EDITAL

CONTRATAÇÃO Nº 264/2026

PREGÃO ELETRÔNICO Nº 91.286/2026

Processo Administrativo nº E:41506.0000000158/2026

Torna-se público que a **AGÊNCIA DE MODERNIZAÇÃO DA GESTÃO DE PROCESSOS - AMGESP**, por meio da **COMISSÃO PERMANENTE DE LICITAÇÃO** designados pela **Portaria nº 279/2026**, publicada no Diário Oficial do Estado de Alagoas em 20 de agosto de 2026, sediada na Avenida Walter Ananias, nº. 35 - A, Jaraguá - Maceió - AL - CEP 57025-510 realizará licitação, por registro de preço, na modalidade **PREGÃO**, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto n° 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

Valor total da contratação: R$ 49.491.654,52 (quarenta e nove milhões quatrocentos e noventa e um mil seiscentos e cinquenta e quatro reais e cinquenta e dois centavos)

Data da sessão pública: 16/11/2026.

Horário: 09h - horário de Brasília.

Critério de Julgamento: menor preço, por grupo de itens.

Modo de disputa: aberto.

Preferências ME/EPP/Equiparadas: sim.

Local: Sistema de Compras do Governo Federal (www.gov.br/compras).

1. DO OBJETO

1.1. O objeto da presente licitação é o **registro de preços para futura e eventual CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE CIBERSEGURANÇA, NA MODALIDADE SAAS (SOFTWARE AS A SERVICE),** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formado por 09 (nove) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste certame 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).

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

3.3. 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.

3.4. 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.

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

3.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

3.7. Não poderão disputar esta licitação:

3.7.1. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.7.2. Sociedade que desempenhe atividade incompatível com o objeto da licitação;

3.7.3. Sociedades cooperativas;

3.7.4. Empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

3.7.5. 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;

3.7.6. 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;

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

3.7.8. 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;

3.7.9. Empresas controladoras, controladas ou coligadas, nos termos da lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

3.7.10. 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;

3.7.11. Organizações da sociedade civil de interesse público - oscip, atuando nessa condição;

3.8. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, 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.

3.9. O impedimento de que trata o item 3.7.7 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.

3.10. A critério da administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.7.5 e 3.7.6 poderão 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.

3.11. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.12. O disposto nos itens 3.7.5 e 3.7.6 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.

3.13. 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, de 2021.

3.14. A vedação de que trata o item 3.10 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.

4. DO ORÇAMENTO ESTIMADO

4.1. O orçamento estimado da presente contratação não será de caráter sigiloso.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

5.2. 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.

5.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 9.1.1 e 9.13.2 deste Edital.

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

5.4.1. 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;

5.4.2. 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;

5.4.3. 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;

5.4.4. 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.

5.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

5.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

5.6.1. No item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

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

5.7. Não poderá se beneficiar do tratamento jurídico diferenciado estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, a pessoa jurídica:

5.7.1. De cujo capital participe outra pessoa jurídica;

5.7.2. Que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

5.7.3. De cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado nos termos da Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.4. Cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada pela Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.5. Cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;

5.7.6. Constituída sob a forma de cooperativas, salvo as de consumo;

5.7.7. Que participe do capital de outra pessoa jurídica;

5.7.8. Que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

5.7.9. Resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

5.7.10. Constituída sob a forma de sociedade por ações.

5.7.11. Cujos titulares ou sócios guardem, cumulativamente, com o contratante do serviço, relação de pessoalidade, subordinação e habitualidade.

5.8. O licitante deverá declarar em campo próprio do sistema que desenvolve programa de integridade, nos termos do Decreto nº 12.304, de 2024, e da Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025, para fazer jus ao benefício do critério de desempate previsto no art. 60, caput, inciso IV, da Lei nº 14.133, de 2021.

5.9. A falsidade da declaração de que trata os itens 5.4, 5.6 ou 5.8 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

5.10. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

5.11. 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.

5.12. 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.

5.13. 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:

5.13.1. 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

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

5.14. 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:

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

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

5.15. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 5.13 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.

5.16. 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.

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

6. DO PREENCHIMENTO DA PROPOSTA

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

6.1.1. Valor unitário e total do item;

6.1.2. Marca;

6.1.3. Fabricante;

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

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

6.3. 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.

6.4. 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.

6.5. 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.

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

6.7. 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.

6.8. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

6.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

6.10. Caso o critério de julgamento seja o de menor preço, os licitantes devem respeitar os preços máximos previstos no Termo de Referência/Projeto Básico;

6.11. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no Termo de Referência/Projeto Básico.

6.12. O descumprimento das regras supramencionadas pode ensejar a responsabilização pelo Tribunal de Contas da União 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.

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

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

7.2. 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.

7.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro/Agente de Contratação/Comissão e os licitantes.

7.4. 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.

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

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

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. 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).

7.9. 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.

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

7.11. Caso seja adotado para o envio de lances o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem de

classificação, sem prejuízo da aplicação da margem de preferência e do desempate ficto, conforme disposto neste edital, quando for o caso.

7.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o Pregoeiro/Agente de Contratação/Comissão, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

7.12. Caso seja adotado para o envio de lances o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

7.12.1. 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.

7.12.2. 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.

7.12.3. Caso o item em disputa envolva objeto abrangido por margem de preferência, o percentual referido na disposição anterior será de 20%, nos termos do § 6º do artigo 24 da Instrução Normativa SEGES/ME nº 73, de 30 de setembro de 2022, incluído pela Instrução Normativa SEGES/MGI nº 79, de 12 de setembro de 2024.

7.12.4. 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.

7.12.5. 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.

7.13. Caso seja adotado para o envio de lances o modo de disputa "fechado e aberto", poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

7.13.1. Caso o item em disputa envolva objeto abrangido por margem de preferência, o percentual referido na disposição anterior será de 20%, nos termos do § 5º do artigo 25 da Instrução Normativa SEGES/ME nº 73, de 30 de setembro de 2022, incluído pela Instrução Normativa SEGES/MGI nº 79, de 12 de setembro de 2024.

7.13.2. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 7.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

7.13.3. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.13.4. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.13.5. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

7.13.6. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o Pregoeiro/Agente de Contratação/Comissão, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.13.7. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

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

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

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

7.17. No caso de desconexão com o Pregoeiro/Agente de Contratação/Comissão, no decorrer da etapa competitiva da licitação, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.18. Quando a desconexão do sistema eletrônico para o Pregoeiro/Agente de Contratação/Comissão 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/Agente de Contratação/Comissão aos participantes, no sítio eletrônico utilizado para divulgação.

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

7.20. Ao final da fase de lances, será aplicado o benefício da margem de preferência, nos termos do art. 26 da Lei nº 14.133, de 2021.

7.20.1. Para produtos ou serviços abrangidos por margem de preferência normal ou adicional, caso a proposta de menor preço não tenha por objeto produto ou serviço contemplado pela referida margem, o sistema automaticamente indicará as propostas de produtos ou serviços que façam jus ao diferencial de preço, pela ordem de classificação, para fins de aceitação pelo Pregoeiro/Agente de Contratação/Comissão/Agente de Contratação/Comissão.

7.20.2. Nestas situações, a proposta beneficiada pela aplicação da margem de preferência normal ou adicional, conforme o caso, tornar-se-á a proposta classificada em primeiro lugar.

7.21. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial, caso a contratação não se enquadre nas vedações dos §§1º e 2º do art. 4º da Lei nº 14.133, de 2021. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21.1. Quando houver propostas beneficiadas com as margens de preferência, apenas poderão se valer do critério de desempate previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, as propostas de microempresas e empresas de pequeno porte que também fizerem jus às margens de preferência (art. 5º, §9º, I, do Decreto nº 8538, de 2015).

7.21.2. O parâmetro para o empate ficto, nesse caso, consistirá no preço ofertado pela fornecedora classificada em primeiro lugar em razão da aplicação da margem de preferência.

7.21.3. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 10% (dez por cento), caso se trate de uma concorrência, ou de até 5% (cinco por cento), caso se trate de um pregão, serão consideradas empatadas com a primeira colocada.

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

7.21.5. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de até 10% (dez por cento), caso se trate de uma concorrência, ou de até 5% (cinco por cento), caso se trate de um pregão, na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

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

7.21.7. Nas licitações que prevejam cota reservada destinada à contratação de microempresas e empresas de pequeno porte, não havendo vencedor para a cota reservada, esta poderá ser adjudicada ao vencedor da cota principal; em caso de recusa deste, a adjudicação será ofertada aos licitantes remanescentes, observada a ordem de classificação, desde que pratiquem o preço do primeiro colocado da cota principal.

7.21.8. A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

7.22. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

7.22.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

7.22.1.1. Bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

7.22.1.2. Bens e serviços com tecnologia desenvolvida no País; e

7.22.1.3. Bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

7.22.2. Os licitantes classificados que estejam enquadrados no item 7.22.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

7.22.3. Caso a preferência não seja exercida na forma do item 7.22.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 7.22.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 7.22.1.3 caso esse direito não seja exercido.

7.22.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

7.23. 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.

7.24. 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:

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

7.24.1.2. Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, nos termos do Decreto nº 11.430, de 2023, e da Instrução Normativa SEGES/MGI nº 382, de 17 de setembro de 2025;

7.24.1.3. Declaração do licitante de que desenvolve programa de integridade, conforme Decreto n° 12.304, de 2024, e Portaria Normativa SE/CGU n° 226, de 9 de setembro de 2025.

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

7.24.2.1. Empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

7.24.2.2. Empresas brasileiras;

7.24.2.3. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

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

7.25. 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, vedado qualquer outro processo.

7.26. 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/Agente de Contratação/Comissão poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

7.26.1. Tratando-se de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade e serão observados como critério de aceitabilidade os preços unitários máximos definidos no Termo de Referência.

7.26.2. 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.

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

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

7.26.5. 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.

7.26.6. É facultado ao Pregoeiro/Agente de Contratação/Comissão prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.27. Após a negociação do preço, o Pregoeiro/Agente de Contratação/Comissão iniciará a fase de aceitação e julgamento da proposta.

8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o Pregoeiro/Agente de Contratação/Comissão 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, de 2021, legislação correlata e no item 3.7 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.1.1. SICAF;

8.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;

8.1.3. Cadastro Nacional de Empresas Punidas – CNEP e

8.1.4. Lista de licitantes inidôneos, mantida pelo Tribunal de Contas da União.

8.2. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

8.2.1. A consulta no CEIS quanto às sanções previstas na Lei nº 8.429, de 1992, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

8.3. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas ao CEIS, CNEP e Lista de licitantes inidôneos pela Consulta Consolidada de Pessoa Jurídica do TCU.

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

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

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

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

8.5. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

8.6. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs ou tenha se valido da aplicação da margem de preferência, o Pregoeiro/Agente de Contratação/ Comissão verificará se o licitante faz jus ao benefício aplicado.

8.6.1. Caso o licitante não venha a comprovar o atendimento dos requisitos para fazer jus ao benefício da margem de preferência, as propostas serão reclassificadas, para fins de nova aplicação da margem de preferência.

8.7. Verificadas as condições de participação e de utilização do tratamento favorecido, o Pregoeiro/Agente de Contratação/Comissão 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 nos arts. 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

8.8. Será desclassificada a proposta vencedora que:

8.8.1. Contiver vícios insanáveis;

8.8.2. Não obedecer às especificações técnicas contidas no termo de referência;

8.8.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

8.8.4. Não tiverem sua exequibilidade demonstrada, quando exigido pela administração;

8.8.5. Não cumpra os critérios de aceitabilidade de preços definidos no termo de referência;

8.8.6. Apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável.

8.9. 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.

8.10. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro/Agente de Contratação/Comissão, que comprove:

8.10.1.1. Que o custo do licitante ultrapassa o valor da proposta; e

8.10.1.2. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

8.11. 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.

8.12. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

8.12.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos

preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semi-integrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

8.12.2. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

8.12.3. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

8.12.4. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

8.13. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha 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;

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

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

8.16. 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.

8.17. Concluída a etapa final de lances, as empresas licitantes deverão ajustar suas propostas, apresentando os valores unitários e totais com a limitação de duas casas decimais após a vírgula, desconsiderando as duas últimas casas decimais adicionais. Caso seja necessário proceder ao arredondamento, este deverá ser efetuado para o valor imediatamente inferior, vedada a adoção de valor superior ao lance final apresentado.

8.18. Caso o Termo de Referência exija a apresentação de carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor, o licitante classificado em primeiro lugar deverá apresentá-la, sob pena de não aceitação da proposta.

8.19. 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.

8.20. 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.

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

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

8.23. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro/Agente de Contratação/Comissão 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.

8.24. Quando os itens estiverem dispostos em grupo de itens (lote), o critério de julgamento adotado será aplicado individualmente a cada item que o integre, não podendo qualquer deles ultrapassar a pesquisa de mercado que fundamenta a estimativa da Administração. Após a tentativa de negociação, será desclassificado o licitante que mantiver proposta com itens cujos valores unitários permaneçam superiores à referida estimativa.

9. DA FASE DE HABILITAÇÃO

9.1. 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.

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

9.2. 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.

9.3. 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.

9.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

9.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

9.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou por com declaração do licitante de sua autenticidade.

9.6. 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.

9.7. 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.

9.8. 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.

9.9. 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.

9.10. Considerando que na presente contratação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

9.10.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado pelo e-mail: klinsmanamgesp@gmail.com, o agendamento deverá ocorrer com antecedência mínima de 02 (dois) dias úteis e deverá ser solicitado com no máximo 3 (três) dias úteis de antecedência da data do certame, a vistoria será acompanhada por servidor técnico designado para esse fim, em horário de expediente (08h às 18h), de modo que seu agendamento não coincida com o agendamento de outros licitantes.

9.10.2. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

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

9.11.1. 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.

9.12. 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.

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

9.13. A verificação pelo Pregoeiro/Agente de Contratação/Comissão, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

9.13.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do Pregoeiro/Agente de Contratação/Comissão.

9.13.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.

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

9.14.1. 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.

9.14.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

9.14.3. Encerrado o prazo para envio da documentação de que trata o item 9.13.1, poderá ser admitida, mediante decisão fundamentada do Pregoeiro, a apresentação de novos documentos de habilitação ou a complementação de informações acerca dos documentos já apresentados pelos licitantes, em até 2 (duas) horas para:

9.14.4. A aferição das condições de habilitação do licitante, desde que decorrentes de fatos existentes à época da abertura do certame;

9.14.5. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

9.14.6. Suprimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante;

9.14.7. Suprimento da ausência de certidão e/ou documento de cunho declaratório expedido por órgão ou entidade cujos atos gozem de presunção de veracidade e fé pública.

9.15. Findo o prazo assinalado sem o envio da nova documentação, restará preclusa essa oportunidade conferida ao licitante, implicando sua inabilitação.

9.16. 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.

9.17. Na hipótese de o licitante não atender às exigências para habilitação, o Pregoeiro/Agente de Contratação/Comissão 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 disposto no subitem 9.13.1.

9.18. 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.

9.19. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação.

9.20. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

10. DO TERMO DE CONTRATO

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

10.2. 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.

10.3. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá: a)

disponibilizar acesso ao sistema de processo eletrônico para que seja assinado digitalmente em até 05 (cinco) dias úteis; ou b) outro meio eletrônico, assegurado o prazo de 05 (cinco) dias úteis para resposta após recebimento da notificação pela Administração.

10.4. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida ao fornecedor adjudicado, implica o reconhecimento de que:

10.4.1. Referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

10.4.2. A contratada se vincula à sua proposta e às previsões contidas neste Edital;

10.4.3. A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

10.5. Os prazos dos itens 10.2 e 10.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

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

10.7. Na assinatura do contrato ou instrumento equivalente será exigido o Cadastro Informativo de Créditos não Quitados do Setor Público Federal – Cadin e a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

10.7.1. A existência de registro no Cadin constitui fator impeditivo para a contratação.

11. DA ATA DE REGISTRO DE PREÇOS

11.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 5 (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.

11.2. 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:

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

11.2.2. a justificativa apresentada seja aceita pela Administração.

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

11.4. 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.

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

11.6. 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.

11.7. 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.

11.8. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

11.9. Em caso de prorrogação da ata, poderá ser renovado o quantitativo originalmente registrado.

12. DA FORMAÇÃO DO CADASTRO DE RESERVA

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

12.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação e excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 26 da Lei nº 14.133, de 2021; e

12.1.2. dos licitantes que mantiverem sua proposta original.

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

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

12.2.2. 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.

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

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

12.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

12.4. 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:

12.4.1. 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

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

13. DOS RECURSOS

13.1. 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.

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

13.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

13.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

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

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

13.3.4. 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.

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

13.5. 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.

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

13.7. 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.

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

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

13.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico Sistema Eletrônico de Informações do Estado de Alagoas – SEI! Alagoas (https://portal.sei.al.gov.br/).

14. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

14.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Pregoeiro/Agente de Contratação/Comissão/a durante o certame;

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

14.1.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

14.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

14.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

14.1.2.4. Deixar de apresentar amostra;

14.1.2.5. Apresentar proposta ou amostra em desacordo com as especificações do edital;

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

14.1.4. 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;

14.1.5. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

14.1.6. Fraudar a licitação;

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

14.1.7.1. Agir em conluio ou em desconformidade com a lei;

14.1.7.2. Induzir deliberadamente a erro no julgamento;

14.1.7.3. Apresentar amostra falsificada ou deteriorada;

14.1.8. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação

14.1.9. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

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

14.2.1. Advertência;

14.2.2. Multa;

14.2.3. Impedimento de licitar e contratar e

14.2.4. 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.

14.3. Na aplicação das sanções serão considerados:

14.3.1. A natureza e a gravidade da infração cometida.

14.3.2. As peculiaridades do caso concreto

14.3.3. As circunstâncias agravantes ou atenuantes

14.3.4. Os danos que dela provierem para a Administração Pública

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

14.4. A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

14.4.1. Para as infrações previstas nos itens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0,5% a 3,2% do valor do contrato licitado.

14.4.2. Para as infrações previstas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8, 14.1.9 e 14.1.9, a multa será de 15% a 30% do valor do contrato licitado.

14.5. 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.

14.6. 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.

14.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 14.1.1, 14.1.2, 14.1.3 e 14.1.4, 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.

14.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8 e 14.1.9, bem como pelas infrações administrativas previstas nos itens 14.1.1, 14.1.2 e 14.1.3 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 nº 14.133, de 2021

14.9. 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 14.1.3, 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, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

14.10. 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.

14.11. 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.

14.12. 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.

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

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

14.15. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

14.15.1. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicaf serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

15. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

15.1. 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.

15.2. 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.

15.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo e-mail: klinsmanamgesp@gmail.com, ou por petição dirigida ou protocolada na Avenida Walter Ananias, n.º 35A – Jaraguá, CEP: 57025-510 – Maceió/AL.

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

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

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

16. DAS DISPOSIÇÕES GERAIS

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

16.2. 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/Agente de Contratação/Comissão.

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

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

16.5. 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.

16.6. 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.

16.7. 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.

16.8. 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.

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

16.10. Em caso de divergência entre as especificações, unidades de medida, condições ou demais exigências dos itens licitados constantes do Portal Comprasnet e aquelas previstas no Termo de Referência, prevalecerão, para todos os fins, as disposições contidas no Termo de Referência.

16.11. O “Quadro de Avisos” disponibilizado no Portal Comprasnet possui caráter instrutório e vinculante, integrando o presente Edital para todos os fins e efeitos, devendo ser integralmente observado pelos licitantes.

16.12. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP).

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

14.11.1 ANEXO A – Modelo de Proposta Final;

14.11.2. ANEXO B – Minuta de Ata de Registro de Preços;

14.11.3. ANEXO C – Minuta de Termo de Contrato;

14.11.4. ANEXO D – Termo de Referência;

14.11.4.1. ANEXO I – Apêndice I - Especificação dos itens e requisitos;

14.11.4.2. ANEXO II – Apêndice II - Escopo para Prova de Conceito (PoC);

14.11.4.3. ANEXO III – Apêndice III - Matriz de Riscos;

14.11.4.4. ANEXO IV – Apêndice IV - Acordo de nível de serviço (ANS/SLA);

14.11.4.5. ANEXO V – Apêndice V - Inventário de ativos (base de cálculo);

14.11.4.6. ANEXO VI – Apêndice VI - Modelo de Ordem de Serviço (OS);

14.11.4.7. ANEXO VII – Apêndice VII - Termo de Ciência e Compromisso de Sigilo (NDA);

14.11.4.8. ANEXO VIII – Apêndice VIII- Modelo de Relatório Mensal de Nível de Serviço (RNS);

14.11.4.9. ANEXO IX – Apêndice IX - Declaração de adequação à LGPD e compromisso de tratamento seguro de dados pessoais;

14.11.4.10. ANEXO X – Apêndice X - Modelo de Proposta de Preços.

14.11.5. Apêndice do Anexo D – Estudo Técnico Preliminar.

Maceió (AL), 26 de outubro de 2026.

