa atualmente implementados.

2. INTEGRAÇÃO TECNOLÓGICA E INTEROPERABILIDADE DA PLATAFORMA DE SEGURANÇA:

A arquitetura de segurança atualmente adotada pelo TJAP baseia-se na integração nativa entre diferentes soluções da fabricante Fortinet, que compartilham:

- Inteligência de ameaças;
- Correlação de eventos de segurança;
- Políticas centralizadas;
- Automação de respostas a incidentes.

Essa integração ocorre por meio da arquitetura denominada *Security Fabric*, que permite que os diferentes dispositivos e soluções de segurança operem de forma coordenada, compartilhando informações em tempo real. Entre os benefícios dessa integração destacam-se:

- Detecção mais rápida de incidentes de segurança;
- Resposta automatizada a ameaças;
- Correlação de eventos entre múltiplas camadas de segurança;
- Simplificação da gestão da infraestrutura de proteção.

A substituição parcial ou a introdução de soluções de fabricantes distintos poderia comprometer esse modelo integrado, reduzindo a capacidade de resposta a incidentes e aumentando a complexidade de gerenciamento da infraestrutura de segurança.

3. APROVEITAMENTO DOS INVESTIMENTOS REALIZADOS PELO TRIBUNAL:

Outro fator relevante para a indicação da marca Fortinet é o aproveitamento dos investimentos já realizados pelo Tribunal, tanto em infraestrutura quanto em capacitação da equipe técnica.

Além das aquisições de equipamentos e licenças, o TJAP também investiu na qualificação de seus servidores para operação e administração das soluções de segurança desse fabricante.

A seguir, são apresentados os processos administrativos de capacitação em soluções Fortinet:

- PA 098457/2024;
- PA 092668/2024;
- PA 130654/2024.

Esses investimentos permitiram que a equipe técnica do Tribunal adquirisse conhecimentos especializados na operação das plataformas Fortinet, garantindo maior eficiência na gestão da segurança da informação.

A adoção de soluções de fabricantes distintos demandaria novos investimentos em capacitação, aumento do tempo de aprendizagem da equipe e possível redução da eficiência operacional durante o período de adaptação.

4. EFICIÊNCIA OPERACIONAL E REDUÇÃO DE CUSTOS DE MANUTENÇÃO:

A padronização tecnológica também contribui diretamente para a redução de custos operacionais e maior eficiência na gestão da infraestrutura de segurança. Entre os principais benefícios observados destacam-se:

- Simplificação da gestão da infraestrutura de segurança;
- Redução da necessidade de múltiplas plataformas de gerenciamento;
- Diminuição da complexidade operacional;
- Redução do tempo de diagnóstico e resolução de incidentes;
- Melhor aproveitamento dos recursos humanos e orçamentários.

A adoção de soluções padronizadas também facilita a manutenção do ambiente tecnológico, permitindo maior previsibilidade na gestão de contratos de suporte, atualização de licenças e expansão da infraestrutura.

5. MANUTENÇÃO DA COMPETITIVIDADE DO PROCESSO LICITATÓRIO:

A indicação da marca Fortinet não compromete a competitividade do processo licitatório. No mercado brasileiro existem diversas empresas integradoras, revendedores e parceiros autorizados da fabricante Fortinet, aptos a fornecer equipamentos, licenças e serviços associados. Assim, a competição ocorrerá entre os diversos fornecedores habilitados, assegurando o cumprimento dos princípios da administração pública.

Essa dinâmica garante que o Tribunal possa selecionar a proposta mais vantajosa para a Administração, mantendo simultaneamente a padronização tecnológica necessária para a continuidade e segurança das operações.

6. CONCLUSÃO:

Diante do exposto, a indicação da marca FORTINET para as soluções de segurança cibernética a serem contratadas pelo TJAP, justifica-se pelos seguintes fatores:

- Padronização tecnológica do parque de segurança institucional;
- Integração nativa entre as soluções já implantadas;
- Aproveitamento dos investimentos realizados em infraestrutura e capacitação;
- Maior eficiência operacional e redução de custos de manutenção;
- Continuidade do modelo de segurança atualmente adotado.

Dessa forma, conclui-se que a indicação da marca Fortinet representa a alternativa tecnicamente mais adequada e vantajosa para atender às necessidades do TJAP, garantindo segurança, eficiência e continuidade na proteção da infraestrutura tecnológica da instituição.

ANEXO V - MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO N.º XXX/202X

ATA DE REGISTRO DE PREÇOS N.º:

CONTRATO N.º:

PROCESSO SEI N.º:

CONTRATANTE: Tribunal de Justiça do Estado do Amapá (TJAP)

CONTRATADA:

---

1. OBJETO:

Execução de serviços técnicos especializados de Tecnologia da Informação, sob demanda, na modalidade:

( ) Banco de Horas Técnicas
( ) Unidade de Serviço Técnico (UST)

---

2. DESCRIÇÃO DA DEMANDA:

---

3. QUANTITATIVO:

TIPO	QTD.
Horas Técnicas ( )	
UST ( )	

---

4. PRAZO DE EXECUÇÃO:

Início:
Término:

---

5. FORMA DE EXECUÇÃO:

( ) Remoto
( ) Presencial
( ) Híbrido

Local (se aplicável): _____

---

6. CRITÉRIO DE MEDIÇÃO:

• Banco de Horas: por horas efetivamente executadas
• UST: por unidade de serviço concluída

Mediante validação do Fiscal Técnico do contrato.

7. VALOR ESTIMADO:

Valor total estimado: R$ _____

---

8. ACEITE:

A presente Ordem de Serviço será considerada concluída após a execução dos serviços e validação pelo Fiscal Técnico.

---

9. RESPONSÁVEIS:

Solicitante: _____
Fiscal Técnico: _____

10. OBSERVAÇÕES:

Serviço sob demanda, conforme condições estabelecidas na Ata de Registro de Preços (ARP) e no Contrato.

ANEXO VI - MINUTA DE ATA DE REGISTRO DE PREÇOS

O Estado do Amapá, por intermédio do Tribunal de Justiça do Estado do Amapá, na cidade de Macapá-AP, inscrito(a) no CNPJ sob o nº 34.870.576/0001-21, neste ato representado pelo Excelentíssimo Senhor Presidente, o Desembargador JAYME HENRIQUE FERREIRA, cujo termo de posse foi publicado no Diário de Justiça Eletrônico nº XX, de XX de XXXXX de 202X, considerando o julgamento da licitação na modalidade de pregão nº ...../200..., mediante sistema de registro de preços, processo administrativo n.º ....., RESOLVE registrar os preços da empresa XXXXXXXX, inscrita no CNPJ sob o nº xxxxxxxxxxxx, com sede em xxxxxxxxxxx, neste ato representada por xxxxxxxxxxxx, atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 01 de abril de 2021, na Resolução nº 1.594, de 10 de maio de 2023, e em conformidade com as disposições a seguir:

1. **OBJETO**

1.1. O objeto do presente instrumento é o registro de preços para aquisição de.....

1.2. Vinculam-se a esta contratação, independentemente de transcrição:

1.2.1. O edital da licitação;

1.2.2. O termo de referência;

1.2.3. A proposta da contratada; e

1.2.4. Eventuais anexos dos documentos supracitados.

2. PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades mínimas e máximas, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item	Especificação	Quantidade	Valor unitário

2.2. É fornecedor adjudicatário da presente ata de registro de preços:

2.2.1. Razão social:

2.2.2. CNPJ:

2.2.3. Endereço:

2.2.4. Representante:

2.2.5. Contato:

2.3. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

2.4. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

3. ADESÃO À ATA DE REGISTRO DE PREÇOS

3.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

3.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou de descontinuidade de serviço público;

3.1.2. demonstração da compatibilidade dos valores registrados com os valores praticados pelo mercado, na forma prevista no art. 23 da Lei nº 14.133, de 2021; e

3.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

3.2. A autorização do TJAP apenas será realizada após a aceitação da adesão pelo fornecedor.

3.2.1. O TJAP poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

3.3. Após a autorização do TJAP, o órgão ou a entidade não participante efetivará a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

3.3.1. O prazo poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo TJAP, desde que respeitado o limite temporal de vigência da ata de registro de preços.

3.4. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos previstos neste instrumento.

3.5. Serão observadas as seguintes regras de controle para a adesão à ata de registro de preços:

3.5.1. As aquisições ou as contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o TJAP e para os órgãos ou as entidades participantes; e

3.5.2. o quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o TJAP e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

4. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

4.1. O prazo de vigência da ata de registro de preços será de um ano, contado do primeiro dia útil subsequente

à data de publicação no Diário de Justiça Eletrônico, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso e que o fornecedor tenha manifestado interesse na prorrogação.

4.1.1. A prorrogação da vigência da ata de registro de preço renova a quantidade inicial registrada, excluindo-se eventual saldo quantitativo remanescente da vigência inicial.

5. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

5.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

5.1.1. 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 da ata tal como pactuada, nos termos do disposto na alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

5.1.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados; ou

5.1.3. na hipótese de previsão no instrumento convocatório de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos do disposto na Lei nº 14.133, de2021.

5.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

a) A anualidade será contada a partir da data do orçamento estimado da licitação, fixada em 21/05/2026.

b) Para atualização do preço, aplica-se o Índice de Custo da Tecnologia da Informação (ICTI).

5.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

6. NEGOCIAÇÃO DOS PREÇOS REGISTRADOS

6.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado, por motivo superveniente, o TJAP convocará o fornecedor para negociar a redução do preço registrado.

6.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

6.1.2. Na hipótese prevista no item 6.1.1, o TJAP convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado.

6.1.3. Se não obtiver êxito nas negociações, o TJAP procederá ao cancelamento da ata de registro de preços e adotará as medidas cabíveis para a obtenção de contratação mais vantajosa.

6.1.4. Na hipótese de redução do preço registrado, o TJAP comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços, para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual.

6.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não puder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao TJAP a alteração do preço registrado, mediante comprovação de fato superveniente que o impossibilite de cumprir o compromisso.

6.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

6.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo TJAP e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, sem prejuízo da aplicação das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

6.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do disposto no item 6.2.2, o TJAP convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados.

6.2.4. Se não obtiver êxito nas negociações, o TJAP procederá ao cancelamento da ata de registro de preços e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

6.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto nos itens 6.2 e 6.2.1, o TJAP atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

6.2.6. O TJAP comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de

registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual.

7. CANCELAMENTO DO REGISTRO DO FORNECEDOR E DOS PREÇOS REGISTRADOS

7.1. O registro do fornecedor será cancelado pelo TJAP, quando o fornecedor:

7.1.1. descumprir as condições da ata de registro de preços sem motivo justificado;

7.1.2. não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

7.1.3. não aceitar manter seu preço registrado, na hipótese prevista no item 6.2.2; ou

7.1.4. sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

7.2. Na hipótese prevista no item 7.1.4, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, o TJAP poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas novas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

7.3. O cancelamento do registro nas hipóteses previstas no item 7.1 será formalizado por despacho, garantidos os princípios do contraditório e da ampla defesa.

7.4. Na hipótese de cancelamento do registro do fornecedor, o TJAP poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

7.5. O cancelamento dos preços registrados poderá ser realizado pelo TJAP, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

7.5.1. por razão de interesse público;

7.5.2. a pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

7.5.3. se não houver êxito nas negociações, nos termos do disposto nos itens 6.1.3 e 6.2.4.

8. CONTRATAÇÃO COM FORNECEDORES REGISTRADOS

8.1. A contratação com os fornecedores registrados na ata será formalizada por meio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o disposto no art. 95 da Lei nº 14.133, de 2021.

8.1.1. Os instrumentos serão assinados no prazo de validade da ata de registro de preços.

8.2. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8.3. A vigência dos contratos decorrentes do sistema de registro de preços será estabelecida no instrumento convocatório, conforme o disposto no art. 105 da Lei nº 14.133, de 2021, e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

8.4. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

8.5. A contratação posterior de item específico constante de grupo de itens exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou entidade.

9. PENALIDADES

9.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

9.1.1. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

9.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço, exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade.

9.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no edital ou no termo de referência, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

10. CONDIÇÕES GERAIS

10.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no edital e seus anexos.

Macapá-AP, *data da assinatura eletrônica*.

Desembargador Jayme Henrique Ferreira
Presidente

XXXXXXXXXX
Fornecedor

ANEXO VII - MINUTA DE CONTRATO

CONTRATO Nº XXX/2026-TJAP

CONTRATO QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ E A EMPRESA XXXXXXXXX, PARA OS FINS NELE DECLARADOS.

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ** , com sede na Rua General Rondon, nº 1295, na cidade de Macapá/Estado do Amapá, inscrito no CNPJ sob o nº 34.870.576/0001-21, neste ato representado pelo seu Presidente, Desembargador **JAYME HENRIQUE FERREIRA**, cujo termo de posse foi publicado no Diário da Justiça de nº 38 do dia 25 de fevereiro de 2025, doravante denominado **CONTRATANTE**, e a empresa XXXXXXXXXXXX, inscrita no CNPJ XXXXXXXXX, situada no endereço XXXXXXXXXXXX, através de seu representante legal o Sr. XXXXXXXXX, RG Nº XXXXXXX, CPF/MF Nº XXXXXXXX, doravante denominada **CONTRATADA** e, tendo em vista o que consta no Processo Administrativo nºXXXXXXXXX.8.03.0901-SEI e, em observância às disposições da Lei nº 14.133, de 2021, resolvem celebrar o presente Termo de Contrato, decorrente do Edital de Licitação referente ao Pregão Eletrônico nº XXX/2026, mediante as cláusulas e condições a seguir enunciadas.