LUYZA RAPHAELA TENORIO VITORINO:12111734454 2026.10.26 09:28:14 -03'00'

Luyza Raphaela Tenório Vitorino

Assessora de Apoio de Contratação

Ruan Klinsman Colácio Da Silva

Pregoeiro Responsável

ANEXO A - MODELO DE PROPOSTA FINAL

Razão Social da Licitante: .....

CNPJ: .....

Endereço:.....

CEP .....

Telefone: ..... E-Mail: .....

As planilhas de quantitativos e custos conterão as descrições dos produtos que compõem a solução proposta, incluindo as respectivas quantidades, unidades, preços unitários e totais gerais, expressos em reais (R$).

ITEM	**DESCRIÇÃO**	**Marca e modelo:**	Unid.	Qnt.	**PREÇO expresso em R$**	
					UNITÁRIO	TOTAL
01	XXXXXXXXXX		Unidade	XX		
TOTAL GERAL						

PRAZO DE ENTREGA E EXECUÇÃO: A execução dos serviços de segurança cibernética estará condicionada à emissão de Ordem de Serviço (OS) pela Fiscalização do Contrato (Conforme Termo de Referência), de acordo com as necessidades da Administração.

VALIDADE DA PROPOSTA: O Prazo de Validade desta Proposta é de 60 (sessenta) dias corridos, contados a partir da data da abertura deste Certame.

PRAZO DE PAGAMENTO: A licitante **DECLARA** que acatará o pagamento da Administração conforme definido na minuta contratual, ANEXO C deste Edital.

CONTA BANCÁRIA: Banco XXXXX, Agência XXXX, Conta Corrente XXXXX.

Declaro:

1) que estão incluídas nesta proposta comercial, as despesas com todos os impostos, taxas, encargos sociais, encargos fiscais, desembaraço aduaneiro, encargos previdenciários e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto da licitação.

2) que estou de acordo com todas as normas e condições deste Edital e seus anexos

ANEXO B – MINUTA DE ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS Nº (...)/(20...)

Processo Administrativo nº E:41506.0000000158/2026

A **Agência de Modernização da Gestão de Processos – AMGESP**, UASG: 925998 com sede na Avenida Walter Ananias, n.º 35A – Jaraguá, CEP: 57025-510 – Maceió/AL, inscrita no CNPJ/MF sob o nº 07.424.905/0001-38, neste ato representada pelo seu Diretor-Presidente, **Sr. Amilton Barbosa Silva**, nomeado pela decreto nº 86.124, de 01 de Janeiro de 2023, publicada no DOE/AL de 01 de Janeiro de 2023, portador da matrícula funcional nº 163-5, considerando o julgamento da licitação na modalidade de Pregão, na forma eletrônica, para REGISTRO DE PREÇOS AMGESP - **PREGÃO/ANO**, publicada no Portal Nacional de Contratações Públicas em XX de XXX de 2026, e no Diário Oficial do Estado de Alagoas em XX de XXX de 2026, referente ao Processo Administrativo nº E:41506.0000000158/2026, RESOLVE registrar os preços da empresa indicada e qualificada nesta ATA, de acordo com a classificação por ela alcançada e na quantidade cotada, atendendo às condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual **CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE CIBERSEGURANÇA**, especificado(s) no(s) item(ns) nº XXX do Termo de Referência anexo do Edital de Licitação nº **PREGÃO/ANO**, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Fornecedor: CNPJ:, Inscrição Estadual:, sediada na : , CEP: , Telefone: , E-mail: , representado pelo Sr. (a): , Inscrito (a) no CPF: , sob o RG n°:.							
Item	CATMAT/ CATSER	Descrição	Unidade de Medida	Quantidade	Marca / Modelo	Valor Unitário (R$)	Valor Total (R$)
(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)

(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)
(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)
VALOR TOTAL: R$ XXXXXX (XXXXXX).							

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. DO ÓRGÃO OU ENTIDADE GERENCIADORA EPARTICIPANTES

3.1. São órgãos e entidades públicas participantes do registro de preços:

ITEM	UNIDADE DE COMPRA	ÓRGÃO	REQUISIÇÃO MÍNIMA PARA UTILIZAÇÃO DE ATA	REQUISIÇÃO MÁXIMA PARA UTILIZAÇÃO DE ATA	TOTAL
XXX	XX	XXX	**10%**	**50%**	**XXX**
XXX	XX	XXX	**10%**	**50%**	**XXX**

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. 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:

4.1.1. Apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. Demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. Consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da Ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da Ata de Registro de Preços.

4.5. O órgão ou a entidade poderá aderir a item da Ata de Registro de Preços da qual sejaintegrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1.

Dos limites para as adesões

4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na Ata de Registro de Preços para o gerenciador e para os participantes.

4.7. 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 gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à Ata de Registro de Preços.

4.8. A adesão à Ata de Registro de Preços por órgãos e entidades da Administração Pública distrital e municipal poderá ser exigida para fins de transferências voluntárias.

Vedação a acréscimo de quantitativos

4.9. É vedado efetuar acréscimos nos quantitativos fixados na Ata de Registro de Preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado apartir do primeiro dia útil subsequente à data de divulgação no Portal Nacional de Contratações Públicas – PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1. O contrato decorrente da Ata de Registro de Preços terá sua vigência estabelecida no próprio instrumento contratual 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.

5.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgãoou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho ded espesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

5.2.1. O instrumento contratual de que trata o item 5.2. deverá ser assinado no prazo de validade da Ata de Registro de Preços.

5.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

5.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da Ata de Registro de Preços:

5.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no Edital ou no Aviso de Contratação Direta e se obrigar nos limites dela;

5.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.2.2. Mantiverem sua proposta original.

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

5.5. O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.7.1. Quando o licitante vencedor não assinar a Ata de Registro de Preços, no prazo e nas condições estabelecidos no Edital ou no Aviso de Contratação Direta; e

5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da Ata de Registro de Preços.

5.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a Ata de Registro de Preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A Ata de Registro de Preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.11. Quando o convocado não assinar a Ata de Registro de Preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.7, 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.

5.12. Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital ou do aviso de contratação direta, poderá:

5.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13. 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.

6. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. 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:

6.1.1. 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 da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

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

6.1.3. Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. 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.

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos eàs 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, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. 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.

7.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da Ata de Registro de Preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.2 e no item 7.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora 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, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1. As quantidades previstas para os itens com preços registrados na Ata de Registro de Preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

8.2. O remanejamento somente poderá ser feito:

8.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

8.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos para as adesões.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

9. CANCELAMENTO DO REGISTRO DO FORNECEDOR E DOS PREÇOS REGISTRADOS

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da Ata de Registro de Preços, sem motivo justificado;

9.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3. Não aceitar manter seu preço registrado, na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Leinº 14.133, de 2021.

9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da Ata de Registro de Preços, poderá o órgão ou a entidade gerenciadora, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada Ata de Registro de Preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado se tornar superior ou inferior ao preço registrado.

10. DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital ou no aviso de contratação direta.

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do 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 ou entidade participante, caso no qual caberá ao respectivo órgão ou entidade participante a aplicação da penalidade.

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, anexo ao edital ou ao aviso de contratação direta.

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 02 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelo órgão ou entidade gerenciadora e fornecedor(es) e encaminhada, por cópia, aos Órgãos Participantes.

Maceió (AL), em (...) de (...) de (...).

_____

ÓRGÃO GERENCIADOR

_____

FORNECEDOR

_____

FORNECEDOR

_____

FORNECEDOR

(...)

TESTEMUNHA CPF Nº

TESTEMUNHA CPF Nº

ANEXO

Cadastro Reserva

Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais ao adjudicatário:

Fornecedor: (...razão social, CNPJ/MF, endereço, contatos, representante...)						
Item	Descrição	Unidade de Medida	Quantidade	Valor (R$) ou Percentual de Desconto (%)	Requisição Mínima	Requisição Máxima
(...)	(...)	(...)	(...)	(...)	(...)	(...)
(...)	(...)	(...)	(...)	(...)	(...)	(...)

Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Fornecedor: (...razão social, CNPJ/MF, endereço, contatos, representante...)						
Item	Descrição	Unidade de Medida	Quantidade	Valor (R$) ou Percentual de Desconto (%)	Requisição Mínima	Requisição Máxima
(...)	(...)	(...)	(...)	(...)	(...)	(...)
(...)	(...)	(...)	(...)	(...)	(...)	(...)

ANEXO C– MINUTA DE TERMO DE CONTRATO

TERMO DE CONTRATO (...) Nº (...)/(20...), QUE ENTRE SI CELEBRAM O(A)(...ESTADO DE ALAGOAS, POR INTERMÉDIO DA(O)(...ÓRGÃO...),/AUTARQUIA/FUNDAÇÃO. ..) E A EMPRESA (...),PARA A CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE CIBERSEGURANÇA.

CONTRATANTE: O(A)(...Estado de Alagoas, por intermédio da(o) (...órgão...),/Autarquia/Fundação...), inscrita(o) no CNPJ sob o nº (...) e com sede na (...endereço...), representado(a) pelo (...cargo do ordenador de despesas...), Sr. (...nome...), nomeado pelo(a)(...Decreto/Portaria...)nº (...), de (...) de (...) de 20(...), publicado(a) no DOE/AL de (...) de (...) de 20(...), portador da matrícula funcional nº (...);

CONTRATADO: A empresa (...nome...), inscrita no CNPJ sob o nº (...), com sede na (...endereço...) e com o seguinte endereço eletrônico (...@...), representada pelo seu (...cargo do representante legal...), Sr. (...nome...), de acordo com a representação legal que lhe é outorgada por (...procuração/contrato social/estatuto social...), inscrito no CPF sob o nº (...);

Os CONTRATANTES, em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e aos preceitos de direito público, aplicados, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, inclusive Lei nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor, celebram o presente contrato, decorrente do processo administrativo nº 41506.0000000158/2026 e do Pregão nº (...), mediante as cláusulas e condições a seguir:

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de **CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE CIBERSEGURANÇA**, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de **12 (doze) meses** contados da contados da data de sua assinatura, prorrogável para até 120 (cento e vinte) meses, na forma do art. 114 da Lei n° 14.133, de 2021

2.2. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação e nos demais aspectos que forem julgados relevantes, atentando, ainda, para o cumprimento dos seguintes requisitos:

2.2.1. Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

2.2.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.2.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.2.4. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

2.2.5. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação; e

2.2.6. Não haja registro no Cadastro Informativo de créditos não quitados do setor público federal (Cadin).

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. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando o CONTRATADO tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. As regras sobre a subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor mensal da contratação é de R$ **xxxxxx** (**xxxxxxxxx**), perfazendo o valor total de R$ **xxxxxx** (**xxxxxxxxx**).

5.2. 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.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA - PAGAMENTO

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1. As regras acerca do reajuste do valor contratual são aquelas definidas no Termo de Referência, anexo a este Contrato.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do CONTRATANTE:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o CONTRATADO, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando

prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo CONTRATADO;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao CONTRATADO do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao CONTRATADO as sanções previstas na lei e neste Contrato;

8.1.8. Não praticar atos de ingerência na administração do CONTRATADO, tais como:

8.1.8.1. indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

8.1.8.2. fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo CONTRATADO;

8.1.8.3. estabelecer vínculo de subordinação com funcionário do CONTRATADO;

8.1.8.4. definir forma de pagamento mediante exclusivo reembolso dos salários pagos;

8.1.8.5. demandar a funcionário do CONTRATADO a execução de tarefas fora do escopo do objeto da contratação; e

8.1.8.6. prever exigências que constituam intervenção indevida da Administração na gestão interna do CONTRATADO.

8.1.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo CONTRATADO;

8.1.10. 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;

8.1.10.1. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo CONTRATADO no prazo máximo de 30 (trinta) dias;

8.1.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

8.1.13. Comunicar o CONTRATADO na hipótese de posterior alteração do projeto pelo CONTRATANTE, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.2. 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.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O CONTRATADO deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo CONTRATANTE, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.5. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

9.5.1. prova de regularidade relativa à Seguridade Social;

9.5.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

9.5.3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do CONTRATADO;

9.5.4. Certidão de Regularidade do FGTS – CRF; e

9.5.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

9.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE e não poderá onerar o objeto do contrato;

9.7. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;

9.8. 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;

9.9. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.10. 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;

9.11. 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;

9.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.13. 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;

9.14. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE;

9.15. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados;

9.16. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos;

9.17. Fornecer todos os materiais, equipamentos, ferramentas e utensílios demandados, em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação de regência;

9.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;

9.19. 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;

9.20. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

9.21. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

9.22. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

9.23. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 12 de junho de 2008;

9.24. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

9.25. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato;

9.25.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.26. 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 tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133, de 2021;

9.27. 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 contrato;

9.28. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

9.29. Assegurar aos seus trabalhadores ambiente de trabalho e instalações em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho;

9.30. Fornecer equipamentos de proteção individual (EPI) e equipamentos de proteção coletiva (EPC), quando for o caso;

9.31. Garantir o acesso do CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.32. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;

9.33. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

9.34. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo o CONTRATADO relatar ao CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

9.35. Realizar os serviços de manutenção e assistência técnica no(s) seguinte(s) local(is) ... (inserir endereço(s));

9.36. Realizar 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 dos serviços;

9.37. Ceder ao CONTRATANTE todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do CONTRATADO.

9.37.1. Considerando que o projeto contratado se refere a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão dos direitos a que se refere o subitem acima inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação da obra.

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. 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.

10.2. 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.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. 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.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. 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.

10.10. 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.

10.10.1. 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.

10.11. 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.

10.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no Termo de Referência, anexo a este Contrato.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os arts. 138 e 139 da mesma Lei.

13.5.2. 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.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido de:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. 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.

13.8. O CONTRATANTE poderá ainda:

13.8.1. nos casos de obrigação de pagamento de multa pelo CONTRATADO, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

13.8.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do CONTRATADO decorrentes do contrato.

13.9. 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 que 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 (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

14.2. 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.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.4. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do CONTRATANTE, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês.

14.5. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

15. CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

I) Gestão/Unidade: [...];
II) Fonte de Recursos: [...];
III) Programa de Trabalho: [...];
IV) Elemento de Despesa: [...];
V) Plano Interno: [...];
VI) Nota de Empenho: [...];

15.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

16. CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais 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.

17. CLÁUSULA DÉCIMA SÉTIMA – 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 respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

18. CLÁUSULA DÉCIMA OITAVA– FORO

18.1. Fica eleito o foro da comarca de Maceió, Alagoas para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Para firmeza e validade do pactuado, este termo de contrato foi lavrado em 2 (duas) vias de igual teor e forma, o qual, depois de lido e achado em ordem, vai assinado pelos Contratantes.

Maceió (AL), em (...) de (...) de (...).

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

ANEXO D – TERMO DE REFERÊNCIA;

ANEXO I – APÊNDICE I - ESPECIFICAÇÃO DOS ITENS E REQUISITOS;

ANEXO II – APÊNDICE II - ESCOPO PARA PROVA DE CONCEITO (POC);

ANEXO III – APÊNDICE III - MATRIZ DE RISCOS;

ANEXO IV – APÊNDICE IV - ACORDO DE NÍVEL DE SERVIÇO (ANS/SLA);

ANEXO V – APÊNDICE V - INVENTÁRIO DE ATIVOS (BASE DE CÁLCULO);

ANEXO VI – APÊNDICE VI - MODELO DE ORDEM DE SERVIÇO (OS);

ANEXO VII – APÊNDICE VII - TERMO DE CIÊNCIA E COMPROMISSO DE SIGILO (NDA);

ANEXO VIII – APÊNDICE VIII- MODELO DE RELATÓRIO MENSAL DE NÍVEL DE SERVIÇO (RNS);

ANEXO IX – APÊNDICE IX - DECLARAÇÃO DE ADEQUAÇÃO À LGPD E COMPROMISSO DE TRATAMENTO SEGURO DE DADOS PESSOAIS;

ANEXO X – APÊNDICE X - MODELO DE PROPOSTA DE PREÇOS.

APÊNDICE DO ANEXO D – ESTUDO TÉCNICO PRELIMINAR.

INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS

Termo de Referência 4/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
4/2026	926217-INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	FELIPE GOMES ATHAYDE	27/05/2026 18:42 (v 0.6)
Status			
ASSINADO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	40/2026	E:41506.0000000158/2026

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de Solução Integrada de Cibersegurança, na modalidade SaaS (Software as a Service), compreendendo licenciamento de plataforma unificada de segurança, monitoramento contínuo (SOC 24x7), gestão de vulnerabilidades e conformidade à LGPD, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE ÚNICO						
Item	**Especificação**	**CATSER /CATMAT**	**Métrica ou Unidade de Medida**	**Quantidade**	**Valor Unitário**	**Valor Total**
1	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Plataforma Unificada de Cibersegurança (Core)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual /Ativo	4.430	R$ 520,14	R $ 2.304.220,20
2	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:**	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:**	18.099	R$ 397,92	R $ 7.201.954,08

	Inteligência e Proteção de Marca (OSINT/EASM)		Assinatura Anual (Por Dominio e e-mail)			
3	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Proteção de Endpoint (EDR/XDR)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual /Endpoint	4.430	R$ 392,75	R $ 1.739.882,50
4	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Segurança de Web e Containers (CS /KSPM)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual /Node	56	R$ 24.774,00	R $ 1.387.344,00
5	**Descrição CATMAT:** Módulo eletrônico Tipo: Token Modelo: Chip Criptográfico Uso: Usb Aplicação: Armazenamento De Certificado Digital Características Adicionais: Homologado Para Chaves: Tipo Rsa 2048 Bits; Certif **Descrição complementar:** Chaves de Hardware (FIDO2)	485464	**Unidade de medida CATMAT:** Unidade	108	R$ 661,28	R$ 71.418,24
6	**Descrição CATSER:**	26999		36	R$ 467.806,00	R $ 16.841.016,00

	Serviços de Gerenciamento de Redes de Tecnologia da Informação e Comunicação (TIC) **Descrição complementar:** Operação de Segurança (SOC) e Suporte 24x7		**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Mês			
7	**Descrição CATSER:** Treinamento Informática - Sistema / Software **Descrição complementar:** Implantação, Integração e Treinamento	3840	**Unidade de medida CATSER:** Hora **Unidade de Medida complementar:** Hora Técnica	1.700	R$ 752,83	R $ 1.279.811,00
8	**Descrição CATSER:** Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC) **Descrição complementar:** Gestão de Vulnerabilidades e Apoio à Remediação	27014	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Mês	36	R$ 473.712,00	R $ 17.053.632,00
9	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Controle de Acesso à Rede (NAC)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual /Disp.	3.370	R$ 478,45	R $ 1.612.376,50

1.2. Estimativas de consumo individualizadas, do órgão gerenciador e órgão(s) e entidade(s) participante(s).

					REQUISIÇÃO MÍNIMA	**REQUISIÇÃO MÁXIMA**	

ITEM	UNIDADE DE MEDIDA	DETRAN	ITEC	SSP	PARA UTILIZAÇÃO DA ATA	PARA UTILIZAÇÃO DA ATA	TOTAL A LICITAR
01	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Licença Anual /Ativo	1.000	1.430	2.000	10%	50%	4.430
02	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Assinatura Anual (Por Dominio e email)	600	17.499	0	10%	50%	18.099
03	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Licença Anual /Endpoint	1.000	1.430	2.000	10%	50%	4.430
04	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Licença Anual /Node	15	11	30	10%	50%	56

05	Unidade de m e d i d a CATMAT: Unidade	20	38	50	10%	50%	108
06	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Mês	12	12	12	10%	50%	36
07	Unidade de m e d i d a CATSER: Hora **Unidade de M e d i d a complementar:** Hora Técnica	300	600	800	10%	50%	1.700
08	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Mês	12	12	12	10%	50%	36
09	Unidade de m e d i d a CATSER: Unidade **Unidade de M e d i d a complementar:** Licença Anual /Disp.	1.120	2.250	0	10%	50%	3.370

1.2.1. Em atendimento ao art. 9°, do Decreto Estadual n° 95.019/2023, cumpre destacar a possibilidade de participação de outros órgãos ou entidades da Administração Pública no presente procedimento.

Classificação do objeto quanto à heterogeneidade ou complexidade

1.3. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.

Classificação do objeto quanto ao modelo de execução

1.4. O serviço é enquadrado como continuado, tendo em vista que a operação de segurança cibernética e o monitoramento contra ameaças cibernéticas são atividades essenciais e ininterruptas para a garantia da proteção da infraestrutura de TI e dos dados do Governo do Estado, sendo a vigência plurianual indispensável para a manutenção do baseline de defesa e conformidade legal.