1. OBJETO

1.1. O objeto do presente instrumento é aquisição, mediante registro de preços, de soluções de segurança da informação incluindo firewalls, soluções de gerenciamento, controle de acesso, acessórios necessários e serviços de sustentação e suporte, nos termos das condições estabelecidas neste instrumento e conforme tabela abaixo:

GRUPO ÚNICO					
ITEM	**DESCRIÇÃO**	**QTD.**	**UNIDADE DE MEDIDA**	**PREÇO UNITÁRIO ESTIMADO (R$)**	**PREÇO TOTAL ESTIMADO (R$)**
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	Unidade	XX.XXX,XX	XX.XXX,XX
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	4	Unidade	XX.XXX,XX	XX.XXX,XX
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	4	Unidade	XX.XXX,XX	XX.XXX,XX
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	6	Unidade	XX.XXX,XX	XX.XXX,XX
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	20	Unidade	XX.XXX,XX	XX.XXX,XX
6	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 06	4	Unidade	XX.XXX,XX	XX.XXX,XX
7	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) COMO SERVIÇO - TIPO 02	240	Firewall por mês	XX.XXX,XX	XX.XXX,XX
8	LICENCIAMENTO UTP PARA NGFW - TIPO 03	2	Unidade	XX.XXX,XX	XX.XXX,XX
9	LICENCIAMENTO UTP PARA NGFW - TIPO 04	4	Unidade	XX.XXX,XX	XX.XXX,XX

10	LICENCIAMENTO UTP PARA NGFW - TIPO 05	22	Unidade	XX.XXX,XX	XX.XXX,XX
11	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA - TIPO 01	10	Unidade	XX.XXX,XX	XX.XXX,XX
12	SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATORIA COMO SERVIÇO - TIPO 01	600	Unidade	XX.XXX,XX	XX.XXX,XX
13	SOLUÇÃO DE GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO	6	Unidade	XX.XXX,XX	XX.XXX,XX
14	SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC) PARA GRUPO DE 100 ENDPOINTS	50	Unidade	XX.XXX,XX	XX.XXX,XX
15	SOLUÇÃO DE ACESSO À REDE DE CONFIANÇA ZERO (ZTNA)	20	Unidade	XX.XXX,XX	XX.XXX,XX
16	SOLUÇÃO DE SERVIÇO DE ACESSO SEGURO DE BORDA (SASE)	1000	Unidade	XX.XXX,XX	XX.XXX,XX
17	SOLUÇÃO DE TOKEN PARA MFA PARA GRUPO DE 50 USUÁRIOS	20	Unidade	XX.XXX,XX	XX.XXX,XX
18	TRANSCEIVER SFP 1000Base-SX	40	Unidade	XX.XXX,XX	XX.XXX,XX
19	TRANSCEIVER SFP+ 10GBase-SR	20	Unidade	XX.XXX,XX	XX.XXX,XX
20	TRANSCEIVER SFP+ 10GBase-LR	10	Unidade	XX.XXX,XX	XX.XXX,XX
21	TRANSCEIVER QSFP+ 40GBase-SR4	10	Unidade	XX.XXX,XX	XX.XXX,XX
22	BANCO DE HORAS TÉCNICAS	1000	Horas Técnicas	XX.XXX,XX	XX.XXX,XX
23	UNIDADES DE SERVIÇOS TÉCNICOS (UST) PARA INSTALAÇÃO, CONFIGURAÇÃO E HANDS ON	500	UST	XX.XXX,XX	XX.XXX,XX
PREÇO GLOBAL ESTIMADO (R$)					**XX.XXX,XX**

1.2. São anexos a este instrumento e vinculam esta contratação, independentemente de transcrição:

1.2.1. O Termo de Referência que embasou a contratação e eventuais anexos;

1.2.2. O Edital do Pregão Eletrônico nº XXXX/2026; e

1.2.3. A Proposta do contratado e eventuais anexos.

2. VIGÊNCIA

2.1. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. A prorrogação prevista nos arts. 106 e 107 da Lei nº 14.133/2021 aplica-se apenas às parcelas de natureza contínua, não alcançando os itens de entrega única. Os prazos de garantia, suporte, atualização e licenciamento observarão as disposições específicas previstas no Termo de Referência.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando ainda para o cumprimento dos seguintes requisitos:

2.2.1. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.2.2. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.2.3. Haja manifestação expressa do contratado informando o interesse na prorrogação;

2.2.4. Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. A Administração deverá atestar a cada novo exercício financeiro, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção;

2.6. A administração poderá extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

3. MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAL

3.1. Os critérios referentes ao modelo de execução e de gestão contratual do objeto estão definidos nos itens 5 e 6, respectivamente, do Termo de Referência.

4. DESCRIÇÃO DA SOLUÇÃO DO OBJETO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

4.1. A descrição da solução como um todo, encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice do Termo de Referência.

5. PREÇO E CONDIÇÕES DE PAGAMENTO

5.1. **Preço:**

5.1.1. O valor total do contrato é de R$ XXXXXX (XXXXXXX);

5.1.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.1.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados.

5.2. **Condições de Pagamento:**

5.3. A forma, o prazo e demais condições para o pagamento à contratada estão definidos no Termo de Referência.

6. DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO (REAJUSTE E REVISÃO)

Do Reajuste:

6.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de 01 (um) ano, contado da data do orçamento estimado.

6.2. Após o interregno de um ano mencionado no item anterior os preços iniciais serão reajustados, mediante a aplicação do Índice de Custo da Tecnologia da Informação (ICTI), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.3. É dever e responsabilidade exclusiva da Contratada a apresentação do pedido de reajuste junto à Administração Pública, por escrito, anexando a memória de cálculo e a documentação pertinente que demonstre a variação dos custos.

6.4. O pedido deve ser apresentado a partir da data em que se completar o período de 12 (doze) meses, durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão do direito ao reajuste do período anterior.

6.5. Caso o índice, no momento da prorrogação, ainda não tenha sido publicado oficialmente, a contratada deve manifestar o interesse expresso quanto ao reajuste, ficando a seu cargo a demonstração analítica dos valores quando da efetiva publicação do índice.

6.6. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

6.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

6.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.9. O reajuste será realizado por meio de apostilamento.

Da Revisão:

6.10. O reequilíbrio por meio de revisão de preços dar-se-á em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizam a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato. A base para cálculo da revisão retroagirá até a data do fato que a motivou e deverá ser formalizada por termo aditivo próprio.

6.11. Ficará a cargo da contratada a demonstração da necessidade de revisão nos preços contratados, devendo encaminhar os pedidos devidamente fundamentados e justificados, com documentos de comprovação de suas alegações e planilhas com os novos valores, podendo ainda a contratante fazê-lo, unilateralmente, quando verificar as ocorrências descritas no item 6.10, com as devidas justificativas.

7. OBRIGAÇÕES DO CONTRATANTE

7.1. Exigir o cumprimento de todas as obrigações assumidas pelo contratado, de acordo com o contrato e seus anexos;

7.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência e que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

7.3. Notificar o contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas, conforme o caso;

7.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo contratado;

7.5. Efetuar o pagamento ao contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato;

7.6. Aplicar ao contratado as sanções motivadas pela inexecução total ou parcial do Contrato;

7.7. Cientificar o órgão de representação judicial do Estado do Amapá para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado, quando for o caso;

7.8. Explicitamente emitir decisão 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.

a) Concluída a instrução do requerimento, a Administração terá o prazo de 1 (um) mês para decidir, admitida a prorrogação motivada por igual período.

7.9. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais, caso possua.

7.10. A Administração não responderá por quaisquer compromissos assumidos pelo contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do contratado, de seus empregados, prepostos ou subordinados.

7.11. Nomear gestor e fiscais técnico, administrativo e requisitante do contrato, conforme o contrato, para acompanhar e fiscalizar a execução do contrato;

7.12. Encaminhar formalmente a demanda por meio de nota de empenho, ordem de fornecimento ou outro instrumento equivalente, de acordo com os critérios estabelecidos neste termo de referência;

7.13. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

7.14. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;

7.15. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

8. OBRIGAÇÕES DO CONTRATADO

8.1. O contratado deverá cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e observando, ainda, as obrigações a seguir dispostas:

8.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/2021);

8.3. Alocar os empregados necessários, com habilitação, vestuários e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência, respeitando as normas referentes à segurança e medicina do trabalho;

8.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

8.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros por dolo ou culpa de seus representantes legais, prepostos ou empregados, não reduzindo essa responsabilidade a fiscalização ou ao acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