Prazo de vigência

1.5. Tratando-se de contratação que prevê operação continuada de sistemas estruturantes de tecnologia da informação, o prazo de vigência da contratação é de 12 (doze) meses, prorrogável para até 120 meses, contados da data de sua assinatura, na forma do artigo 114 da Lei n° 14.133, de 2021.

1.6. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se pela necessidade crítica de elevar a maturidade da segurança da informação do Governo do Estado, mitigando os riscos crescentes de incidentes cibernéticos que ameaçam a integridade, a disponibilidade e a confidencialidade dos dados sob custódia da Administração Pública. A atual infraestrutura de TIC do ITEC-AL, caracterizada pela coexistência de sistemas legados, ambientes virtualizados, contêineres e dispositivos IoT, demanda uma abordagem de defesa em profundidade (Defense-in-Depth) que apenas uma plataforma unificada pode prover. A fragmentação operacional, resultante da utilização de ferramentas isoladas, tem criado pontos cegos que dificultam a detecção rápida de ameaças e o Tempo Médio de Resposta (MTTR) a incidentes. Desta forma, a solução integrada permitirá a automação de processos de segurança, a orquestração de respostas a ataques de Ransomware e DDoS, e a visibilidade centralizada exigida para a conformidade com as políticas estaduais de segurança cibernética, garantindo a continuidade dos serviços essenciais ao cidadão e a preservação do ativo de informação governamental.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme consta das informações básicas deste termo de referência.

2.5. O objeto da contratação também está alinhado com o Planejamento Estratégico do ITEC, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
1.1.	Aprimorar as ações de Transformação Digital no Governo de Alagoas, fortalecendo a governança e capacidade digital, incrementando a eficiênciana prestação de serviços públicos e satisfação dos cidadãos.
3.2.	Elevar o nível de eficiência e eficácia dos projetos desenvolvidos pela organização, aumentando a capacidade de entrega de valor para os clientes.

2.6. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.[A3]

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em no apêndice I deste Termo de Referência.

3.2. A solução de TIC consiste na prestação de serviços continuados de Segurança Cibernética Gerenciada, estruturada por meio de uma plataforma unificada de Defesa Ativa, Visibilidade e Segurança Ofensiva. A solução integra, em um ecossistema coeso, tecnologias de proteção de endpoints (EDR /XDR), gerenciamento de vulnerabilidades, inteligência de ameaças externas (OSINT/Dark Web) e controle de acesso a rede (Zero Trust), visando garantir a resiliência da infraestrutura tecnológica, a detecção preditiva de vetores de ataque, a contenção automatizada de incidentes e a proteção de dados críticos. O ciclo de vida do objeto abrange desde o licenciamento de software na modalidade Software as a Service (SaaS), a implantação técnica e a parametrização em ambientes legados, até a operação assistida por um Centro de Operações de Segurança (SOC) especializado 24x7 e o suporte contínuo à remediação de falhas.

3.3. Plataforma Unificada de Gestão e Governança (Core)
A plataforma atua como o eixo central de gerenciamento, consolidando dados telemétricos provenientes de todas as camadas defensivas da organização, endpoints, nuvem e contêineres. Sua finalidade é prover uma visão holística e unificada do risco cibernético organizacional por meio de um Risk Score dinâmico, facilitando a governança e o atendimento aos requisitos de auditoria e conformidade. O sistema consolida a gestão de ativos e permite a orquestração de respostas a incidentes (SOAR) e a guarda de evidências com integridade baseada em Blockchain, conferindo validade técnica e jurídica aos relatórios gerados, em conformidade com o Art. 369 do Código de Processo Civil.

3.4. Inteligência, Defesa Ativa e Segurança Ofensiva
O ciclo de vida da solução prevê, ainda, uma camada de inteligência e validação contínua, a proteção contra ameaças externas e o monitoramento da Dark Web (OSINT) estendem o perímetro de segurança para além da rede física, enquanto a segurança de contêineres garante que a modernização tecnológica não abra novas brechas em ambientes de nuvem. O controle de acesso (NAC) atua na borda física e lógica, aplicando os princípios Zero Trust para restringir o acesso a dispositivos IoT e visitantes, enquanto as chaves de hardware (FIDO2) elevam a segurança da identidade corporativa, eliminando o risco de phishing nos acessos administrativos. A segurança ofensiva (Pentest automatizado e DDoS) promove o teste de estresse contínuo da resiliência dos serviços, permitindo que a organização corrija falhas antes da exploração por agentes maliciosos.

3.5. Gestão do Ciclo de Vida da Vulnerabilidade e Resposta (SOC/Blue Team)
A solução compreende a operação humana integrada, garantindo que a tecnologia contratada seja operada por especialistas de segurança, o serviço de SOC realiza o monitoramento ininterrupto e a triagem de alertas, enquanto o serviço de gestão de vulnerabilidades atua no lifecycle preventivo (análise, priorização e apoio técnico à correção). Esta abordagem garante que a organização não apenas detete uma vulnerabilidade ou invasão, mas possua a capacidade técnica para operacionalizar o patching, a mitigação de riscos e a validação posterior do ambiente (Rescan), fechando o ciclo de detecção-resposta-correção.

3.6. Implantação, Integração e Capacitação
Para assegurar a sustentabilidade da contratação, o ciclo de vida do objeto contempla serviços especializados de implantação e transferência de conhecimento, esta fase garante a integração técnica com o legado tecnológico da contratante, assegurando que sistemas operacionais obsoletos e infraestruturas críticas não percam visibilidade ou segurança durante a adoção da nova plataforma. O treinamento oficial certificado, integrado ao suporte técnico continuado, capacita a equipe da instituição na operação das ferramentas de defesa, na escrita de playbooks de automação e na governança da privacidade de dados, assegurando a independência do órgão na gestão do ecossistema de segurança cibernética a longo prazo.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio, visando mitigar riscos operacionais, garantir a continuidade dos serviços públicos e a proteção do patrimônio informacional do Estado:

4.1.1 Assegurar a implementação das medidas técnicas e administrativas aptas a proteger os dados pessoais e sensíveis sob custódia da Administração contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação, em estrita observância ao disposto no art. 46 da Lei nº 13.709/2018 (LGPD).

4.1.2 Prover à Alta Gestão e às equipes técnicas visibilidade completa e monitoramento em tempo real de todos os ativos de TIC (físicos, virtuais, em nuvem e contêineres), permitindo a quantificação da exposição a vulnerabilidades através de métricas de Risk Score dinâmico, fundamentando a tomada de decisão baseada em riscos reais e não apenas em percepções subjetivas.

4.1.3 Otimizar a operação de segurança através da automação de tarefas repetitivas (orquestração via SOAR), reduzindo a fadiga de alertas da equipe técnica e assegurando capacidade de resposta rápida, padronizada e coordenada frente a incidentes cibernéticos complexos, como ataques de Ransomware e tentativas de exfiltração de dados.

4.1.4 Garantir a integridade e disponibilidade dos sistemas de missão crítica do órgão, inclusive aqueles baseados em arquiteturas legadas que não podem ser descontinuadas imediatamente, assegurando que o monitoramento de segurança seja extensível a todos os ativos da rede sem degradar o desempenho das aplicações de negócio.

4.1.5 Implementar processos contínuos de capacitação e validação de resiliência dos colaboradores, minimizando a superfície de ataque decorrente de engenharia social (phishing) e promovendo uma cultura organizacional de proteção de dados e cibersegurança.

4.1.6 Assegurar a rastreabilidade integral de todas as ações de segurança e administração da plataforma por meio de trilhas de auditoria imutáveis (via tecnologia Blockchain/Hashchain), fornecendo evidências técnicas com validade jurídica necessárias para o atendimento a órgãos de controle, auditorias externas e processos de fiscalização.
Requisitos de Capacitação

4.2. A solução deve incluir um programa de capacitação técnica inicial e continuada para os administradores, operadores técnicos (SOC) e gestores de segurança da informação da Contratante, visando a transferência integral de conhecimento para o uso autônomo, eficaz e seguro da plataforma.

4.3. O fornecedor deve disponibilizar trilhas de aprendizagem específicas para cada perfil de usuário, com a obrigatoriedade de emissão de certificados de conclusão para os participantes que atingirem os requisitos de aproveitamento definidos no plano de treinamento.

4.4. O programa de capacitação deverá contemplar, no mínimo, as seguintes competências técnicas:

4.4.1 Configuração de dashboards, gestão de inventário de ativos, parametrização de varreduras de vulnerabilidades e interpretação do Risk Score.

4.4.2 Capacitação na interpretação de alertas de endpoints, utilização da matriz MITRE ATT&CK para análise contextual de ameaças e técnicas avançadas de Threat Hunting.

4.4.3 Treinamento para o desenvolvimento, testes e implantação de novos Playbooks de automação de resposta a incidentes, visando a redução do MTTR.

4.4.4 Metodologias para a correta triagem, priorização de falhas de segurança e acompanhamento do ciclo de remediação até a validação final (Rescan).

4.4.5 Operação das ferramentas de simulação (DDoS e Phishing) e interpretação de relatórios analíticos gerados por Inteligência Artificial.

4.5. A Contratada deverá realizar workshops técnicos periódicos, no mínimo semestrais, para garantir que a equipe da Contratante esteja atualizada sobre novas funcionalidades incorporadas à plataforma, além de novas técnicas de invasão e tendências de ameaças cibernéticas (como Ransomware e ataques de dia zero).

4.6. Deverá ser fornecida, em língua portuguesa, toda a documentação técnica atualizada, incluindo guias de operação (User Guides), manuais de arquitetura, documentação de APIs, tutoriais de troubleshooting e materiais educativos para conscientização de usuários finais (pílulas de aprendizado sobre Phishing e engenharia social).

4.7. Os treinamentos deverão ser ministrados por instrutores certificados no produto, sendo aceitas modalidades presenciais, remota (ao vivo) ou EaD, desde que garantida a interação técnica para esclarecimento de dúvidas. A Contratada deverá disponibilizar um ambiente de homologação (laboratório) que replique a topologia da Contratante para a realização das atividades práticas (hands-on).

4.8. Caso o treinamento proposto utilize plataformas de ensino a distância, o acesso aos conteúdos gravados e aos materiais de apoio deve ser garantido aos servidores da Contratante durante toda a vigência contratual.

Requisitos Legais

4.9. O processo de contratação e a execução do objeto devem observar rigorosamente a legislação pátria vigente, com destaque para:

4.9.1 Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos): Observância aos princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência e planejamento, além do estrito cumprimento das regras de parcelamento do objeto, matriz de riscos e fiscalização contratual.

4.9.2 Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD): A Contratada obriga-se a tratar os dados pessoais e as informações sensíveis da Contratante em estrita conformidade com os princípios e fundamentos da LGPD, adotando medidas de segurança, técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas.

4.9.3 Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022: Atendimento integral às diretrizes para o processo de contratação de soluções de Tecnologia da Informação e Comunicação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

4.9.4 Decreto nº 11.856, de 26 de dezembro de 2023 (Política Nacional de Cibersegurança - PNCiber): A solução deve estar alinhada com as diretrizes da PNCiber, visando promover a resiliência das infraestruturas críticas, a detecção proativa de ameaças e o fortalecimento da capacidade de resposta a incidentes cibernéticos no âmbito da Administração Pública.

4.9.5 Lei nº 12.846, de 1º de agosto de 2013 (Lei Anticorrupção): A Contratada declara, para os fins da Lei Anticorrupção, que não pratica e não praticará, direta ou indiretamente, atos contra a Administração Pública nacional ou estrangeira, adotando práticas de integridade e ética corporativa.

4.9.6 Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021: Observância aos procedimentos de pesquisa de preços para aquisição de bens e contratação de serviços.
Requisitos de Manutenção

4.10. Dada a natureza dinâmica e a criticidade da solução, a Contratada deverá prestar serviços de manutenção contínua, abrangendo as vertentes corretiva, adaptativa e evolutiva, de forma a garantir a resiliência da infraestrutura de segurança e a eficácia das medidas de proteção cibernética.

4.11. A Contratada deverá realizar, sem ônus adicional, a correção de quaisquer falhas de programação (bugs), erros de processamento, vulnerabilidades sistêmicas ou inconsistências operacionais detectadas na plataforma SaaS. Estão inclusas a aplicação contínua e transparente de patches de segurança, a atualização de feeds de inteligência de ameaças, bem como a atualização dos repositórios de testes de vulnerabilidade (NVTs), garantindo proteção imediata contra vetores de ataque Zero-Day e novas ameaças emergentes mapeadas globalmente.

4.12. A solução deverá ser mantida permanentemente atualizada com o estado da arte das tecnologias de defesa. A Contratada obriga-se a disponibilizar novas versões (releases) do software, incluindo melhorias de desempenho, otimização de algoritmos de detecção, inclusão de novos conectores de integração, bem como adequações normativas decorrentes de alterações na legislação brasileira (ex: novas normas da ANPD) ou mudanças nos frameworks de segurança de mercado (ex: revisões da matriz MITRE ATT&CK ou normas ISO/IEC).

4.13. O suporte técnico deverá ser oferecido de forma multicanal (telefone, e-mail e portal web), com atendimento disponível 24 horas por dia, 7 dias por semana (24x7x365), para incidentes críticos que afetem a segurança, a disponibilidade ou a visibilidade da plataforma.

4.13.1 O suporte de nível operacional (dúvidas de uso, ajustes de configuração, parametrização) estará disponível em horário comercial (08h às 18h), em dias úteis.

4.13.2 A Contratada deverá manter uma Base de Conhecimento técnica disponível à Contratante, contendo tutoriais de troubleshooting e guias de melhores práticas para a operação dos módulos de EDR, Vulnerabilidades e Orquestração (SOAR).

4.14. A Contratada deve garantir a disponibilidade da plataforma SaaS com índice mínimo de 99,8% (noventa e nove vírgula oito por cento) ao mês. Eventuais interrupções deverão ser prontamente comunicadas à Contratante, acompanhadas de plano de ação para restabelecimento imediato e relatório técnico de causa raiz (Root Cause Analysis - RCA) para incidentes que causem indisponibilidade superior a 1 (uma) hora.

4.15. Toda e qualquer alteração significativa na infraestrutura da plataforma SaaS (mudanças de versão ou infraestrutura) que possa causar interrupção temporária deve ser comunicada com antecedência mínima de 5 (cinco) dias úteis, devendo ser executada, preferencialmente, em janelas de manutenção acordadas com a fiscalização da Contratante, visando minimizar o impacto na operação do órgão.

Requisitos Temporais

4.16. A contratação do serviço continuado terá prazo de vigência inicial de 12 (doze) meses, contados a partir da data de sua assinatura, podendo ser prorrogada por períodos sucessivos até o limite de 120 (cento e vinte) meses, conforme o art. 108 da Lei nº 14.133/2021, mediante comprovação de vantagem e desempenho satisfatório.

4.17. A solução (incluindo o licenciamento, a instalação dos agentes, a parametrização das políticas de segurança, a integração com sistemas legados e o treinamento oficial) deverá estar completamente disponibilizada e operacional em até 45 (quarenta e cinco) dias corridos, contados a partir da Ordem de Início de Serviços (OIS), sob pena de caracterização de mora.

4.18. Em caso de renovação contratual por meio de termo aditivo, o suporte técnico e a disponibilidade da plataforma devem ser prestados de forma contínua, não sendo admitida qualquer interrupção dos serviços. Caso ocorra descontinuidade injustificada, o atraso será computado em dias corridos, ensejando as glosas e penalidades previstas neste Termo de Referência.

4.19. Na contagem dos prazos estabelecidos neste instrumento, excluir-se-á o dia do início e incluir-se-á o do vencimento. Todos os prazos citados, salvo menção contrária, serão considerados em dias corridos.

4.20. Os esclarecimentos técnicos solicitados formalmente pela fiscalização do contrato deverão ser prestados imediatamente pela Contratada, sendo o prazo limite de 6 (seis) horas úteis para demandas que envolvam análises técnicas complexas ou levantamento de dados.

4.21. Na execução dos serviços de suporte técnico e gestão de incidentes, a Contratada deverá observar os seguintes prazos máximos, contados a partir da abertura do chamado (através de sistema de ticketing oficial):

Severidade	Prazo máximo de início de atendimento (Resposta)	Prazo máximo de solução (Contorno/Resolução)

Crítica (Plataforma inacessível ou falha massiva de EDR)	30 minutos	24 horas
Alta (Falha em módulo específico ou vulnerabilidade exposta)	2 horas	2 dias úteis
Normal (Dúvidas operacionais, relatórios, ajustes de política)	4 horas	4 dias úteis
Baixa (Solicitações de melhoria ou dúvidas de interface)	8 horas	6 dias úteis

Requisitos de Segurança e Privacidade

4.22. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, e deve ser implementada e mantida em estrita observância aos controles de segurança estabelecidos na norma ISO/IEC 27001 e ISO/IEC 27002, visando assegurar a integridade, a confidencialidade e a disponibilidade do ecossistema de TI. A Contratada obriga-se a disponibilizar suporte contínuo para as seguintes ações:

4.22.1 Criptografia: Apoio e garantia da implementação de criptografia forte (padrão industrial AES-256 ou superior) para todos os dados em repouso (at rest) e protocolos de transporte seguros (TLS 1.2 ou superior) para dados em trânsito (in transit).

4.22.2 Autenticação Forte: Obrigatoriedade de suporte a autenticação com chave de hardware para todos os acessos administrativos à plataforma, com prioridade para dispositivos de autenticação física (chaves FIDO2/YubiKey), mitigando riscos de acesso indevido por captura de senhas.

4.22.3 Monitoramento de Logs: Manutenção de registros imutáveis de logs de acesso, administração e execução de comandos, os quais deverão ser disponibilizados para auditoria em tempo real, sendo vedada a exclusão ou alteração retroativa dos registros pelos operadores da solução.

4.22.4 Plano de Resposta a Incidentes: Colaboração ativa com a equipe de cibersegurança da Contratante na elaboração e execução de procedimentos operacionais de resposta a incidentes, incluindo a definição de playbooks para contenção de vazamentos e resposta a ataques de Ransomware.

4.22.5 Continuidade (Backup e DR): Suporte à implementação de políticas de backup redundante e planos de recuperação de desastres (Disaster Recovery), garantindo a persistência dos dados de segurança coletados e a disponibilidade da plataforma em casos de falhas catastróficas.

4.23. A Contratada, na qualidade de operadora de dados, deve atuar em conformidade com as diretrizes da Lei nº 13.709/2018, garantindo que o tratamento de dados pessoais realizado pelos módulos da plataforma (especialmente via SOAR e DFIR) respeite os princípios da finalidade, adequação e necessidade.:

4.23.1 As ferramentas de simulação (como o módulo de Phishing) devem possuir mecanismos nativos de anonimização ou ofuscação de dados pessoais coletados durante as campanhas, garantindo que credenciais reais digitadas erroneamente pelos usuários não sejam armazenadas ou acessíveis em texto simples.

4.23.2 A solução deve permitir a correta identificação e gestão de registros que envolvam dados pessoais, possibilitando o atendimento a solicitações de eliminação ou acesso, conforme exigido pela ANPD.

4.23.3 Caso a solução utilize nuvem para processamento, o tratamento de dados deve ocorrer em território nacional ou em jurisdições que garantam níveis de proteção de dados pessoais equivalentes aos exigidos pela legislação brasileira, sendo vedado o armazenamento de dados sensíveis fora destas condições sem autorização expressa e fundamentada da Contratante

4.24. Todos os testes de intrusão, simulações de phishing e testes de estresse (DDoS) realizados pela solução devem ser estritamente controlados, documentados e autorizados pela Contratante, não podendo causar prejuízos às operações de TI ou ao atendimento ao cidadão. O fornecedor deve garantir que a ferramenta possua mecanismos de "Parada de Emergência" (Kill Switch) para interrupção imediata de qualquer atividade ofensiva caso seja detectado desvio de comportamento ou impacto negativo não planejado na produção.

4.25. A contratante reserva-se o direito de realizar auditorias técnicas periódicas, solicitar evidências de testes de penetração na própria infraestrutura de nuvem do fornecedor (pentest do provedor do serviço SaaS) e exigir a apresentação de certificações de segurança como SOC2 Tipo II ou equivalente, visando atestar o nível de maturidade dos controles de segurança do fornecedor contratado.

Requisitos Sociais, Ambientais e Culturais

4.26. Todos os manuais, guias de operação, treinamentos e as próprias interfaces de usuário (dashboards e consoles de gestão) da solução de TIC deverão estar disponíveis, obrigatoriamente, no idioma Português do Brasil (PT-BR), com terminologia técnica clara e precisa. Caso algum componente acessório (como firmwares ou documentação de APIs de fabricantes globais) não possua versão em português, a Contratada deverá fornecer glossários técnicos ou tradução assistida dos pontos críticos de operação.