8.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou de agente público que atue na fiscalização ou na

gestão do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

8.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, no prazo de 05 dias, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal, Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

8.8. Comunicar ao Fiscal do contrato, imediatamente, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

8.9. Prestar todo esclarecimento ou informação solicitada pelo contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

8.10. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

8.11. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

8.12. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

8.13. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

8.14. Não permitir a utilização de qualquer trabalho do menor de dezesseis 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;

8.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação, ou para qualificação, na contratação direta, quando for o caso;

8.16. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

8.17. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

8.18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

8.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

8.20. A contratada deverá respeitar as Normas e Legislação Ambiental regulamentadoras pertinentes, em especial, quanto a devida destinação final dos resíduos gerados e quanto a poluição sonora.

8.21. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8.22. Indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

8.23. Propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

8.24. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

8.25. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

8.26. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e

as bases de dados à Administração;

8.27. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

9. OBRIGAÇÕES PERTINENTES À LGPD

9.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

9.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

9.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

9.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de sub-operação firmados ou que venham a ser celebrados pelo Contratado.

9.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

9.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

9.7. O Contratado deverá exigir de sub operadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

9.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

9.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

9.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

9.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

9.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

9.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

10. GARANTIA DE EXECUÇÃO DO OBJETO

10.1. Da garantia da execução do objeto:

10.1.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133, de 2021, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

10.1.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

10.1.2.1. caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

10.1.2.2. seguro-garantia;

10.1.2.3. fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.

10.1.2.4. título de capitalização custeado por pagamento único, com resgate pelo valor total.

10.1.3. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ser apresentada, no prazo máximo até a data de assinatura do contrato, bem como deverá ter validade durante toda a execução do contrato e por mais 90 (noventa) dias após o término da vigência contratual, e ainda, permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas. A garantia, nas demais modalidades como caução em dinheiro ou

em títulos da dívida pública, títulos de capitalização e fiança bancária, deverão ser prestadas em até 10 dias úteis após a assinatura do contrato.

10.1.3.1. A apólice do seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal, mediante a emissão do respectivo endosso pela seguradora.

10.1.4. Caso utilizada outra modalidade de garantia, somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada/corrigida monetariamente através da variação do índice da poupança.

10.1.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

10.1.6. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.1.6.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

10.1.6.2. multas moratórias e punitivas aplicadas pela Administração à contratado; e

12.1.6.3. obrigações trabalhistas e previdenciárias de qualquer natureza, verbas rescisórias e obrigações para com o FGTS não adimplidas pelo contratado.

10.1.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

10.1.8. A garantia em dinheiro deverá ser efetuada em favor da Contratante, a qual deverá ser depositada, mediante "Depósito Identificado" com o CNPJ da empresa, na conta abaixo indicada:

BANCO DO BRASIL
AGÊNCIA Nº 3575-0 (Agência Setor Público)
CONTA CORRENTE Nº 5.217-5 (TJAP – Caução de Licitação)

10.1.8.1. A realização da restituição à empresa da caução depositada, somente ocorrerá após a certificação pela fiscalização de que os serviços foram executados fielmente e será corrigida monetariamente, devendo a contratada informar a conta bancária para devolução;

10.1.9. 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 Economia.

10.1.10. No caso de garantia na modalidade de fiança bancária, 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.

10.1.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

10.1.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o contratado obriga-se a fazer a respectiva reposição no prazo máximo de 5 (cinco) dias úteis, contados da data em que for notificada.

10.1.13. O contratante executará a garantia na forma prevista na legislação que rege a matéria.

10.1.14. Será considerada extinta a garantia com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

10.1.15. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao contratado.

10.1.16. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no Edital e no Contrato.

11. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

11.1.1. der causa à inexecução parcial do contrato;

11.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

11.1.3. der causa à inexecução total do contrato;

11.1.4. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

11.1.5. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

11.1.6. praticar ato fraudulento na execução do contrato;

11.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

11.1.8. praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

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

11.2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

11.2.1. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei).

11.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 11.1.2, 11.1.3 e 11.1.4 do item acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito do Estado do Amapá, pelo prazo máximo de 3 (três) anos. (art. 156, §4º, da Lei).

11.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 11.1.5, 11.1.6, 11.1.7, 11.1.8 e 11.1.9 do item acima deste Contrato, bem como nos subitens 11.1.2, 11.1.3 e 11.1.4, que justifiquem a imposição de penalidade mais grave do que a descrita no item 11.2.2, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos. (art. 156, §5º, da Lei).

11.2.4. Multa:

11.2.4.1. moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, limitada a 30 dias, não podendo ultrapassar o percentual de 30% do valor total do contrato;

11.2.4.2. moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando houver.

a) O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

11.2.4.3. Compensatória, para as infrações descritas nos subitens 11.1.5 a 11.1.9, entre 0,5% e 25% do valor do contrato, conforme a gravidade.

11.2.4.4. Compensatória entre 0,5% e 30% sobre o valor total do contrato, conforme a gravidade, no caso de inexecução total do objeto.

11.2.4.5. Compensatória entre 0,5% e 5% do valor do contrato, conforme a gravidade, para infração descrita no subitem 11.1.1.

11.2.4.6. Compensatória entre 0,5% e 10% do valor do contrato, conforme a gravidade, para infração descrita no subitem 11.1.2.

11.2.4.7. Compensatória entre 0,5% e 15% do valor do contrato, conforme a gravidade, para infração descrita no subitem 11.1.4.

11.3. O valor da multa aplicada será:

11.3.1. retido dos pagamentos devidos pela Administração;

11.3.2. pago por meio de depósito bancário na conta do Tribunal Justiça do Amapá;

11.3.3. descontado do valor da garantia prestada; ou

11.3.4. cobrado judicialmente.

Parágrafo Primeiro. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo contratante ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º).

Parágrafo Segundo. Excepcionalmente, desde que devidamente justificado pelo gestor do contrato no processo administrativo, o Tribunal poderá, ad cautelam, efetuar a retenção do valor da multa presumida, conforme determinações previstas no instrumento convocatório ou no contrato, e instaurar de imediato o procedimento administrativo, que deverá ter tramitação prioritária.

Parágrafo Terceiro. Quando houver provimento da defesa prévia, do recurso ou reconsideração da decisão que aplicar a penalidade, os valores retidos cautelarmente serão devolvidos ao interessado.

Parágrafo Quarto. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

Parágrafo Quinto. Quando o contratado já tiver sofrido Advertência e reincidir na prática do mesmo ato, poderá receber nova advertência, cumulada com multa.

11.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à contratante (art. 156, §9º).

11.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

11.6. Na aplicação das sanções serão considerados (art. 156, §1º):

11.6.1. a natureza e a gravidade da infração cometida;

11.6.2. as peculiaridades do caso concreto;

11.6.3. as circunstâncias agravantes ou atenuantes;

11.6.4. os danos que dela provierem para o contratante;

11.6.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.6.6. a reincidência.

11.7. Antes da aplicação de qualquer das sanções tipificadas nos subitens 11.2.1 a 11.2.4, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.8. Da decisão que aplicar as sanções previstas nos subitens 11.2.1 a 11.2.4, caberá recurso administrativo no prazo de 15 (quinze) dias úteis, contado da data da intimação.

11.9. Concluído o julgamento e mantida a penalidade aplicada, o processo retornará à Comissão, que certificará o trânsito em julgado administrativo, procedendo à publicação da decisão no Diário de Justiça Eletrônico e registrando as sanções nos sistemas próprios.

11.10. O Tribunal não arcará com eventuais despesas relacionadas às provas solicitadas pelo licitante ou pelo contratado.

11.10.1. As provas propostas pelo licitante ou pelo contratado, quando forem ilícitas, impertinentes, desnecessárias ou protelatórias, poderão ser recusadas, mediante decisão fundamentada.

11.11. Na contagem dos prazos, excluir-se-á o dia do início e incluir-se-á o do vencimento.

11.11.1. Os prazos fluirão a partir do primeiro dia útil após o recebimento da intimação.

11.11.2. O prazo considerar-se-á prorrogado até o primeiro dia útil seguinte se o vencimento ocorrer no sábado, domingo ou feriado, e quando não houver expediente no TJAP.

11.12. 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 nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

11.13. A personalidade jurídica do contratado 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 o contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160).

11.14. O contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161).

11.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei nº 14.133/21.

11.16. Demais disposições quanto aos procedimentos e aplicabilidade das sanções à contratada serão feitas e decididas conforme a INSTRUÇÃO NORMATIVA Nº 119/2024-GP/TJAP, que regulamenta o procedimento de apuração de infrações e aplicação de sanções administrativas aos licitantes e contratados, nos termos da Lei Federal nº 14.133, de 1º de abril de 2021, no âmbito do Tribunal de Justiça do Estado do Amapá.