4.27. A presente contratação orienta-se pelos princípios da Agenda Ambiental na Administração Pública (A3P) e pelas diretrizes de contratações sustentáveis do Governo Federal:

4.27.1 O fornecedor de serviços SaaS deve priorizar a hospedagem da plataforma em datacenters que comprovem práticas de eficiência energética (como certificações PUE - Power Usage Effectiveness otimizadas), visando a redução da pegada de carbono resultante do processamento de dados e armazenamento de logs.

4.27.2 No que tange aos dispositivos físicos (chaves FIDO2 - Item 05), a Contratada deverá adotar práticas de logística reversa, garantindo a destinação ambientalmente adequada ao final da vida útil dos dispositivos, conforme disposto na Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos).

4.27.3 As chaves de hardware (tokens FIDO2) fornecidas devem atender às normas de restrição ao uso de substâncias perigosas em equipamentos elétricos e eletrônicos, tais como a diretriz europeia RoHS (Restriction of Hazardous Substances), comprovando a ausência de chumbo, mercúrio, cádmio e outros componentes tóxicos.

4.28. A Contratada deverá garantir condições de trabalho dignas e seguras para todos os profissionais envolvidos na prestação dos serviços, respeitando integralmente a legislação trabalhista brasileira:

4.28.1 Quando os profissionais da Contratada necessitarem realizar atividades presenciais nas dependências da Contratante, deverão pautar-se por padrões éticos, apresentar-se identificados (uso de crachá funcional) e trajar-se de forma adequada ao ambiente administrativo público.

4.28.2 A Contratada compromete-se, através de autodeclaração, apresentada junto a proposta, a promover políticas de diversidade e inclusão em seu quadro de pessoal, vedada qualquer prática discriminatória de raça, gênero, orientação sexual, credo ou origem, nos termos da legislação brasileira vigente.

4.29. A solução deverá estar em constante processo de inovação, com a Contratada mantendo o compromisso de atualizar tecnologicamente a plataforma ao longo da vigência do contrato, incorporando novos recursos de cibersegurança que permitam à Administração acompanhar a evolução das ameaças, sem que isso represente custos adicionais de licenciamento, desde que dentro das funcionalidades previstas neste Termo de Referência.

Requisitos da Arquitetura Tecnológica

4.30. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante. A solução deverá apresentar alta resiliência, disponibilidade e escalabilidade, suportando o crescimento da infraestrutura de TIC da Contratante sem a necessidade de reestruturação arquitetural.

4.31. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.32. A solução deverá ser fornecida preferencialmente na modalidade Software as a Service (SaaS), com processamento e armazenamento em ambiente de nuvem segura, exigindo-se que os Datacenters responsáveis possuam certificações de mercado (ex: ISO 27001, SOC 2 Tipo II, PCI-DSS) e garantam a soberania e a proteção dos dados governamentais conforme as diretrizes da ANPD. A infraestrutura de nuvem deve estar, preferencialmente, alocada em regiões geográficas que permitam a conformidade com a legislação nacional e baixa latência para os acessos dos usuários da Contratante.

4.33. A solução deve possuir integração nativa e bidirecional via APIs (padrão RESTful ou SOAP) para interoperabilidade total com o ecossistema tecnológico existente.

4.33.1 A plataforma deve possuir capacidade de coexistência e monitoramento de ativos legados (ex: servidores com SOs descontinuados, dispositivos de rede com protocolos restritos) sem a imposição de requisitos de hardware proprietários ou alterações disruptivas na arquitetura atual de rede.

4.33.2 A arquitetura da solução deve ser baseada em padrões abertos e amplamente adotados pela indústria, sendo vedado o uso de tecnologias proprietárias que gerem dependência tecnológica (Vendor Lock-in) ou que impossibilitem a integração com futuras ferramentas de segurança que o órgão venha a adquirir.

4.34. Qualquer adoção de tecnologia ou alteração arquitetural que impacte a topologia de rede da Contratante (como a instalação de MID Servers, Gateways de segurança ou alteração de regras de firewall em larga escala) deverá ser submetida à autorização prévia e formal da área técnica da Contratante. É vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas validadas pelo Plano de Implantação e pela Fiscalização.

4.35. A arquitetura do sistema deve ser elástica, permitindo que a Contratante expanda o número de endpoints monitorados, o volume de logs processados ou a quantidade de imagens de contêineres analisadas sem a necessidade de novas migrações complexas de plataforma. O modelo de licenciamento e a capacidade de processamento do Core devem suportar, de forma transparente, a expansão de até 25% do parque atual durante a vigência do contrato, garantindo a viabilidade técnica da ata de registro de preços (SRP).

4.36. Todos os componentes da arquitetura, incluindo eventuais coletores, sensores ou agentes, devem possuir mecanismos de comunicação cifrada (End-to-End Encryption) utilizando protocolos de transporte seguros (TLS 1.2 ou superior), com verificação de identidade dos servidores através de certificados digitais válidos, sendo vedado o tráfego de dados sensíveis de segurança em texto claro (plain-text) na rede interna ou na Internet.
Requisitos de Projeto e de Implementação

4.37. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.37.1 A execução contratual deverá ser gerenciada como um projeto formal. A Contratada deverá designar um Gerente de Projetos (GP) que atuará como líder e ponto focal, responsável pela gestão das entregas, pela interlocução entre a equipe da Contratada e a equipe da Contratante, e por garantir a qualidade técnica dos resultados em todas as fases do projeto.

4.37.2 A Contratada deverá apresentar, junto a proposta, após a etapa de lances, documento com proposta de um Plano de Implantação Detalhado, contendo todas as fases, atividades, cronograma físico-financeiro, matriz de responsabilidades, alocação de recursos humanos e materiais, mapeamento de riscos e interdependências que posteriormente, caso habilitado será revisitado em reunião de kick-off (reunião inicial), esse documento poderá ser ajustado durante a reunião e em momento posterior, em casos devidamente justificados bem como aprovados por ambas as partes.

4.37.3 Todas as atividades de projeto e deslocamento de equipe técnica (caso necessário) correrão por conta e risco da Contratada, sem ônus adicionais ou custos logísticos para a Contratante.

Requisitos de Implantação

4.38. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.38.1 Antes da configuração efetiva, a Contratada deverá realizar um levantamento detalhado do ambiente de TIC da Contratante, mapeando a superfície de ataque, realizando inventário preliminar de ativos, aferindo a volumetria de logs e identificando as integrações necessárias (ex: AD/LDAP, sistemas legados, cloud gateways).

4.38.2 A implantação compreende a ativação das subscrições SaaS, o provisionamento dos tenants, a instalação dos agentes/sensores nos endpoints e servidores, a configuração de políticas de segurança (como regras de isolamento no NAC e monitoramento de integridade - FIM), a parametrização dos módulos de detecção de ameaças e a integração com os serviços de diretório.

4.38.3 A implantação só será considerada concluída após a demonstração de funcionalidade completa com dados reais da Contratante, incluindo a realização de testes assistidos de vulnerabilidade e a validação dos alertas de segurança no painel central (cockpit).

4.38.4 Todo o ciclo de implantação, desde o diagnóstico inicial até a homologação final, deverá ser concluído no prazo máximo de 45 (quarenta e cinco) dias corridos, contados a partir da Ordem de Início de Serviço (OIS), salvo prorrogação devidamente justificada pela Contratada e formalmente aceita pela Contratante.

4.38.5 A Contratada deverá apoiar a criação e a utilização de um ambiente de homologação ou sandbox para testes de validação de políticas antes da aplicação definitiva de configurações críticas em produção, visando garantir a estabilidade dos serviços de negócio.

Requisitos de Garantia e Manutenção

4.39. O prazo de garantia contratual será de 12 (doze) meses, concomitante à vigência do contrato, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.40. A garantia da solução SaaS compreende a manutenção da disponibilidade da plataforma (Uptime mínimo de 99,8% mensal), a correção de falhas de programação (bugs), inconsistências ou erros de processamento, bem como a garantia absoluta de integridade e confidencialidade dos dados armazenados na plataforma.

4.41. Para os dispositivos de autenticação (Item 05) fornecidos, a garantia cobre defeitos de fabricação e falhas de funcionamento, devendo a Contratada realizar a substituição imediata de dispositivos defeituosos, sem ônus, mediante solicitação formal.

4.42. A Contratada deve garantir que a solução receba atualizações periódicas (releases) para incorporação de novas funcionalidades, melhorias de desempenho e, obrigatoriamente, adequações a novas exigências legais ou regulatórias (ex: novas normas da ANPD) que surjam durante a vigência contratual.

4.43. A Contratada deverá aplicar patches de segurança, correções de vulnerabilidades e atualizações de assinaturas de ameaças de forma contínua, garantindo proteção contra novos vetores de ataque (Zero-Day), preferencialmente em horários que não impactem a operação do órgão.
Requisitos de Experiência Profissional e Formação da Equipe

4.44. Os serviços técnicos especializados deverão ser prestados por profissionais devidamente qualificados e certificados, garantindo a excelência na execução das atividades de privacidade, segurança ofensiva, SOC e gestão de projetos. A Contratada deverá comprovar a disponibilidade da equipe técnica conforme os perfis abaixo, sendo que a apresentação destas comprovações é condição obrigatória para a Qualificação Técnica da licitante.

4.44.1 Perfil 1: Analista de Segurança Cibernética (Residente/SOC)
Atribuição: Operação do SOC, triagem de incidentes, análise de logs e uso da Plataforma (Item 01).
Formação: Curso superior completo em TIC ou Engenharia.
Certificação Obrigatória (pelo menos uma): CompTIA Security+; CySA+ (Cybersecurity Analyst); ou GSEC (GIAC Security Essentials).

4.44.2 Perfil 2: Gerente de Projetos (Gestão de Implantação)
Atribuição: Gestão do cronograma, interface com a Contratante e condução do kick-off e aceite.
Formação: Curso superior completo em TI ou área correlata.
Certificação Obrigatória: PMP (Project Management Professional) ou certificação Scrum Master (CSM) se metodologia ágil for adotada.

4.44.3 Perfil 3: Analista de SOC Nível 3 (Investigação e DFIR)
Atribuição: Investigação de incidentes críticos, perícia digital (DFIR) e orquestração (SOAR).
Formação: Curso superior completo em TI.
Certificação Obrigatória (pelo menos uma): CompTIA CySA+; ECSA (EC-Council Certified Security Analyst); ou GCIH (GIAC Certified Incident Handler).

4.44.4 Perfil 4: Especialista em Gestão de Vulnerabilidades (Blue Team)
Atribuição: Análise de vulnerabilidades, curadoria de patches e gestão de obsolescência tecnológica.
Formação: Curso superior completo em TI ou área correlata.
Certificação Obrigatória (pelo menos uma): Information Security Foundation (ISO 27001); ou CompTIA Security+; ou GPEN (GIAC Penetration Tester).

4.44.5 Perfil 5: Especialista em Testes de Intrusão (Pentester/Red Team)
Atribuição: Execução de testes de intrusão, validação da resiliência dos sistemas (DDoS) e auditoria de segurança ofensiva.
Certificação Obrigatória (pelo menos uma): OSCP (Offensive Security Certified Professional); ou CEH (EC-Council Certified Ethical Hacker) versão Practical; ou eJPT (eLearnSecurity Junior Penetration Tester).

4.44.6 Perfil 6: Arquiteto de Soluções de Segurança (Integração e Hardening)
Atribuição: Setup técnico, integração de APIs, integração com AD/LDAP, hardening de sistemas e arquitetura em nuvem.
Formação: Curso superior completo em TI ou área correlata.
Certificação Obrigatória (pelo menos uma): CISSP (Certified Information Systems Security Professional); ou certificações avançadas de nuvem (AWS Certified Security – Specialty ou Azure Security Engineer Associate).

4.45. Regras de Comprovação da Equipe Técnica

4.45.1 A licitante deverá apresentar, na fase de habilitação técnica, a relação nominal dos profissionais indicados para cada um dos perfis exigidos, acompanhada da comprovação de vínculo profissional ou de disponibilidade para a execução do objeto.

4.45.2 A comprovação de que trata o item anterior poderá ser realizada por meio de um dos seguintes documentos:
a) Cópia da Carteira de Trabalho e Previdência Social (CTPS) devidamente assinada;
b) Cópia do Contrato de Trabalho ou de prestação de serviços (quando autônomos ou consultores);
c) Contrato Social (quando o profissional for sócio da empresa licitante);
d) Declaração de Contratação Futura: Caso o profissional ainda não possua vínculo, a licitante poderá apresentar declaração formal de contratação futura, assinada pelo representante legal da empresa e pelo profissional indicado, comprometendo-se este a integrar a equipe técnica na hipótese de adjudicação do objeto em favor da licitante.

4.45.3 Além da comprovação de vínculo, a licitante deverá apresentar obrigatoriamente:
a) Currículo profissional detalhado, evidenciando a experiência compatível com o perfil pleiteado;
b) Cópia do diploma ou certificado de graduação em nível superior (ou equivalente, quando aplicável), reconhecido pelo Ministério da Educação (MEC);
c) Cópia das certificações técnicas exigidas para cada perfil (ex: CISSP, OSCP, CEH, Security+, etc.), que deverão estar vigentes e passíveis de verificação de autenticidade junto aos órgãos certificadores.

4.45.4 A Contratante reserva-se o direito de realizar entrevistas técnicas com os profissionais indicados para validar a conformidade dos conhecimentos com a realidade do ambiente de TIC da ITEC, podendo solicitar a substituição, no prazo máximo de 05 (cinco) dias úteis, de qualquer profissional que não demonstre a qualificação declarada, sem ônus para a Administração.

4.45.5 A substituição de profissionais durante a vigência contratual somente será permitida mediante prévia autorização da fiscalização, devendo o novo profissional apresentar documentação equivalente que comprove possuir qualificação técnica, formação e certificações de nível igual ou superior ao profissional substituído.

4.45.6 A falsidade de qualquer informação ou documento apresentado para a comprovação da qualificação técnica ensejará a imediata desclassificação da licitante, sem prejuízo da aplicação das sanções administrativas previstas neste Termo de Referência e na Lei nº 14.133/2021, bem como a comunicação aos órgãos de controle.

4.46. Requisitos de Idioma e Ética

4.46.1 Todos os profissionais devem ter domínio fluente do português para interface com o corpo técnico.

4.46.2 Dada a sensibilidade dos dados, toda a equipe deverá assinar Termo de Confidencialidade e Sigilo (NDA), sob pena de responsabilidade civil e criminal, conforme a natureza sensível dos dados governamentais acessados.

Requisitos de Metodologia de Trabalho

4.47. A execução dos serviços de segurança cibernética estará condicionada à emissão de Ordem de Serviço (OS) pela Fiscalização do Contrato. A OS formalizará a demanda específica, o escopo, a prioridade e o prazo de entrega, servindo como documento norteador para a medição da qualidade do serviço prestado.

4.48. O Contratado deve obrigatoriamente disponibilizar uma ferramenta de Service Desk (ou integrar-se ao ITSM da Contratante) para o registro e controle de todos os incidentes e solicitações.

4.48.1 O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 7 dias por semana por via telefônica.

4.49. Rotinas Operacionais e Accountability:

4.49.1 A Contratada deverá realizar reuniões mensais de Service Review com a equipe técnica e gestores do ITEC-AL. Nestas reuniões, serão revisados os indicadores de desempenho (SLA), a efetividade dos Playbooks de automação (SOAR), o status dos planos de remediação de vulnerabilidades e a evolução da postura de risco cibernético.

4.49.2 A entrega de relatórios mensais é obrigatória, devendo conter, minimamente: (a) relação de incidentes de segurança detectados e tempo médio de resolução (MTTR); (b) status do plano de remediação de vulnerabilidades; (c) performance dos agentes de endpoint (Item 03); (d) relatórios de conformidade e uso das chaves FIDO2.

4.49.3 Todas as configurações, regras de correlação, playbooks desenvolvidos e topologias de segurança devem ser documentados em base de conhecimento compartilhada, garantindo que o conhecimento gerado durante a execução contratual pertença à Contratante.

4.50. Metodologia de Resposta a Incidentes: O Contratado deve atuar em conformidade com as melhores práticas de mercado (ex: NIST Cybersecurity Framework ou SANS Institute).

4.50.1 Em caso de incidente cibernético, o Contratado deverá aplicar o fluxo de trabalho de Incident Response, que envolve a preparação, detecção, contenção, erradicação e, por fim, a lição aprendida (lessons learned).

4.50.2 Toda ação tomada pelos analistas do SOC (tanto automáticas via SOAR quanto manuais) deve ser registrada no histórico do chamado para fins de auditoria forense e conformidade regulatória.

4.51. Qualquer alteração na configuração dos sensores, agentes ou nas regras de detecção da Plataforma Unificada deve seguir um fluxo de gestão de mudanças aprovado previamente pela fiscalização do contrato. É vedada a implementação de regras de bloqueio (blocking mode) em ativos críticos sem prévia validação em ambiente de homologação ou autorização por escrito dos gestores da Contratante.

4.52. Ética, Sigilo e Segurança da Informação:

4.52.1 O Contratado compromete-se a tratar todas as informações de segurança (topologia, vulnerabilidades, logs de acesso, dados de negócio) como confidenciais.

4.52.2 É vedada a utilização de informações obtidas durante a execução do serviço para finalidades que não sejam a estrita execução deste objeto, sendo terminantemente proibida a comercialização, divulgação ou uso indevido de dados da Contratante.

4.52.3 O descumprimento dos requisitos de sigilo, especialmente no que tange a incidentes de privacidade detectados, sujeitará a Contratada à rescisão contratual e às penalidades previstas na LGPD.

4.53. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

Requisitos de Segurança da Informação e Privacidade

4.54. O Contratado deverá observar integralmente as normas de Segurança da Informação (SI) e Privacidade previstas na Política de Segurança da Informação (PSI) da Contratante, bem como as diretrizes da Lei nº 13.709/2018 (LGPD), obrigando-se a implementar controles técnicos e organizacionais que assegurem a integridade e a confidencialidade dos dados processados pela plataforma.

4.55. Proteção no Tratamento de Dados Pessoais:

4.55.1 A Contratada deverá limitar o acesso aos dados pessoais processados no âmbito da plataforma estritamente ao necessário para a execução do objeto contratual, é vedado o tratamento de dados pessoais para finalidades distintas das previstas neste Termo de Referência, especialmente para treinamento de algoritmos de IA de terceiros ou exploração comercial pela Contratada.

4.55.2 Sempre que os objetivos de segurança (como testes de phishing ou análises forenses) puderem ser alcançados sem a identificação do titular, a Contratada deverá aplicar técnicas de anonimização ou pseudonimização dos dados pessoais coletados.

4.55.3 A Contratada obriga-se a manter medidas de proteção contra a perda, destruição não autorizada, divulgação ou alteração de dados pessoais ou sensíveis, comunicando à Contratante, no prazo de até 24 (vinte e quatro) horas, qualquer suspeita ou ocorrência de incidente de segurança que possa resultar em risco relevante aos direitos e liberdades dos titulares.

4.56. Medidas Técnicas de Segurança:

4.56.1 Todos os dados armazenados pela plataforma (at rest) e em fluxo de rede (in transit) devem ser protegidos por protocolos de criptografia de padrão industrial (AES-256 ou superior; TLS 1.3), sendo proibida a manutenção de senhas ou chaves em texto claro.

4.56.2 O acesso dos profissionais da Contratada à plataforma deverá ser controlado por autenticação forte (FIDO2) e submetido a auditoria contínua. Toda e qualquer ação de configuração ou administração realizada pela equipe técnica da Contratada deverá ser registrada em trilha de auditoria inviolável e protegida por mecanismo de hash (Blockchain) conforme especificado no Item 01.

4.56.3 A infraestrutura de nuvem onde a solução SaaS estiver hospedada deve possuir hardening (endurecimento de segurança) certificado, garantindo que o isolamento entre tenants de diferentes clientes da Contratada seja logicamente completo, impedindo qualquer acesso cruzado de dados.

4.57. Direitos dos Titulares e Transparência:

4.57.1 Caso a solução utilize algoritmos de IA (SOAR, análise comportamental ou Risk Score) para tomada de decisão que afete funcionários ou cidadãos, a Contratada deverá garantir a "explicabilidade" dos modelos (Explainable AI), fornecendo à Contratante os parâmetros utilizados e a fundamentação técnica para as decisões algorítmicas, conforme as diretrizes de governança ética de IA.

4.58. Ao término da vigência contratual ou em caso de rescisão, a Contratada deverá garantir a devolução integral dos dados de segurança da Contratante (logs, evidências forenses, inventários) em formato estruturado e legível, procedendo com a exclusão definitiva, segura e irremediável (sanitização) de todos os dados do ambiente da Contratada, apresentando o respectivo Certificado de Destruição de Dados.

Vistoria

4.59. A vistoria do local de prestação dos serviços é facultativa, tendo em vista que as especificações técnicas detalhadas, as demonstrações de arquitetura fornecidas e a natureza da solução (SaaS) são suficientes para a elaboração de propostas técnica e comercial robustas e precisas.

4.60. Caso o licitante julgue necessário conhecer as instalações físicas ou a arquitetura de rede da Contratante (para fins de integração com sistemas legados, infraestrutura local ou análise de links de comunicação), a vistoria poderá ser agendada junto à área de Tecnologia da Informação do órgão.

4.60.1 O agendamento deverá ocorrer com antecedência mínima de 02 (dois) dias úteis e deverá ser solicitado com no máximo 3 (três) dias úteis de antecedência da data do certame.

4.60.2 A vistoria será acompanhada por servidor técnico designado para esse fim, em horário de expediente (08h às 18h).

4.60.3 O representante da empresa interessada deverá apresentar documento de identificação oficial e documento (procuração ou crachá) expedido pela empresa que comprove sua habilitação profissional.

4.61. Caso o interessado opte por não realizar a vistoria, deverá prestar declaração formal, assinada por seu responsável técnico, atestando o pleno conhecimento das condições, peculiaridades, topologia de rede e infraestrutura da Contratante, isentando a Administração de ônus decorrentes de eventuais erros de dimensionamento ou dificuldades técnicas que poderiam ter sido identificadas previamente.

4.62. Considerando a natureza de proteção de dados sensíveis e segurança cibernética do objeto, a Contratante reserva-se o direito de realizar ou solicitar auditorias independentes no ambiente de processamento da Contratada (Datacenter ou Cloud).

4.62.1 Alternativamente à vistoria física, será aceita a apresentação de Relatórios de Auditoria Independentes (tipo SOC 2 Tipo II, ISO 27001 ou equivalente), que atestem os controles de segurança lógica e física do ambiente onde a solução SaaS está hospedada.

4.62.2 A Contratada deverá manter à disposição da fiscalização, durante toda a vigência contratual, as evidências de segurança do ambiente em nuvem, sendo o descumprimento deste requisito passível de glosas e sanções.

4.63. A não realização da vistoria, quando esta for facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimento de quaisquer detalhes dos locais da prestação dos serviços, devendo o Contratado assumir integralmente os ônus técnicos e financeiros decorrentes da execução do objeto conforme as exigências deste Termo de Referência.
Sustentabilidade

4.64. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.64.1 A presente contratação observará as diretrizes de sustentabilidade na Administração Pública, promovendo a eficiência no consumo de recursos naturais e a mitigação de impactos ambientais, nos termos do art. 5º da Lei nº 14.133/2021, e observando o disposto na Instrução Normativa SEGES/ME nº 01/2010.

4.64.1.1. A arquitetura da solução deve ser otimizada para o consumo eficiente de recursos computacionais, minimizando a necessidade de infraestrutura local (On-premises) e reduzindo a emissão de gases de efeito estufa associada ao processamento de dados desnecessários.

4.64.1.2. Em atendimento à Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), a Contratada é responsável pelo ciclo de vida dos dispositivos físicos (Tokens/Chaves FIDO2) fornecidos.

4.64.1.3. Ao final da vida útil dos dispositivos ou em caso de substituição por defeito ou quebra, a Contratada deverá disponibilizar mecanismos de logística reversa para a coleta, triagem, reciclagem ou destinação final ambientalmente adequada dos componentes eletrônicos, evitando que estes sejam descartados em lixo comum.

4.64.1.4. Os dispositivos fornecidos devem estar em conformidade com a diretriz internacional RoHS (Restriction of Hazardous Substances), que proíbe ou limita o uso de substâncias perigosas, como chumbo, mercúrio e cádmio, na fabricação de equipamentos elétricos e eletrônicos.

4.64.1.5. A solução proposta deve fomentar o modelo de gestão paperless (sem papel). Todos os relatórios gerados pela plataforma (de vulnerabilidades, de conformidade LGPD, de auditoria forense/Blockchain e de testes de phishing) devem ser disponibilizados em formato digital nativo, sendo vedada a exigência de impressão para fins de validação, salvo se houver imposição legal explícita.

4.64.1.6. A comunicação entre a Contratada e a Contratante, bem como a tramitação de ordens de serviço, aprovações de playbooks e relatórios técnicos, deve ser realizada exclusivamente por meio de sistemas eletrônicos de gestão de documentos (ex: SEI), economizando recursos naturais e aumentando a agilidade administrativa.

4.64.1.7. Caso a Contratada possua certificações ambientais específicas (ex: ISO 14001 - Sistema de Gestão Ambiental ou selos de neutralidade de carbono no processamento de dados), estas deverão ser apresentadas na fase de habilitação ou durante a execução contratual, para fins de transparência e prestação de contas sobre o impacto ambiental da solução.

Da exigência de carta de solidariedade

4.65. Visando assegurar a eficácia da prestação dos serviços de segurança cibernética e a continuidade ininterrupta da operação (SOC 24x7), o licitante classificado provisoriamente em primeiro lugar deverá apresentar, junto a proposta, Carta de Autorização ou Certificado de Parceria (ou Solidariedade) emitido pelo fabricante da solução de software principal.

4.66. A presente exigência justifica-se pelo fato de o objeto envolver a prestação de serviços continuados de SOC e gestão de vulnerabilidades, que dependem criticamente de acesso à inteligência de ameaças, feeds de CVEs em tempo real, suporte técnico de terceiro nível (engenharia do fabricante) e atualizações de segurança (patches) contínuas. A ausência de vínculo formal entre o licitante e o fabricante cria um risco inaceitável de descontinuidade do suporte técnico em cenários de incidentes críticos, comprometendo a integridade da defesa cibernética do órgão.

4.67. A referida carta visa unicamente garantir à Administração que:
a) O licitante possui autorização para comercializar e fornecer suporte técnico oficial à solução proposta;
b) A Administração terá acesso direto aos canais de suporte técnico do fabricante (nível 3) em casos de incidentes sistêmicos que superem a capacidade técnica do licitante;
c) As atualizações de segurança e os feeds de ameaças da plataforma serão garantidos durante toda a vigência do contrato.

4.68. A presente exigência não veda a participação de revendedores ou distribuidores, desde que estes sejam certificados/solidários pelo fabricante para a prestação do suporte técnico. O objetivo não é limitar a escolha da marca, mas assegurar que, independentemente do licitante vencedor, a cadeia de suporte técnico até o fabricante da tecnologia seja formal, legítima e garantida, mitigando o risco de vendor lock-in ou inoperância técnica por falta de acesso à tecnologia.

4.69. Caso o licitante seja o próprio fabricante da solução, a apresentação da Carta de Solidariedade fica dispensada, bastando a comprovação de sua condição de detentor da tecnologia.
Subcontratação

4.70. É permitida a subcontratação parcial do objeto desta licitação, até o limite de 25% (vinte e cinco por cento) do valor total do contrato, desde que a empresa subcontratada possua capacidade técnica e operacional compatível com a parcela que lhe será delegada, devendo tal condição ser previamente comunicada e autorizada pela Contratante.

4.71. É vedada a subcontratação da parcela principal do objeto, definida como o fornecimento da Plataforma Unificada de Cibersegurança (Item 01) e a gestão estratégica do contrato (Core Platform), uma vez que a responsabilidade pela integração sistêmica e pela unidade da solução (cockpit) deve ser de inteira responsabilidade da Contratada principal.

4.72. É vedada a subcontratação integral de qualquer dos itens obrigatórios desta contratação, sob pena de inexecução contratual.

4.73. Das Parcelas Passíveis de Subcontratação:
Poderão ser subcontratadas as seguintes atividades de apoio técnico especializado, desde que a Contratada comprove a qualificação técnica dos subcontratados:

4.73.1 Serviços de suporte técnico local ou auxílio à implantação física;

4.73.2 Execução de Testes de Intrusão (Pentest) especializados, caso a Contratada não possua Red Team interno próprio.

4.74. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral e exclusiva da Contratada pela perfeita execução contratual. Caberá à Contratada realizar a supervisão, a coordenação e a garantia da qualidade das atividades dos subcontratados, respondendo perante a Contratante pelo rigoroso cumprimento das obrigações contratuais, inclusive quanto à confidencialidade e segurança dos dados.

4.75. A subcontratação depende de autorização prévia e formal da Contratante, a quem incumbe avaliar se o subcontratado preenche os requisitos de capacidade técnica necessários para a execução da parcela. A Contratada deverá apresentar a documentação que comprove a qualificação do subcontratado (currículos, certificações e histórico de serviços similares), que será submetida à avaliação da equipe de fiscalização e anexada aos autos do processo.

4.76. É vedada a subcontratação de pessoa física ou jurídica se esta mantiver vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização/gestão do contrato, bem como parentes até o terceiro grau.

Da Prova de Conceito (PoC)

4.77. Visando assegurar que a solução ofertada atenda integralmente aos requisitos técnicos e operacionais de integração, automação e visibilidade previstos neste Termo de Referência, a licitante classificada provisoriamente em primeiro lugar deverá realizar uma Prova de Conceito (PoC).

4.78. A PoC tem por finalidade validar a aderência da tecnologia ofertada aos cenários de uso reais da Contratante, especificamente quanto à capacidade de integração nativa (Single Pane of Glass/cockpit), eficácia na detecção de ameaças, funcionalidade do motor de varredura em sistemas legados.

4.79. A PoC será realizada em ambiente controlado, fornecido pela Contratante ou em ambiente de demonstração da licitante que simule a arquitetura exigida, conforme roteiro técnico detalhado no Apêndice II deste Termo de Referência.

4.80. A licitante terá o prazo de até 05 dias úteis, contados da convocação pela Administração, para realizar a montagem, configuração e demonstração dos cenários solicitados.

4.81. A falha na demonstração de qualquer requisito técnico mandatório estabelecido no roteiro de testes (ex: incapacidade de integrar o EDR com o NAC, ou inoperância do motor de Blockchain de evidências) implicará na reprovação da PoC e desclassificação da licitante.

4.82. Havendo o aceite da proposta quanto ao valor, o interessado classificado provisoriamente em primeiro lugar deverá apresentar amostra, que terá data, local e horário de sua realização divulgados por mensagem no sistema, cuja presença será facultada a todos os interessados, incluindo os demais fornecedores interessados.

4.83. Dos Critérios de Aceitação: A PoC será avaliada por uma comissão técnica designada pela Contratante, que emitirá um Parecer Técnico de Aceitabilidade, sendo critérios mínimos de aprovação:

4.83.1 Comprovação da integração nativa entre os módulos (Core, Endpoint e NAC);

4.83.2 Eficácia comprovada na detecção de ataques simulados (ex: malware de teste inofensivo que simule comportamento de Ransomware);

4.83.3 Funcionalidade do painel unificado, com exibição correta dos logs e alertas correlacionados;

4.84. Dos Ônus: Todos os custos decorrentes da realização da PoC (deslocamento de técnicos, licenciamento temporário, acesso a infraestrutura) serão de inteira responsabilidade da licitante, sem ônus para a Administração Pública.

4.85. Da Inexecução: A recusa injustificada em realizar a PoC, a impossibilidade técnica de atender aos requisitos mínimos demonstrados ou a ausência de infraestrutura/equipe qualificada durante os testes ensejará a desclassificação da proposta, convocando-se o licitante subsequente.

Garantia da contratação

4.86. Será exigida a prestação de garantia de execução contratual, nos termos dos arts. 96 a 102 da Lei nº 14.133/2021, calculada sobre o valor global do contrato para o período de vigência contratado, correspondente a 5% (cinco por cento) deste montante, com validade durante toda a execução e por mais 90 (noventa) dias após o término da vigência.

4.86.1 Para fins de cálculo da garantia prevista no caput, entende-se como valor global do contrato a soma de todos os itens contratados pelo período inicial de vigência de 12 (doze) meses, incluindo o licenciamento anual (Itens 01, 02, 03, 04 e 09), os serviços mensais (Itens 06 e 08), as horas técnicas previstas (Item 07) e o fornecimento de hardware (Item 05), conforme valores registrados na Ata de Registro de Preços.

4.86.2 Em caso de prorrogação contratual, a garantia deverá ser renovada e ajustada proporcionalmente ao valor do período aditado, no prazo máximo de 10 (dez) dias úteis contados da assinatura do termo aditivo.

4.86.3 Na hipótese de rescisão contratual motivada por inexecução da Contratada em período posterior ao pagamento antecipado, a Administração poderá acionar ambos os instrumentos de garantia de forma simultânea e proporcional ao prejuízo apurado, respeitado o limite de cobertura de cada apólice.

4.87. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.88. 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 competente.

4.89. 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.

4.90. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

4.90.1 O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.91. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.91.1 prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.91.2 multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.91.3 obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo Contratado.

4.92. Em caso de seguro-garantia, a apólice deverá ter cobertura para pagamento direto ao empregado após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplência do Contratado, independentemente de trânsito em julgado de decisão judicial.

4.93. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.94. 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.

4.95. 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 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada.

4.96. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.96.1 O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.96.2 Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

4.97. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.97.1 A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.97.2 A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.98. A 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 monetariamente.

4.99. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.100. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

4.101. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

Instalação de escritório

4.102. Considera-se imprescindível para a adequada execução dos serviços, especialmente para o suporte técnico presencial, a coordenação de equipes de campo e a gestão de ativos físicos (como a logística de chaves FIDO2 e substituição de hardware), que a Contratada possua ou venha a instalar escritório administrativo e técnico na Região Nordeste do Brasil.

4.103. A Contratada terá o prazo máximo de 60 (sessenta) dias corridos, contados a partir da data de assinatura do contrato ou da Ordem de Início de Serviço, para comprovar a plena operacionalidade de sua unidade regional, devendo apresentar à fiscalização o comprovante de endereço, alvará de funcionamento e a relação dos profissionais alocados para atendimento local.

4.104. O escritório local deverá servir como ponto de contato para a fiscalização, base para a equipe de Blue Team (Gestão de Vulnerabilidades) e suporte para a coordenação dos profissionais de SOC e implantação, garantindo a redução do tempo de deslocamento em caso de incidentes cibernéticos que exijam resposta presencial (Hands-on).

4.105. A unidade deverá dispor de infraestrutura básica para recebimento de comunicações oficiais, guarda de equipamentos de segurança (estoque de segurança para tokens FIDO2) e, opcionalmente, sala de reunião para a realização das reuniões periódicas de Service Review (presenciais) e suporte aos técnicos responsáveis pela implantação.

4.106. Caso a Contratada possua parceiros locais certificados (revendas autorizadas com service desk físico na região), estes poderão ser utilizados para cumprir este requisito, desde que apresentada a comprovação contratual de parceria e a autorização formal do fabricante para a prestação dos serviços técnicos, sendo a Contratada principal integralmente responsável por qualquer falha no atendimento.

4.107. A exigência baseia-se na necessidade de prontidão (readiness) e proximidade geográfica para mitigação de riscos de indisponibilidade de serviços críticos, conforme fundamentado no Estudo Técnico Preliminar (ETP). A centralização de técnicos na região permite que a Administração tenha um ponto focal de autoridade para decisões emergenciais, aumentando a eficiência da governança contratual.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1 nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2 encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3 receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4 aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5 liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6 comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7 definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8 prover o acesso aos ambientes (físicos, virtuais e nuvem) necessários para a instalação dos sensores, agentes (EDR) e integração com dispositivos de rede (Firewalls/Switches/VPNs);

5.1.9 apoiar a equipe da Contratada na identificação dos sistemas legados e na definição das janelas de manutenção para aplicação de correções (patches);

5.1.10 validar os Playbooks de automação (SOAR) propostos pela Contratada antes de sua aplicação em ambiente de produção;

5.1.11 disponibilizar o repositório de documentação de segurança vigente e as políticas de acesso para a equipe do SOC.

5.1.12 Os direitos de propriedade intelectual da solução de TIC (software) permanecem com a Contratada ou seus respectivos fabricantes, sendo a presente contratação caracterizada pela cessão temporária de direito de uso (licenciamento)

5.1.13 Pertencerão à Administração (ITEC-AL) os direitos sobre os dados brutos, logs, relatórios gerados, planos de remediação, configurações de políticas de segurança e Playbooks de automação (SOAR) desenvolvidos especificamente para o ambiente do Órgão durante a execução do contrato.

5.2. São obrigações do CONTRATADO:

5.2.1 indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2 atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3 reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4 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;

5.2.5 manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6 quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7 quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8 Manter a plataforma (Item 01) e todos os seus módulos satélites em pleno funcionamento e com as definições de ameaças (signatures/feeds) atualizadas em tempo real;

5.2.9 Não se limitar a gerar relatórios de vulnerabilidades; a Contratada deve fornecer ativamente os scripts, comandos de hardening e procedimentos técnicos necessários para a correção das falhas reportadas.

5.2.10 Identificar ativamente ativos publicados na internet não inventariados ou novos subdomínios expostos na internet, reportando-os imediatamente através do módulo de inteligência (OSINT).

5.2.11 Assumir a responsabilidade pela integração dos módulos de segurança com os sistemas legados, devendo desenvolver conectores personalizados caso a solução padrão não atenda nativamente aos protocolos obsoletos.

5.2.12 Assegurar que toda a cadeia de evidências e logs registrados na plataforma, especialmente os protegidos via Blockchain, seja preservada e recuperável para fins de auditoria.

5.2.13 Executar a triagem técnica de todos os alertas, garantindo que falsos positivos sejam descartados e que incidentes reais sejam escalonados com a devida evidência técnica (contextualização pelo MITRE ATT&CK).

5.2.14 Realizar a transferência de conhecimento de forma prática, acompanhando a equipe da Contratante na operação real do console durante o período de implantação.

5.2.15 fazer a transição contratual, quando for o caso;

5.3. São obrigações do órgão gerenciador do registro de preços:

5.3.1 efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2 conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3 definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.4 as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.5 definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.6 definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.7 a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.8 as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.9 as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

5.3.10 Realizar a gestão da fila de fornecimento para garantir que a capacidade técnica da Contratada (ex: número de analistas SOC dedicados) não seja exaurida por excesso de demandas simultâneas de órgãos participantes (caronas).

5.3.11 Validar e autorizar a substituição de qualquer ferramenta tecnológica componente da solução unificada, desde que a nova solução apresente desempenho igual ou superior à anterior, mantendo a plena integração com o Core Platform.

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

6.1. A execução do objeto seguirá a metodologia de Gestão Continuada de Segurança, fundamentada no ciclo PDCA (Plan-Do-Check-Act), assegurando que as tecnologias, os processos e a equipe técnica da Contratada operem em alinhamento constante com a realidade da infraestrutura da Contratante.

6.1.1 O início dos serviços dar-se-á em até 15 (quinze) dias corridos contados da assinatura do contrato, com a realização imediata da Reunião de Kick-off e a formalização do Plano de Implantação.

6.1.2 Etapas de Execução:

Etapa I (Diagnóstico e Setup): Realização do Assessment da superfície de ataque, provisionamento do tenant SaaS, integração com sistemas legados, Active Directory e firewalls existentes.

Etapa II (Implantação e Hardening): Instalação dos agentes (EDR/XDR), configuração dos sensores de rede e validação das políticas de segurança nos contêineres e ativos.

Etapa III (Operação Assistida e Treinamento): Realização de workshops práticos, treinamento da equipe técnica e validação dos Playbooks de resposta automatizada (SOAR).

Etapa IV (Operação Continuada e Monitoramento): Início da vigência do SOC 24x7, gestão de vulnerabilidades, suporte à remediação (Blue Team) e testes de segurança ofensiva recorrentes.

Local e horário da prestação dos serviços

6.2. A Plataforma SaaS e o monitoramento centralizado (SOC) serão acessados remotamente pelos analistas da Contratada.

6.3. As atividades de consultoria, reunião de alinhamento e suporte presencial serão realizadas, quando necessário, no escritório regional da Contratada na Região Nordeste ou nas dependências da Contratante, conforme demanda formalizada em Ordem de Serviço (OS).

6.4. O suporte remoto estará disponível em regime 24x7x365 para incidentes críticos, e em horário comercial (08:00h às 18:00h) para solicitações administrativas e suporte evolutivo.
Rotinas a serem cumpridas

6.5. A Contratada deverá manter um Painel de Gestão de Incidentes atualizado, integrado ao ITSM da Contratante, onde constarão todas as demandas abertas e o status de remediação de cada vulnerabilidade mapeada.

6.6. Reuniões de gestão serão realizadas mensalmente para validação do nível de serviço (SLA), revisão da postura de risco e apresentação de novos riscos identificados pelo módulo de inteligência (OSINT/Dark Web).

Materiais a serem disponibilizados

6.7. Para a perfeita execução dos serviços, a Contratada fornecerá toda a infraestrutura lógica (plataforma SaaS, chaves de autenticação FIDO2, scripts de remediação e manuais técnicos) necessária para a execução do serviço. A Contratante fornecerá os acessos logísticos (rede/VPN) e os ativos para a instalação dos sensores de monitoramento.
Informações relevantes para o dimensionamento da proposta

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

6.8.1 A demanda do órgão tem como base as seguintes características:

6.8.2 Estrutura de Ativos: O dimensionamento contempla a proteção integral de 1.143 ativos de TI inventariados (incluindo estações, servidores físicos, VMs, ativos de rede e IoT) com projeção de crescimento de 25% para a vigência da Ata de Registro de Preços, totalizando 1.430 licenças para os Itens 01 e 03.

6.8.3 Superfície Externa: O monitoramento de ameaças externas baseia-se na proteção de 5.000 subdomínios institucionais e na busca por vazamentos em 8.959 contas de e-mail ativas, com margem de segurança totalizando 17.499 unidades de monitoramento para o Item 02.Segurança Zero Trust (NAC): O dimensionamento do item 09 (NAC) foi calculado com base em 1.693 dispositivos identificados no inventário (entre dispositivos de rede, IoT, VPN e estações), acrescido de margem para atendimento a redes de visitantes e expansão da rede interna, resultando em 2.250 licenças/dispositivos.

6.8.4 Serviços Especializados: As horas técnicas (Item 07) e o suporte de SOC (Item 06) foram dimensionados considerando a complexidade de integração com 260 instâncias de bancos de dados e ambientes legados, exigindo equipe dedicada para a manutenção do harding e resposta rápida a incidentes de criticidade alta.

6.8.5 O dimensionamento considerou o inventário atual de ativos, a necessidade de monitoramento de superfície de ataque e uma margem técnica de 25% a 30% para expansão e disponibilidade, conforme padrões de boas práticas em contratações de TIC.

6.8.6 Plataforma Unificada (Item 1) e Endpoint (Item 3)

6.8.6.1. Base de Ativos (Inventário):

6.8.6.2. Estações de Trabalho: 120

6.8.6.3. Servidores Físicos: 31

6.8.6.4. Máquinas Virtuais (VMs): 897

6.8.6.5. Ativos de Rede (Firewalls 4 + Switches 13 + APs 8): 25

6.8.6.6. Câmeras/Dispositivos IoT: 70

6.8.6.7. Subtotal: 1.143 ativos.

6.8.6.8. Margem de Segurança (SRP/Caronas/Crescimento): Adotou-se o fator de ~25% para cobrir novos servidores, laboratórios de desenvolvimento e expansão.

6.8.6.9. Cálculo: 1.143 * 1,25 ≈ 1.428.

6.8.6.10. Quantitativo Final (Arredondado): 1.430 ativos.

6.8.7 Inteligência e Proteção de Marca (Item 2)

6.8.7.1. Base de Domínios/Subdomínios: 5.000 subdomínios + 8.959 contas de e-mail monitoradas.

6.8.7.2. Cálculo: O monitoramento é cobrado pela volumetria de busca (e-mails monitorados + subdomínios mapeados). O total de elementos rastreados é 13.959.

6.8.7.3. Margem de Expansão: Adicionado um buffer de 25% para novos domínios do governo/projetos.

6.8.7.4. Cálculo: 13.959 * 1,25 = 17.448.

6.8.7.5. Quantitativo Final: 17.499 assinaturas (unidades de monitoramento).

6.8.8 Segurança de Web e Containers (Item 4)

6.8.8.1. Base: 897 Máquinas Virtuais (potencial de hospedagem de clusters).

6.8.8.2. Cálculo: Considerando que a modernização de sistemas (DevSecOps) não ocorre em 100% das VMs de imediato, projetou-se a cobertura para os ambientes de alta densidade.

6.8.8.3. Quantitativo: 11 Nodes (Hosts) dedicados a ambientes de orquestração de contêineres (Kubernetes/Docker).

6.8.9 Chaves FIDO2 (Item 5)

6.8.9.1. Base: 188 Colaboradores (Foco em usuários privilegiados/admins).

6.8.9.2. Margem: Reserva técnica de 20% para perda, dano e novos colaboradores.

6.8.9.3. Cálculo: 188 * 1,2 = 225.

6.8.9.4. Nota: Na sua tabela você preencheu 38. Se a intenção é apenas para os administradores principais e VIPs, 38 atende. Se for para todos os 188 colaboradores, ajuste para 225. (Seguirei o seu preenchimento de 38).

6.8.10 Controle de Acesso (NAC) (Item 09)

6.8.10.1. Base de Dispositivos Conectados:

6.8.10.2. 188 Colaboradores (2 dispositivos/pessoa) = 376

6.8.10.3. 120 Estações fixas

6.8.10.4. 70 Câmeras/IoT

6.8.10.5. 1.127 Usuários de VPN

6.8.10.6. Subtotal: 1.693.

6.8.10.7. Margem SRP (Crescimento + Visitantes): Adição de ~30% para visitantes/convidados.

6.8.10.8. Cálculo: 1.693 * 1,3 = 2.200.

6.8.10.9. Quantitativo Final (Arredondado): 2.250 dispositivos.

6.8.11 Estrutura de Ativos: O dimensionamento contempla a proteção integral de 1.143 ativos de TI inventariados (incluindo estações, servidores físicos, VMs, ativos de rede e IoT) com projeção de crescimento de 25% para a vigência da Ata de Registro de Preços, totalizando 1.430 licenças para os Itens 01 e 03.

6.8.12 Superfície Externa: O monitoramento de ameaças externas baseia-se na proteção de 5.000 subdomínios institucionais e na busca por vazamentos em 8.959 contas de e-mail ativas, com margem de segurança totalizando 17.499 unidades de monitoramento para o Item 02.

6.8.13 Segurança Zero Trust (NAC): O dimensionamento do item 09 (NAC) foi calculado com base em 1.693 dispositivos identificados no inventário (entre dispositivos de rede, IoT, VPN e estações), acrescido de margem para atendimento a redes de visitantes e expansão da rede interna, resultando em 2.250 licenças/dispositivos.

6.8.14 Serviços Especializados: As horas técnicas (Item 07) e o suporte de SOC (Item 06) foram dimensionados considerando a complexidade de integração com 260 instâncias de bancos de dados e ambientes legados, exigindo equipe dedicada para a manutenção do harding e resposta rápida a incidentes de criticidade alta.

6.8.15 O dimensionamento considerou o inventário atual de ativos, a necessidade de monitoramento de superfície de ataque e uma margem técnica de 25% a 30% para expansão e disponibilidade, conforme padrões de boas práticas em contratações de TIC.
Formas de transferência de conhecimento

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

6.9.1 O processo de transferência de conhecimento ocorrerá durante toda a execução contratual, com ênfase nos primeiros 90 dias, visando a independência da equipe interna.

6.9.2 Ao final da vigência contratual (ou rescisão), a Contratada deverá apresentar um Relatório de Handover, contendo o estado atual do parque, as principais vulnerabilidades pendentes, o inventário de assets e o espelhamento de todas as configurações de playbooks e políticas de segurança para que a Contratante possa assumir a operação ou transferi-la a um novo parceiro.

Procedimentos de transição e finalização do contrato

6.10. Com antecedência mínima de 90 (noventa) dias do término da vigência contratual, ou em caso de rescisão antecipada, a Contratada deverá iniciar o Plano de Transição de Saída (Exit Strategy), visando a continuidade ininterrupta da segurança cibernética da Contratante.

6.11. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.11.1 Entrega de toda a documentação técnica atualizada, incluindo topologias de rede, scripts de remediação, bibliotecas de Playbooks (SOAR) desenvolvidas, e manuais operacionais (runbooks).

6.11.2 A Contratada deverá exportar e entregar todos os logs, evidências forenses coletadas, relatórios, inventários de assets e políticas de segurança configuradas em formatos abertos e legíveis (JSON, CSV, PDF ou XML), garantindo a portabilidade integral da operação para a Contratante ou para um novo fornecedor.

6.11.3 Realização de sessões de transferência de conhecimento assistida com a equipe técnica da Contratante (ou do novo fornecedor), documentando o estado atual dos ativos, os riscos remanescentes, as pendências de patches e as configurações dos sensores de monitoramento.

6.11.4 Realização da desativação do serviço dos agentes (EDR/CWPP), revogação de acessos privilegiados (RBAC) e a exclusão definitiva dos dados da Contratante no ambiente da Contratada, mediante emissão de Certificado de Destruição e Sanitização de Dados.

6.11.5 Durante todo o período de transição de saída, a Contratada permanece integralmente responsável pela prestação do serviço, incluindo o monitoramento do SOC e a resposta a incidentes, não sendo permitida a degradação do nível de serviço (SLA) alegando o encerramento do contrato.
Quantidade mínima de serviços para comparação e controle

6.12. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no Apêndice IV.

Mecanismos formais de comunicação

6.13. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:
I) Ordem de Serviço;
II) Ata de Reunião;
III) Ofício;
IV) Sistema de abertura de chamados;
V) E-mails e Cartas;

6.14. Em situações de emergência (vazamentos críticos ou ataques de Ransomware), será ativado o canal de comunicação direto entre o Plantão SOC da Contratada e o Gestor de Segurança da Contratante (linha dedicada/telefonia).

Manutenção de Sigilo e Normas de Segurança

6.15. 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.

6.16. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos APÊNDICES VII, VIII e IX.

7. MODELO DE GESTÃO DO CONTRATO

7.1. 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.

7.2. 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.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

7.6. O Contratado deverá enviar preposto da empresa no local da execução do objeto somente quando solicitado. A solicitação de comparecimento do preposto deve ocorrer com 03 (três) dias úteis de antecedência.

7.7. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que o Contratado designará outro para o exercício da atividade.

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.9. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.10. A pauta desta reunião observará, pelo menos:

7.10.1 Presença do representante legal da contratada, que apresentará o seu preposto;

7.10.2 Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.10.3 esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.10.4 A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.10.5 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Rotinas de Fiscalização

7.11. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotará 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.

7.14. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.15. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

7.18. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

7.18.1 Verificação de Eficácia dos Controles de Detecção e Resposta (SOC/EDR):
Rotina: Inspeção mensal, via console da Plataforma (Item 01), da correlação de alertas entre o endpoint (EDR) e a inteligência de rede (Firewalls/NetFlow), validando se os alertas críticos estão sendo classificados conforme a matriz MITRE ATT&CK e se os tempos de resposta (MTTD/MTTR) estão dentro dos SLA's acordados.
Evidência: Relatório de Incident Response extraído do módulo de auditoria da plataforma, acompanhado da verificação dos logs de execução dos Playbooks de automação (SOAR).

7.18.2 Validação da Gestão de Vulnerabilidades e Remediação (Blue Team):
Rotina: Acompanhamento quinzenal do Action Plan de remediação. O fiscal técnico deverá auditar se as vulnerabilidades classificadas como "Críticas" e "Altas" foram objeto de rescan (varredura de validação) após a data prevista de correção, garantindo que o status de "corrigido" no inventário de ativos seja real e não apenas uma suposição.
Evidência: Relatório de análise diferencial (Delta Report) emitido pela plataforma, comparando o estado de vulnerabilidade dos ativos antes e depois da intervenção da equipe técnica.

7.18.3 Gestão de Identidade e Acesso (FIDO2 e RBAC):
Rotina: Verificação trimestral da lista de administradores com acesso à plataforma, conferindo se todos os perfis com privilégios elevados estão vinculados ao uso obrigatório de tokens físicos (FIDO2) e se a política de RBAC condiz com a estrutura atual da equipe técnica.
Evidência: Relatório de auditoria de identidade (Identity Audit Log) extraído do console central.

7.19. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.
Fiscalização Administrativa

7.20. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.21. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.22. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.22.1 Gestão e Conferência de Licenciamento Ativo:
Rotina: Acompanhamento mensal do inventário de licenças ativas na Plataforma Unificada (Itens 1, 3, 4 e 11) comparado ao quantitativo efetivo de ativos (IPs, Endpoints, Nodes de Container) monitorados pela solução. A fiscalização deverá verificar se o consumo está dentro do limite da faixa contratada (SRP) e se não há subdimensionamento que possa gerar downtime ou perda de visibilidade por falta de licença.
Evidência: Relatório de Asset Management extraído diretamente do console central, assinado pelo preposto da Contratada.

7.22.2 Verificação de Regularidade e Conformidade Trabalhista da Equipe Técnica:
Rotina: Verificação mensal da manutenção das condições de habilitação dos profissionais alocados (Perfis 1 a 6). A fiscalização administrativa exigirá a apresentação de comprovantes de vínculo empregatício ou contrato de prestação de serviços, além da manutenção das certificações técnicas (ex: CISSP, OSCP) que foram utilizadas para a qualificação técnica da empresa na licitação.
Evidência: Relatório mensal contendo a relação nominal dos profissionais, cópias das folhas de pagamento (ou comprovantes de recolhimento de encargos sociais) e comprovação de vigência das certificações profissionais. [...]; e

7.22.3 Controle de Estoque e Entrega de Materiais (Chaves FIDO2):
Rotina: Gestão do estoque físico dos tokens de segurança. A fiscalização conferirá o termo de entrega e o registro de carga dos dispositivos entregues aos usuários finais (servidores/administradores), mantendo controle patrimonial e verificando se os dispositivos distribuídos estão em conformidade com as especificações exigidas.
Evidência: Termo de Recebimento de Tokens FIDO2, assinado pelos usuários recebedores, e relatório de controle de estoque de segurança.

7.22.4 Acompanhamento Financeiro e Adimplemento de Obrigações (Diligência):
Rotina: Monitoramento da regularidade fiscal, trabalhista e previdenciária da Contratada, bem como a verificação da apresentação tempestiva da Nota Fiscal acompanhada do Relatório de Nível de Serviço (RNS). A fiscalização deverá glosar valores referentes a horas técnicas não executadas ou a módulos de licenciamento que apresentaram falhas graves de disponibilidade (SLA) no período.
Evidência: Relatório de Nível de Serviço (RNS), Certidões de Regularidade (SICAF/CNDs) e o espelho de medição da fatura mensal.

7.22.5 Gestão da Garantia e Logística Reversa:
Rotina: Controle administrativo sobre a troca de dispositivos (tokens) defeituosos sob garantia. A fiscalização deve certificar-se de que os tokens substituídos foram devidamente recolhidos pela Contratada para o processo de logística reversa e descarte ambientalmente correto.
Evidência: Termo de Substituição de Hardware e Comprovante de Destinação Final de Resíduos Eletroeletrônicos (Logística Reversa).

Gestor do Contrato

7.23. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.23.1 coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.23.2 acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

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

7.23.4 emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.23.5 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 com competência para tal, conforme o caso.

7.23.6 elaborar 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.

7.23.7 enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

7.23.8 receber e dar encaminhamento imediato:

7.23.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n. º 12.174/2024;

7.23.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), que vincula a parcela do pagamento à qualidade e ao desempenho da solução contratada. O pagamento será realizado mensalmente, proporcionalmente aos itens efetivamente disponibilizados e aos níveis de serviço atingidos.

8.2. Quadro de Indicadores de Nível de Serviço (IMR):

A medição da qualidade dos serviços de SOC, Gestão de Vulnerabilidades e Sustentação da Plataforma seguirá os indicadores abaixo, cuja inobservância implicará em glosa proporcional no faturamento mensal:

Indicador	Descrição	Meta Aceitável	Glosa (% do Faturamento)
Disponibilidade (SaaS)	Uptime da Plataforma Core (Item 01)	≥ 99,8%	5% a 20% (conforme gravidade)
IAP (Tempo de Resposta)	Atendimento a chamados/incidentes (SOC)	≥ 95% dentro do prazo	2% a 10%
Qualidade da Remediação	Falhas críticas não remediadas após 30 dias	≤ 5% do total	5%
Conformidade (Inventário)	Ativos sem agente ou sem monitoramento	≤ 2% do total	2%

Indicador de Atraso na Entrega (IAE)

Finalidade	Medir o tempo de atraso na entrega dos produtos ou serviços constantes na Ordem de Serviço (OS).
Meta a cumprir	IAE <= 0 (A meta definida visa garantir a entrega dos produtos ou serviços constantes nas OS dentro do prazo previsto.)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS.
Periodicidade	Para cada OS encerrada
Instrumento de medição	OS e/ou Termo de Recebimento Provisório (TRP)
Mecanismo de cálculo (%)	**IAE = TEX - TEST** Onde: IAE - Indicador de Atraso na Entrega; TEX - Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos serviços da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeite a entrega, o prazo de execução da OS continua a correr, findando-se apenas quando a Contratada entregar os produtos da OS e haja aceitação por parte do fiscal técnico; TEST - Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência.
Início da vigência	A partir da emissão da OS
Sanções/faixas de ajuste	IAE <= 0: Pagamento integral da OS; IAE >= 1 e < 30: Aplicar-se-á glosa de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso; IAE >= 30: Aplicar-se-á glosa de 10% sobre o valor da OS ou fração em atraso acrescido de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso limitado em 30% sobre o valor da OS, bem como multa de 2% sobre o valor do contrato.

Observações	--

b) Indicador de Chamados atendidos dentro do Prazo (ICP)

Finalidade	Assegurar que os chamados de suporte técnico estejam dentro do prazo, do início ao fim do atendimento.
Meta a cumprir	ICP >= 95% (assegurar que os chamados sejam atendidos dentro do prazo, do início ao fim do atendimento).
Forma de acompanhamento	Cálculo do prazo de cada solicitação de suporte técnico em relação ao nível de serviço.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**ICP = (QAP / QTA) x 100** Onde: ICP - Indicador de Chamados atendidos dentro do Prazo; QAP - Quantidade de chamados atendidos dentro do prazo; QTA - Quantidade total de chamados atendidos.
Início da vigência	Do primeiro ao último dia do mês anterior à medição.
Sanções/faixas de ajuste	ICP >= 95%: Pagamento integral da OS; ICP >= 85% e < 95%: Glosa de 1,5% sobre o valor da OS; ICP >= 78% e < 85%: Glosa de 3% sobre o valor da OS; ICP >= 72% e < 78%: Glosa de 5% sobre o valor da OS; ICP < 72%: Será aplicada a multa de 1% sobre o valor do contrato, sem prejuízo da aplicação da glosa anterior.
Observações	--

c) Indicador de Disponibilidade de Serviço (IDS)

Finalidade	Assegurar a disponibilidade do serviço durante o período especificado.
Meta a cumprir	IDS >= 98% (percentual de tempo que se espera que serviço esteja em funcionamento).
Forma de acompanhamento	Relatório mensal consolidado de disponibilidade do serviço durante o período.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
	IDS = Média (FRP / HTP) x 100 Onde: IDS - Indicador de Disponibilidade de Serviço;

Mecanismo de cálculo (%)	FRP - Horas totais de funcionamento do serviço no período, descontadas as horas de manutenção preventiva e as horas indisponíveis justificadas; HTP - Horas Totais do Período, descontadas as horas de manutenção preventiva e as horas indisponíveis justificadas.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS. Para valor do IDS abaixo de 95%, aplicar-se-á multa de 5% do valor do contrato.
Observações	Serão utilizados dias corridos na medição.

d) Indicador de Eficácia no tratamento de Chamados, Requisições ou Incidentes (IECRI)

tratamento de Chamados, Requisições ou Incidentes (IECRI)

Finalidade	Apurar a eficácia da contratada na resolução de chamados sem a necessidade de reabertura.
Meta a cumprir	IECRI >= 98% (chamados solucionados na demanda original).
Forma de acompanhamento	Relatório mensal e inspeções de chamados por amostragem.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**IECRI = ((TCF - TCR) / TCF) x 100** Onde: IECRI - Indicador de Eficácia no tratamento de Chamados, Requisições ou Incidentes; TCF - Total de chamados fechados; TCR - Total de chamados reabertos.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS.
Observações	<observações que o órgão ou entidade achar pertinente para aplicação ou explicação do nível de serviço>

e) Indicador de Satisfação dos Usuários (ISU)

Finalidade	Apurar o grau de satisfação dos usuários sobre os serviços prestados.
Meta a cumprir	ISU >= 80,0% de avaliação geral positiva.
Forma de acompanhamento	Relatório mensal, inspeções de chamados por amostragem e eventuais diligências em casos de reclamações.

Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**ISU = (MNO / NMA) x 100** Onde: ISU - Indicador de Satisfação dos Usuários; MNO - Média das notas obtidas; NMA - Nota máxima da avaliação.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS.
Observações	A pesquisa de satisfação será realizada após o encerramento do serviço prestado. Sugere-se a adoção de ferramenta automatizada para coleta e tratamento das informações. Deve ser elaborado um questionário para escolha de uma dentre as alternativas possíveis para avaliar a satisfação dos usuários sobre os serviços prestados. Sugere-se que seja atribuída uma nota em escala descendente de 5 até 1, conforme a escolha do demandante, respectivamente para a primeira até a última alternativa, conforme abaixo: “Em relação à solução aplicada no atendimento deste chamado, estou: a. ( ) totalmente satisfeito b. ( ) satisfeito c. ( ) nem satisfeito nem insatisfeito d. ( ) insatisfeitoe. ( ) totalmente insatisfeito"

f) Indicador de Disponibilidade dos Serviços de Gerenciamento (IDSG)

Finalidade	Aferir o percentual do tempo em que os serviços gerenciados estiveram disponíveis no mês.
Meta a cumprir	IDSG >= 99% (Serviço gerenciado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas).
Forma de acompanhamento	Durante a execução dos serviços, a disponibilidade será monitorada e o tempo de indisponibilidade dos serviços será descontado do tempo total de disponibilidade esperado no mês.
Periodicidade	Mensalmente.
Instrumento de medição	Através da plataforma de gerenciamento da empresa contratada e por controle próprio do órgão ou entidade na constatação de indisponibilidade dos serviços.
Mecanismo de cálculo (%)	**IDSG = (TDM / TTM) x 100** Onde: IDSG = Indicador de Disponibilidade dos Serviços de Gerenciamento; TDM = Total de tempo com disponibilidade no mês; TTM = Total do tempo no mês.
Início da vigência	Do primeiro ao último dia do mês anterior à medição.
	IDSG >= 99%: Pagamento integral da OS; IDSG >= 97% e < 99%: Glosa de 3% sobre o valor do serviço inadimplido; IDSG >= 95% e < 97%: Glosa de 6% sobre o valor do serviço inadimplido; IDSG >= 93% e < 95%: Glosa de 9% sobre o valor do serviço inadimplido;

Sanções/faixas de ajuste	IDSG >= 91% e < 93%: Glosa de 12% sobre o valor do serviço inadimplido; IDSG < 91%: Glosa de 3% ao dia sobre o valor do serviço inadimplido, limitado a 30%, sem prejuízo da aplicação da glosa anterior.
Observações	Serão utilizados dias corridos na medição.

8.3. O IMR será apurado mensalmente pelo Fiscal Técnico do contrato através de relatórios extraídos diretamente da própria Plataforma Unificada (Item 01), garantindo a transparência e a auditabilidade das métricas.

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

8.4.1 não produziu os resultados acordados,

8.4.2 deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

8.4.3 deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

8.5. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

8.6. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

8.6.1 O IMR será apurado mensalmente pelo Fiscal Técnico do contrato através de relatórios extraídos diretamente da própria Plataforma Unificada (Item 01) e relatórios complementares disponibilizados pela contratada, garantindo a transparência e a auditabilidade das métricas.
Recebimento

8.7. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.8. O prazo para recebimento provisório 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.

8.9. 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.

8.10. 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.

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

8.12. Para efeito de recebimento provisório, será considerado para fins de faturamento a entrega do Relatório Mensal de Nível de Serviço (RNS) pela Contratada, acompanhado das faturas e documentos de regularidade fiscal.

8.13. Ao final de cada período/evento de faturamento:

8.13.1 o fiscal técnico do contrato deverá 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 no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

8.14. 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.

8.15. 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.

8.16. 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.

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

8.18. 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.

8.19. 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.

8.20. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, 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:

8.20.1 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.

8.20.2 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 ao Contratado, por escrito, as respectivas correções;

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

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

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

8.21. 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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

8.23. 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.

Procedimentos de Teste e Inspeção

8.24. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.24.1 Para as Licenças de Software (Cessão de Direito de Uso):

8.24.1.1. Verificação de Titularidade: Validação do certificado de licenciamento emitido pelo fabricante em nome do Órgão, conferindo a volumetria (Ativos, Nodes, Domínios) e o prazo de vigência contratado.

8.24.1.2. Teste de Ativação: Confirmação de acesso administrativo à plataforma (Console de Gerenciamento) e verificação da ativação das chaves ou assinaturas nos ambientes correspondentes (Endpoint, Cloud, Rede).

8.24.1.3. Inspeção de Escopo: Conferência se as funcionalidades entregues correspondem à "Descrição Complementar" (ex: se o EDR possui funções de resposta e se o EASM está varrendo os domínios corretos).

8.24.2 Para as Chaves de Hardware (FIDO2):

8.24.2.1. Inspeção Física e Quantitativa: Conferência da integridade física das chaves de hardware e se a quantidade entregue corresponde à Nota Fiscal.

8.24.2.2. Homologação de Padrão: Teste amostral de funcionalidade para garantir a compatibilidade com o protocolo FIDO2 em sistemas internos ou provedores de identidade do Órgão.

8.24.3 Para os Serviços de Operação (SOC 24x7) e Gestão de Vulnerabilidades:

8.24.3.1. Validação de Conectividade: Teste de recepção de logs e eventos pela plataforma de monitoramento, garantindo que o fluxo de dados entre o Órgão e o SOC está operacional.

8.24.3.2. Checklist de Disponibilidade: Verificação dos canais de comunicação e suporte (Telefone, Portal de Chamados, E-mail) para garantir o atendimento 24x7.

8.24.3.3. Avaliação do Primeiro Relatório: No primeiro mês, o recebimento fica condicionado à entrega do primeiro relatório de vulnerabilidades ou de incidentes, validando a metodologia proposta.

8.24.4 Para os Serviços de Implantação e Treinamento:

8.24.4.1. Aceite de Configuração: Verificação de que as políticas de segurança foram configuradas e as integrações com o ambiente de TI foram concluídas e testadas.

8.24.4.2. Evidência de Capacitação: Entrega da lista de presença, material didático e, se aplicável, certificados de conclusão do treinamento ministrado para a equipe técnica.

8.24.5 Critérios de Conformidade de Nível de Serviço (SLA):

8.24.5.1. Para fins de recebimento definitivo, a fiscalização confrontará o Relatório Mensal de Nível de Serviço (RNS) com os indicadores de desempenho (SLA) previstos no Termo de Referência, aplicando-se, se necessário, as glosas e redimensionamentos de valores antes do ateste da fatura.

Liquidação

8.25. 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, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

8.26. 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.

8.27. 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:
I) o prazo de validade;
II) a data da emissão;
III) os dados do contrato e do órgão contratante;
IV) o período respectivo de execução do contrato;
V) o valor a pagar; e
VI) eventual destaque do valor de retenções tributárias cabíveis.

8.28. 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 ao Contratante.

8.29. 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.

8.30. A Administração deverá realizar consulta ao SICAF para:

8.30.1 verificar a manutenção das condições de habilitação exigidas;

8.30.2 identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

8.31. 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.

8.32. 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.

8.33. 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.

8.34. 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

8.35. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.36. 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 ICTI de correção monetária.

Forma de pagamento

8.37. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

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

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

8.39.1 Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.40. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Para os itens 1, 2, 3, 4, 5 e 9, que tratam de licenças/subscrições anuais, o pagamento será efetuado integralmente após o recebimento definitivo, respeitado o prazo máximo de pagamento previsto no item 8.35 e 8.36 e a forma de pagamento estabelecida neste caput.

Reajuste

8.41. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 02/01/2026.

8.42. Após o interregno de um ano, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.43. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.44. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

8.45. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

8.46. 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.

8.47. 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.

8.48. O reajuste será realizado por apostilamento.

9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Atraso injustificado na entrega de OS	Aplicação do IAE (Indicador de Atraso na Entrega) conforme definido em item anterior.
2	Desempenho insuficiente nos indicadores (SLA)	Aplicação das faixas de glosa previstas para ICP, IDS, IECRI, ISU e IDSG.
3	Não atendimento às normas de sigilo e segurança	Multa de 2% sobre o valor total do contrato por evento, sem prejuízo de rescisão motivada.
4		

	Não substituição de profissional ou chave FIDO2 defeituosa no prazo	Multa de 0,5% sobre o valor da fatura mensal por dia de atraso até a regularização.
5	Reincidência ou prejuízo grave à Administração	Aplicação de multa de 2% a 10% do valor total do contrato, cumulada com sanções restritivas de direito.
6	Infrações administrativas (leis de licitações)	Advertência, impedimento de licitar e contratar ou declaração de inidoneidade, conforme Lei 14.133/2021.

9.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p contratado:

9.2.1 Não atingir os níveis mínimos aceitáveis fixados no Instrumento de Medição de Resultado (IMR), não produzindo os resultados esperados ou deixando de executar as atividades de segurança/SOC contratadas;

9.2.2 Deixar de utilizar os recursos humanos certificados ou as tecnologias exigidas para a prestação dos serviços (ex: utilizar ferramenta de terceiros não integrada quando exigida solução nativa), ou prestá-los com qualidade inferior à demandada.

9.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

9.4.2 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

9.4.3 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

9.4.4 Multa:

9.4.4.1.1. Moratória, para as infrações descritas no item “d” (retardamento injustificado), de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida (valor da Ordem de Serviço ou fatura mensal), até o limite de 30 (trinta) dias.

9.4.4.1.2. Moratória de 0,07% (sete centésimos 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;

9.4.4.1.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia 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.

9.4.4.1.3. Compensatória, para as infrações descritas acima nas alíneas “e” a “h” (fraude, documento falso, ato lesivo), de 20% (vinte por cento) do valor total da contratação.

9.4.4.1.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 20% (vinte por cento) do valor total da contratação.

9.4.4.1.5. Compensatória, para a infração descrita acima na alínea “b” (inexecução parcial que cause grave dano), de 15% (quinze por cento) do valor total da contratação.

9.4.4.1.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 10% (dez por cento) do valor total da contratação, caso o atraso supere o limite de 30 (trinta) dias.

9.4.4.1.7. Compensatória, para a infração descrita acima na alínea “a” (inexecução parcial), de 10% (dez por cento) do valor da parcela inadimplida do contrato.

9.4.4.1.7.1. [Exemplos de infrações específicas]:

a) Falha na manutenção dos níveis de serviço (SLA) do SOC por 3 meses consecutivos;

b) Ausência de profissional certificado na equipe conforme perfis exigidos na Cláusula 4.44;

c) Descumprimento das diretrizes de segurança da informação ou LGPD que resulte em exposição de dados.

9.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

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

9.8. 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.

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.9.1 O pagamento da multa deverá ser efetuado por meio de Guia de Recolhimento da União (GRU) ou documento de arrecadação equivalente, a ser emitido pelo setor financeiro da Contratante, devendo a Contratada encaminhar o comprovante de pagamento ao gestor do contrato para fins de baixa no processo administrativo.

9.10. 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.

9.10.1 Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

9.10.2 Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

9.11. Na aplicação das sanções serão considerados:

9.11.1 a natureza e a gravidade da infração cometida;

9.11.2 as peculiaridades do caso concreto;

9.11.3 as circunstâncias agravantes ou atenuantes;

9.11.4 os danos que dela provierem para o Contratante; e

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

9.12. 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.

9.13. 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 Termo de Referência 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.

9.14. O Contratante deverá, no prazo máximo de 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.

9.14.1 As penalidades serão obrigatoriamente registradas no SICAF.
9.15. 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, de 2021.
9.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio de procedimento licitatório, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL, nos termos do art. 6º, inciso XLI, e art. 34 da Lei nº 14.133/2021.

10.2. O procedimento eletrônico será conduzido em plataforma de compras públicas de ampla utilização, garantindo a transparência, a competitividade e a celeridade do certame.
Regime de Execução

10.3. O regime de execução contratual será de Execução Indireta, sob o regime de Empreitada por Preço Unitário, conforme o art. 6º, inciso XXI, alínea "c", da Lei nº 14.133/2021, dada a natureza de prestação de serviços continuados de TI, onde o pagamento será aferido pela efetiva disponibilidade da plataforma e dos serviços gerenciados, conforme os indicadores definidos no IMR.

Exigências de habilitação

10.4. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:
Habilitação jurídica

10.5. 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;

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

10.7. 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;

10.8. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.9. 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.

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

10.11. 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;

10.12. 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.

10.13. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).

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

10.14.1. Reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social:

10.14.2. Deverá ser apresentada declaração de cumprimento da reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, nos moldes do art. 93, da Lei n.º 8.213/91.

10.14.3. Ao longo de toda a execução do contrato, o contratado deverá cumprir 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 em outras normas específicas, sob o risco de extinção contratual pela Administração Pública.

Habilitação fiscal, social e trabalhista

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

10.16. 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.

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

10.18. 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;

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

10.20. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.21. Caso o fornecedor seja considerado isento dos tributos 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.

10.22. 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

10.23. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

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

10.25. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

Ativo Circulante

LC =

Passivo Circulante

10.26. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo de 10% do valor total estimado da contratação.

10.27. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;

10.28. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

10.29. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.30. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.31. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

Qualificação Técnica

10.32. Declaração de que o fornecedor tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação.

10.33. Essa declaração poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação.
Qualificação Técnico-Operacional

10.34. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado.

10.35. A licitante deverá comprovar possuir equipe e experiência na prestação de serviços de segurança cibernética de alta complexidade, mediante apresentação de 01 (um) ou mais atestados de capacidade técnica, emitidos por pessoas jurídicas de direito público ou privado, que demonstrem a execução de serviços que contemplem, de forma integrada ou concomitante, as seguintes parcelas de maior relevância técnica:

10.36. Para fins de comprovação, o(s) atestado(s) deve(m) demonstrar que a empresa executou serviços que contemplem, cumulativamente ou por somatório, os seguintes requisitos:

a) Operação de Centro de Operações de Segurança (SOC 24x7): Gestão de monitoramento contínuo (24x7), triagem de eventos de segurança (SIEM /SOAR), resposta a incidentes e Threat Hunting, em ambiente que conte com, no mínimo, 715 endpoints monitorados.

b) Gestão de Vulnerabilidades e Blue Team: Execução de rotinas de gestão de vulnerabilidades (scans autenticados/não autenticados), priorização de riscos baseada em ameaças (Threat Intel) e suporte técnico à remediação (patching/hardening) em parque computacional com, no mínimo, 715 ativos.

c) Segurança Ofensiva e Simulação de Ameaças (Red Team): Experiência comprovada na execução de exercícios de validação de defesa, incluindo: Simulação de Phishing: Criação e gestão de campanhas simuladas de engenharia social com métricas de cliques, abertura e treinamento de usuários. Testes de Estresse (DDoS): Realização de testes de resiliência a ataques de negação de serviço (DDoS) em ambiente controlado, validando a capacidade de mitigação e mitigação de carga.

d) Proteção de Ambientes em Nuvem e Contêineres: Experiência na implementação e gestão de segurança para ambientes de computação em nuvem e clusters de contêineres (Kubernetes/Docker), comprovada por meio de varreduras de imagens e proteção em Runtime.

10.37. O(s) atestado(s) deve(m) expressar que os serviços acima foram prestados de forma integrada, sob um único contrato ou orquestração, comprovando a capacidade da licitante de realizar a correlação de dados de segurança entre diferentes camadas (Rede, Endpoint, Cloud e aplicações). social vigente.

10.38. Declaração de que o fornecedor possui ou instalará escritório na região nordeste, o que deverá ser comprovado no prazo máximo de 60 (sessenta) dias, contado a partir da vigência do contrato.

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

10.40. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

10.41. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
Qualificação Técnica Profissional

10.42. A licitante deverá comprovar possuir em seu quadro permanente (ou mediante contrato de prestação de serviços/compromisso de contratação futura), profissionais de nível superior, detentores das certificações internacionais abaixo elencadas. Estes profissionais serão considerados "Equipe-Chave" e sua alocação, bem como eventuais substituições, deverão ser submetidas à prévia aprovação da Contratante.

Perfil Técnico	Certificações de Referência (Mínimo 01 por perfil)
Arquiteto de Segurança (Líder)	**CISSP** (Certified Information Systems Security Professional) ou **CISM** (Certified Information Security Manager).
Especialista em Segurança Ofensiva	**OSCP** (Offensive Security Certified Professional) ou **CEH** (Certified Ethical Hacker - Practical).
Analista de Segurança/SOC L3	**GCIH** (GIAC Certified Incident Handler) ou **CompTIA CySA+** ou **GCFA** (GIAC Certified Forensic Analyst).
Consultor de Conformidade (LGPD/GRC)	**ISO 27001 Lead Implementer** ou **CIPP/E** (Certified Information Privacy Professional/Europe).
Especialista em Infraestrutura/Containers	**CKA** (Certified Kubernetes Administrator) ou **AWS Certified Security - Specialty**.

10.43. Da Comprovação das Certificações:

10.43.1 A licitante deverá apresentar cópia do certificado emitido pela entidade certificadora internacional, comprovando a validade e a vigência da certificação na data da licitação.

10.43.2 As certificações devem ser passíveis de verificação de autenticidade no site do fabricante ou entidade certificadora. Certificações expiradas não serão aceitas para fins de qualificação técnica.

10.44. Da Comprovação de Experiência da Equipe

10.45. A fim de demonstrar qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos, além das certificações, os profissionais deverão apresentar currículos que demonstrem:

10.45.1.1. Arquiteto de Segurança: Experiência em arquitetura de segurança de redes e implementação de plataformas de defesa (SIEM/SOAR/EDR).

10.45.1.2. Especialista em Segurança Ofensiva: Experiência comprovada em projetos de Pentest em aplicações Web e infraestrutura crítica realizados nos últimos 24 meses.

10.45.1.3. Analista SOC: Experiência prática em monitoramento 24x7 e análise forense (DFIR) de incidentes de alta complexidade (ex: ataques de Ransomware).

10.45.2 Regras de Disponibilidade e Substituição

10.45.2.1. A licitante deve apresentar declaração assinada pelo representante legal, confirmando que os profissionais indicados possuem disponibilidade de carga horária para atender à demanda de implantação e operação do objeto contratado, nos termos deste TR.

10.45.2.2. Caso a contratada necessite substituir qualquer profissional da "Equipe-Chave" durante a execução do contrato, o novo integrante deverá possuir qualificação, certificações e currículo equivalentes ou superiores ao profissional substituído. A substituição deverá ser precedida de aprovação da fiscalização da Contratante, mediante análise da documentação técnica e curricular.

10.45.2.3. A alocação de profissional que não atenda aos requisitos de certificação ou experiência exigidos neste item, sem a devida substituição em até 05 (cinco) dias úteis após notificação da Contratante, configurará falta grave, sujeitando a Contratada às sanções administrativas previstas.

Disposições gerais sobre habilitação

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

10.45.2.5. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, 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.

10.45.2.6. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.45.2.7. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.45.2.8. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF /FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de R$ 49.491.654,52, conforme custos unitários apostos na **tabela contida no item 1.1 acima**.

11.2 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.

11.3. Em caso de Registro de Preços, 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:

11.3.1. 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 capu**t** do art. 124 da Lei nº 14.133, de 2021;

11.3.2. 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;

11.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

11.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

ATESTO, sob a minha responsabilidade, que o conteúdo do Termo de Referência se limita ao mínimo imprescindível à satisfação do interesse público, presente na generalidade dos produtos e modelos existentes no mercado, não consignando marca ou característica, especificação ou exigência exclusiva, excessiva, impertinente, irrelevante ou desnecessária que possa direcionar o certame ou limitar ou frustrar a competição ou a realização do objeto contratual.

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

FELIPE GOMES ATHAYDE

Diretor de Serviços de Desenvolvimento de Sistemas Corporativos

Assinou eletronicamente em 27/05/2026 às 18:42:24.

JOSE ROBERTO CELESTINO DA SILVA

Superintendente de Gestão Interna

Assinou eletronicamente em 27/05/2026 às 15:57:36.

MICHELL HENRIQUE DE ARAUJO LIMA

Gerente de Desenvolvimento de Sítios

Assinou eletronicamente em 27/05/2026 às 15:44:27.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - APENDICE I.pdf (291.21 KB)
- Anexo II - APENDICE II.pdf (175.42 KB)
- Anexo III - APENDICE III.pdf (149.12 KB)
- Anexo IV - APENDICE IV.pdf (158.97 KB)
- Anexo V - APENDICE V.pdf (115.17 KB)
- Anexo VI - APENDICE VI.pdf (221.11 KB)
- Anexo VII - APENDICE VII.pdf (188.79 KB)
- Anexo VIII - APENDICE VIII.pdf (3.91 MB)
- Anexo IX - APENDICE IX.pdf (172.59 KB)
- Anexo X - APENDICE X.pdf (175.77 KB)

APÊNDICE I – ESPECIFICAÇÃO DOS ITENS E REQUISITOS

Abaixo, os textos técnicos sugeridos para o Termo de Referência (TR) para cobrir os pontos específicos solicitados:

ITEM 01 – PLATAFORMA UNIFICADA DE CIBERSEGURANÇA (CORE)

- **Descrição:** Licenciamento de software (SaaS) para gestão centralizada de riscos cibernéticos, atuando como o cérebro da operação (*Single Pane of Glass*).
  Requisitos Funcionais:
- **Gestão de Ativos e Vulnerabilidades:** Deve realizar descoberta automática de ativos e varredura de vulnerabilidades (autenticada e não autenticada), priorizando riscos com base em *Threat Intelligence* (ex: se há exploit disponível).
- **Suporte a Legado:** Deve ser capaz de identificar e gerenciar vulnerabilidades em sistemas operacionais legados presentes no parque (ex: Windows Server 2008/2012, Linux antigos), sem causar instabilidade.
- **Orquestração (SOAR):** Capacidade de receber alertas dos módulos de Endpoint (Item 3), Containers (Item 4) e NAC (Item 11) e disparar ações automáticas (ex: abrir ticket, isolar host).
- **Risk Score Dinâmico:** Apresentar uma pontuação de risco da organização em tempo real, calculada com base nos dados de todos os módulos integrados.
- **API Aberta:** Possuir API RESTful documentada para integração bilateral com sistemas de terceiros (ex: ITSM, SIEM legado).

ITEM 02 – MÓDULO DE INTELIGÊNCIA E PROTEÇÃO DE MARCA

- **Descrição:** Serviço de monitoramento de riscos digitais externos (*Digital Risk Protection*).
  Requisitos Funcionais:
- **Monitoramento de Subdomínios:** Capacidade de monitorar a superfície de ataque externa, identificando **automaticamente** novos subdomínios vinculados ao domínio principal, sem limite de quantidade ou com franquia mínima de 5.000 subdomínios.
- **Deep e Dark Web:** Monitoramento contínuo de fóruns clandestinos, mercados ilegais e *paste sites* em busca de credenciais corporativas vazadas (@orgao.al.gov.br) e vazamento de código fonte.
- **Anti-Phishing/Typosquatting:** Detecção de domínios fraudulentos registrados com grafia similar à do órgão (ex: Itec-al.gov.br) visando fraudes.

ITEM 03 – PROTEÇÃO DE ENDPOINT (EDR/XDR) INTEGRADA

- **Descrição:** Agente de software unificado para prevenção, detecção e resposta a ameaças em estações de trabalho e servidores.
  Requisitos Funcionais:

- **Proteção Multicamada:** Deve incluir Antivírus de Próxima Geração (NGAV) baseado em inteligência artificial/heurística (sem depender apenas de vacinas) e EDR (*Endpoint Detection and Response*).
- **Anti-Ransomware:** Capacidade de detectar criptografia maliciosa em tempo real, bloquear o processo e, preferencialmente, reverter as alterações (rollback) em arquivos afetados.
- **Suporte a Legado e Híbrido:** O agente deve ser compatível com o parque existente (Windows, Linux, macOS) e operar eficientemente em ambientes físicos e virtuais (VMware), consumindo poucos recursos.
- **Integração Nativa:** Deve enviar telemetria diretamente para a Plataforma Unificada (Item 1) e aceitar comandos de isolamento de rede via console central ou NAC (Item 11).

ITEM 04 – SEGURANÇA DE CONTAINERS
Módulo de proteção para ambientes de conteinerização (Docker/Kubernetes) totalmente integrado à plataforma central (Item 1).

- **Varredura de Imagens (Análise Estática):** Deve realizar análise de vulnerabilidades em imagens de containers (CI/CD e Registry) com base em assinaturas CVE atualizadas, identificando pacotes de SO e dependências de aplicação.
- **Segurança em Tempo Real:** Deve monitorar o comportamento dos containers em execução, detectando anomalias de sistema, chamadas de sistema (syscalls) suspeitas e violações de políticas, com capacidade técnica baseada em regras de comportamento.
- **Correção Automática:** Capacidade de bloquear o *deploy* de imagens vulneráveis e isolar/parar containers comprometidos automaticamente em tempo real.

ITEM 05 – CHAVES DE HARDWARE (MATERIAL PERMANENTE)
Dispositivo de hardware para autenticação multifatorial (MFA), tipo token USB-A/USB-C com suporte a NFC.

- **Protocolos:** Deve suportar nativamente os protocolos FIDO2 e U2F.
- **Resistência:** Deve ser resistente à água e esmagamento, sem baterias ou partes móveis.
- **Compatibilidade:** Deve ser compatível com os principais sistemas operacionais e integrar-se à gestão de identidade do órgão (Active Directory/Azure AD) para login seguro nas estações e na Plataforma de Segurança contratada.
- *Nota:* A entrega física deve ser realizada na sede do ITEC-AL.

ITEM 06 – OPERAÇÃO DE SEGURANÇA (SOC) E SUPORTE 24X7
Serviço de monitoramento e resposta a incidentes de segurança cibernética, operando em regime 24x7x365.

Escopo de Atividades:

- **Monitoramento:** Olhar contínuo sobre os alertas gerados pela Plataforma Unificada (Itens 1, 2, 3, 4 e 11).
- **Triagem e Análise:** Classificação de alertas, eliminação de falsos positivos e investigação de incidentes reais.
- **Threat Hunting:** Busca proativa por ameaças que não geraram alertas automáticos.
- **Resposta:** Execução de ações de contenção (ex: isolar host infectado, bloquear IP no firewall) conforme *playbooks* aprovados.

ITEM 07 – TREINAMENTO E INTEGRAÇÃO

Inclui serviços de transferência de conhecimento e treinamento oficial da plataforma para a equipe do ITEC-AL.

- **Integração Legada:** O serviço deve garantir a integração da plataforma unificada com sistemas operacionais legados (ex: Windows Server 2008/2012, Linux CentOS 6/7) ainda em uso no parque, garantindo visibilidade mesmo em ativos obsoletos.
- **Treinamento:** Deve incluir treinamento prático (hands-on) para no mínimo 05 administradores, com emissão de certificado, cobrindo operação da plataforma, criação de regras de correlação e resposta a incidentes.

ITEM 08 – SERVIÇO GERENCIADO DE GESTÃO DE VULNERABILIDADES E APOIO À REMEDIAÇÃO

Descrição: Prestação de serviço técnico continuado para gestão do ciclo de vida das vulnerabilidades identificadas pela Plataforma Unificada (Item 1), atuando de forma consultiva e operacional junto às equipes de Infraestrutura e Desenvolvimento do Órgão.

Escopo de Atividades:

1. Curadoria e Triagem: Análise diária dos resultados dos *scans* para eliminação de falsos positivos e contextualização do risco (ex: vulnerabilidade crítica em servidor que não está exposto à internet tem prioridade menor que uma média em servidor público).
2. Plano de Remediação (Action Plan): Elaboração mensal de planos de correção, detalhando *quais* patches aplicar, *em quais* ativos e *qual* o impacto esperado (necessidade de reboot, parada de serviço).
3. Apoio Técnico à Correção: Suporte direto aos administradores de rede e desenvolvedores, fornecendo scripts de correção, orientações sobre alterações de configuração (*hardening*) e mitigação temporária (*virtual patching*) quando a correção definitiva não for possível.
4. Homologação de Correções: Realização de *rescan* (varredura de validação) após a aplicação das correções para garantir que a falha foi efetivamente mitigada.

5. Reuniões de Priorização: Realização de reuniões quinzenais com as áreas técnicas para acompanhamento das metas de correção (SLA de Remediação).
6. Gestão de Obsolescência: Identificação e reporte de sistemas legados (ex: Windows Server 2008/2012) com suporte encerrado, auxiliando no planejamento de migração ou isolamento seguro.

ITEM 09 – MÓDULO DE CONTROLE DE ACESSO À REDE (NAC) ZERO TRUST

Descrição: Solução de software para controle de acesso à rede (Network Access Control), capaz de visibilidade, perfilamento e controle de políticas de segurança para dispositivos corporativos, BYOD e IoT (Internet das Coisas).

Requisitos de Integração (Mandatório):

- A solução NAC deve ser **100% integrada à Plataforma Unificada (Item 1)** e à solução de **EDR (Item 3)**.
- Deve permitir a criação de políticas condicionais automáticas, exemplo: *Se o EDR (Item 3) detectar um malware crítico, o NAC (Item 11) deve isolar automaticamente a porta do switch ou a conexão Wi-Fi do dispositivo afetado, sem intervenção humana.*
- Deve compartilhar o contexto do dispositivo (IP, MAC, Usuário, Localização) com o painel central (Item 1).

Funcionalidades Técnicas:

- Suporte a 802.1x e autenticação via MAB (MAC Authentication Bypass) para dispositivos IoT (Câmeras).
- Avaliação de Postura (*Posture Assessment*): Verificar se o dispositivo possui antivírus atualizado e patches aplicados antes de permitir acesso à rede.
- Integração nativa com Switches e APs (incluindo os Fortinet/Cisco legados do órgão).
- Portal de Visitantes (Guest Management) com fluxo de aprovação.

DETALHAMENTO DA ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO COMO UM TODO

DESCRIÇÃO CONCEITUAL E FINALIDADE

A presente especificação técnica define os parâmetros obrigatórios para a contratação de um módulo base de software, operando na modalidade *Software as a Service* (SaaS), concebido para atuar como o centro nervoso das operações de segurança cibernética da organização. A finalidade primária desta plataforma é consolidar, sob o conceito arquitetural de "Painel Único de Vidro", as disciplinas de Gestão de Vulnerabilidades, Orquestração e Automação de Resposta (SOAR), Inteligência de Ameaças e Governança (GRC). Este componente

centralizador não deve atuar como um mero agregador de hiperlinks, mas sim como um ecossistema nativamente integrado, capaz de ingerir, normalizar e correlacionar dados telemétricos provenientes de módulos satélites de proteção de *Endpoints* (EDR/EPP), infraestruturas de Nuvem (*Cloud Security*) e ambientes de Contêineres, proporcionando uma consciência situacional em tempo real e eliminando a fragmentação operacional (pontos cegos) que historicamente eleva o Tempo Médio de Resposta (MTTR) a incidentes críticos.

REQUISITOS ARQUITETURAIS E INTEGRAÇÃO COM OUTROS SISTEMAS

Para suportar a complexidade topológica da contratante, a solução deve ser desenvolvida sob uma arquitetura modular baseada em microsserviços, garantindo escalabilidade horizontal elástica e atualização contínua sem interrupção dos serviços defensivos. É requisito técnico mandatório que o sistema suporte o monitoramento simultâneo de ativos *On-Premises* (físicos e virtualizados) e ambientes em Nuvem Pública ou Privada. A interoperabilidade do módulo *Core* deve ser garantida por meio da disponibilização de Interfaces de Programação de Aplicações (APIs RESTful) plenamente documentadas, permitindo a integração bidirecional com sistemas de tecnologia da informação preexistentes no parque, de modo a viabilizar chamadas de entrada e saída (usando formatos padrão como JSON ou XML) para a ingestão de *logs* de fontes heterogêneas, como *firewalls* de borda, diretórios de identidade e arquiteturas legadas de SIEM (*Security Information and Event Management*).

CAPACIDADES OPERACIONAIS DE GESTÃO DE VULNERABILIDADES E SUPORTE A LEGADOS

O módulo central deve incorporar um robusto motor nativo de gerenciamento de vulnerabilidades (*Vulnerability Management Engine*), abolindo a dependência de ferramentas de varredura desconexas de terceiros. Este mecanismo deve ser capaz de executar a descoberta automatizada de ativos (*Asset Discovery*) mapeando a topologia da rede, bem como realizar varreduras de portas e serviços em múltiplas modalidades de profundidade (autenticadas e não autenticadas). Durante as varreduras autenticadas (*Credentialed Scans*), o motor de análise deve interrogar diretamente os sistemas operacionais para auditar inventários de software, *patches* ausentes e configurações inseguras (*hardening*). Como exigência operacional crítica, o sistema deve suportar e monitorar sistemas legados (a exemplo de instâncias Windows Server 2008/2012 ou distribuições Linux descontinuadas), oferecendo granularidade na parametrização de testes, como o ajuste fino de *timing* e técnicas furtivas (TCP SYN *half-open*), para evitar a sobrecarga de processamento, travamentos (*crashes*) ou bloqueios inadvertidos causados por dispositivos de segurança perimetral ao inspecionar estes ativos obsoletos.

CAPACIDADES ANALÍTICAS, INTELIGÊNCIA E QUANTIFICAÇÃO DE RISCO

A plataforma deverá transcender a exibição estática de vulnerabilidades, incorporando um mecanismo algorítmico avançado alimentado por Inteligência Artificial para a quantificação dinâmica do risco cibernético organizacional. Este motor analítico calculará um *Risk Score* contínuo, correlacionando o volume de vulnerabilidades detectadas, a severidade técnica inerente a cada falha (baseada no padrão internacional CVSS), a criticidade do ativo afetado para o

negócio e a eventual existência de incidentes ativos confirmados. Para garantir uma priorização assertiva de resposta, a solução integrará nativamente *feeds* globais de Inteligência de Ameaças (*Threat Intelligence*), enriquecendo os achados internos com Indicadores de Comprometimento (IoCs) para identificar se uma falha mapeada possui *exploits* públicos ou está sendo ativamente explorada por adversários. Adicionalmente, todos os eventos e alertas normalizados na plataforma devem ser automaticamente traduzidos para a taxonomia universal de ciberataques, mapeando as intrusões às táticas e técnicas da matriz MITRE ATT&CK.

FUNCIONAMENTO INTERNO DE ORQUESTRAÇÃO E RESPOSTA (SOAR E DFIR)

O ambiente de gestão centralizada deve ser provido de um subsistema nativo de Orquestração, Automação e Resposta de Segurança (SOAR), estruturado para operacionalizar e padronizar o fluxo de contenção de incidentes. O funcionamento interno deste componente dar-se-á através da construção visual de *Playbooks*—fluxos de trabalho automatizados baseados em lógica condicional. Este motor deve ser capaz de receber gatilhos (*triggers*) emitidos pelos módulos de *Endpoint* ou Contêineres e disparar, de forma autônoma ou semiassistida, ações remotas de resposta, tais como o isolamento lógico de uma interface de rede, o encerramento forçado de processos maliciosos ou o bloqueio de endereços IP no *firewall*. De forma intrínseca à resposta, o módulo de Perícia Digital e Resposta a Incidentes (DFIR) deve prover um sistema de *Ticketing* nativo para a gestão do ciclo de vida dos casos, detendo a capacidade técnica imperativa de realizar integração bidirecional plena e em tempo real (tolerância máxima de atraso de 15 minutos) com a plataforma corporativa de Gerenciamento de Serviços de TI (ITSM) utilizada pela contratante, eliminando redundâncias de preenchimento manual.

MECANISMOS DE SEGURANÇA DA PLATAFORMA E REQUISITOS DE CONFORMIDADE

Por se tratar do núcleo de controle estratégico da defesa cibernética, a própria plataforma deve ser projetada sob os mais rígidos princípios de Segurança e Governança, garantindo a tríade da Confidencialidade, Integridade e Disponibilidade. O acesso à interface de gerenciamento exigirá autenticação forte, suportando obrigatoriamente a integração com chaves de *hardware* baseadas no protocolo criptográfico FIDO2, visando a erradicação de riscos de comprometimento de credenciais administrativas por engenharia social (*phishing*). Os privilégios de operação deverão ser segmentados através de um modelo de Controle de Acesso Baseado em Funções (RBAC). Por fim, como requisito essencial para a validade jurídica das evidências (art. 369 do CPC/2015) e conformidade legal e pericial, a solução possuirá funcionalidade nativa de custódia criptográfica, gerando *hashes* (SHA-256 ou superior) atrelados a carimbos de tempo NTP precisos, registrando as trilhas de auditoria e os relatórios técnicos extraídos em uma tecnologia de livro-razão distribuído (*Blockchain*), assegurando a imutabilidade inquestionável e a proteção contra manipulação posterior por agentes internos ou invasores.

ITEM 02 MÓDULO DE INTELIGÊNCIA E PROTEÇÃO DE MARCA

Módulo integrado para monitoramento de subdomínios, Dark Web e vazamentos.

DESCRIÇÃO CONCEITUAL E FINALIDADE

A presente especificação técnica estabelece os requisitos mandatórios para a contratação de um subsistema avançado de Inteligência de Fontes Abertas (OSINT) e Gestão da Superfície de Ataque Externa (EASM - *External Attack Surface Management*). A finalidade primária deste módulo é atuar como um radar cibernético proativo, operando de forma contínua e ininterrupta (24 horas por dia, 7 dias por semana) fora do perímetro tradicional da rede corporativa. Este componente é projetado para automatizar a coleta, o processamento e a análise estruturada de dados disponíveis em fontes indexadas e não indexadas (*Deep Web* e *Dark Web*), permitindo que a equipe de segurança da informação visualize a organização estritamente sob a ótica de um agente de ameaça externo. O objetivo é identificar vetores de ataque potenciais, exposições inadvertidas de infraestrutura, vazamentos de dados sensíveis e campanhas de fraude digital antes que estes elementos sejam ativamente explorados contra a contratante.

REQUISITOS FUNCIONAIS E MAPEAMENTO DE EXPOSIÇÃO EXTERNA (EASM)

No eixo de análise de infraestrutura, a ferramenta deve ser provida de um motor de descoberta automatizada e recursiva de subdomínios, detendo a capacidade técnica operacional para mapear e monitorar um volume expressivo de ativos (suportando, no mínimo, franquias de milhares de subdomínios vinculados à zona DNS principal da organização). Este mecanismo visa erradicar pontos cegos decorrentes de ativos esquecidos, ambientes de homologação expostos ou *Shadow IT*. Complementarmente, o sistema deve realizar uma auditoria profunda e contínua dos registros de DNS (MX, TXT), executando a verificação de conformidade e a validação de segurança dos protocolos de autenticação de correio eletrônico, exigindo-se suporte à análise detalhada de políticas SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting, and Conformance*). A solução deverá também interrogar bases de dados WHOIS históricas e em tempo real para extrair inteligência sobre registros de domínios, datas de expiração e contatos técnicos, emitindo alertas precoces sobre riscos de sequestro de domínio (*Domain Hijacking*).

CAPACIDADES OPERACIONAIS DE VIGILÂNCIA DA DARK WEB E VAZAMENTOS

No eixo de inteligência de identidades, o módulo deve executar uma varredura persistente em ambientes hostis, abrangendo comunidades clandestinas, fóruns de cibercrime, mercados negros digitais, redes *Peer-to-Peer* (P2P), repositórios de vazamento de dados (como *paste sites*) e canais privados de mensageria não supervisionados. O escopo de rastreamento deve suportar a configuração de múltiplos identificadores corporativos simultâneos, incluindo blocos de endereços IP públicos, nomenclaturas de projetos sensíveis e, fundamentalmente, os domínios de e-mail corporativo da instituição, suportando a volumetria de milhares de contas ativas. Ao detectar um incidente de exposição, a plataforma deve categorizar a severidade do vazamento e tentar

inferir a origem dos dados, distinguindo analiticamente se o comprometimento é fruto de uma violação direta na infraestrutura da organização, de um ataque à cadeia de suprimentos (*Supply Chain Attack*) envolvendo terceiros, ou da infecção de dispositivos de usuários finais por *malwares* do tipo *Infostealer*.

MECANISMOS DE SEGURANÇA, PROTEÇÃO DE MARCA E CONFORMIDADE

Como mecanismo essencial de proteção à reputação institucional, a solução deve possuir recursos voltados à detecção de fraudes baseadas em engenharia social, identificando proativamente o registro de domínios maliciosos que utilizem técnicas de *typosquatting* ou caracteres homógrafos (domínios visualmente idênticos ou com grafia similar ao da contratante) com o intuito de hospedar páginas falsas para captura de credenciais. No tange à privacidade e conformidade com a Lei Geral de Proteção de Dados (LGPD), a plataforma deve fornecer visibilidade granular sobre credenciais comprometidas exibindo as senhas de forma parcialmente ofuscada, permitindo a validação de risco pela equipe de resposta a incidentes sem expor o dado sensível em texto claro. Adicionalmente, o sistema deve possuir algoritmos para identificar a exposição de outros Dados Pessoais Identificáveis (PII), subsidiando o Encarregado de Dados (DPO) com evidências técnicas para a eventual notificação de incidentes à autoridade reguladora.

CAPACIDADES ANALÍTICAS OU DE INTELIGÊNCIA

Para viabilizar a compreensão de cenários de ameaça complexos, a plataforma deve disponibilizar uma interface de mapeamento analítico baseada em Grafos de Relacionamento. Esta funcionalidade deve converter a massa de dados textuais e metadados coletados em uma representação visual dinâmica (composta por nós e arestas), permitindo que os analistas de segurança explorem de forma interativa as conexões e correlações ocultas entre domínios fraudulentos, endereços IP maliciosos, servidores de Comando e Controle (C2) e contas de e-mail vazadas. O módulo deve ser potencializado por motores de Inteligência Artificial capazes de processar esses grandes volumes de dados brutos (*dumps*), gerando relatórios executivos interpretativos que expliquem o nível de severidade da exposição externa e prescrevam táticas imediatas para o endurecimento (*hardening*) da superfície de ataque corporativa.

INTEGRAÇÃO COM OUTROS SISTEMAS E ORQUESTRAÇÃO UNIFICADA

Para garantir a integridade da arquitetura de defesa proposta, é requisito técnico obrigatório que este módulo de Inteligência e Proteção de Marca não opere como um silo informacional isolado. Todos os achados externos, vulnerabilidades de fronteira e credenciais vazadas identificados por este componente devem ser transmitidos e consumidos nativamente pela Plataforma Unificada de Cibersegurança (*Core* - Item 