12. DA EXTINÇÃO CONTRATUAL

12.1. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

12.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

12.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

12.3.1. ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

12.3.2. poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

12.4. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

12.4.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

12.4.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

12.4.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

12.5. O termo de extinção, sempre que possível, será precedido:

12.5.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.5.2. Relação dos pagamentos já efetuados e ainda devidos;

12.5.3. Indenizações e multas.

12.6. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

12.7. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau.

13. DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados na Lei Orçamentária Anual do exercício atual, conforme dotação orçamentária abaixo discriminada:

13.1.1. O valor total de R$ XXXXXX (XXXXXXXX), será custeado através da nota de empenho nº XXXXXX, programa de trabalho nº XXXXXXXX, elemento de despesa nº XXXXXXXXX, fonte XXXXXX.

13.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes.

14. DA SUBCONTRATAÇÃO

14.1. Não será admitida a subcontratação do objeto do contrato.

15. DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021 e demais normas aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos, bem como normas internas do TJAP.

16. ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. Registros que não caracterizam alteração do contrato poderão ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/2021.

17. PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no Diário de Justiça Eletrônico do TJAP.

18. FORO

18.1. É eleito o Foro da Comarca de Macapá para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/2021.

18.2. Com fundamento no § 4º do art. 784 do CPC, fica dispensada a assinatura de testemunhas quando o contrato for assinado no SEI ou por qualquer modalidade de assinatura eletrônica prevista em lei, quando sua integridade for conferida por provedor de assinatura.

Macapá-AP, *data da assinatura eletrônica*.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ
CNPJ sob o nº 34.870.576/0001-21
Desembargador JAYME HENRIQUE FERREIRA
Presidente
CONTRATANTE

Empresa XXXXXXXXXXXXXXX
CNPJ nº XXXXXXXXXXXXX
Representante Legal XXXXXXXXXXXXX
CONTRATADA

ANEXO VIII - MODELO DE PROPOSTA

MODELO DE PROPOSTA

Razão social:

Cnpj:

Endereço:

E-mail:

Contato telefônico:

Número de whatsapp:

Dados bancários (banco, agência e conta corrente):

Nome do representante legal da empresa:

[Sugere-se um texto de apresentação]

Objeto:

Item	Descrição	Marca / Modelo	Unidade	Quantidade	Valor unitário	Subtotal
Total						

O valor da proposta deve incluir todos os eventuais custos de frete, mão de obra, taxas, impostos, seguros, encargos sociais, administração, trabalhistas, previdenciários, contribuições fiscais e outros que venham a incidir sobre o objeto do Termo de Referência.

Validade da proposta: 90 dias.

Município-UF, dia de mês de ano

Assinatura

ANEXO IX - DECLARAÇÃO DE INEXISTÊNCIA DE NEPOTISMO

DECLARAÇÃO DE INEXISTÊNCIA DE NEPOTISMO

(Resolução CNJ nº 7/2005, art. 2º, VI)

Razão Social (ou Nome Empresarial):
CNPJ:
Endereço:
Representante legal:

Na qualidade de representante legal da pessoa jurídica acima identificada, **DECLARO**, ao **TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ**, para fins de atendimento ao disposto na Resolução do Conselho Nacional de Justiça nº 7, de 18 de outubro de 2005, especialmente o art. 2º, VI, e para que produza seus jurídicos e legais efeitos, que:

Não há, no quadro societário (sócios/acionistas) desta empresa cônjuge, companheiro(a) ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, nem de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação do presente certame, circunstância vedada pelo art. 2º, VI, da Resolução CNJ nº 7/2005.

Tenho ciência de que a configuração de quaisquer das hipóteses acima caracteriza prática de nepotismo, sujeitando a empresa e seus responsáveis às consequências legais e administrativas cabíveis, inclusive inabilitação/impedimento, rescisão contratual, aplicação de sanções previstas na Lei nº 14.133/2021 e demais normas aplicáveis, sem prejuízo das responsabilidades civil e penal.

Comprometo-me a comunicar imediatamente (no máximo em cinco dias úteis) à Administração qualquer alteração superveniente no quadro societário que possa enquadrar-se nas hipóteses vedadas, ciente de que a omissão ou falsidade sujeita esta empresa às sanções legais.

Para fins de transparência, declaro que **INEXISTEM** situações enquadráveis como nepotismo nos termos acima.

Declaro, por fim, que li e compreendi o conteúdo desta declaração e que as informações prestadas são verdadeiras, estando ciente das penalidades previstas em lei para o caso de falsidade.

Local e data:

Assinatura: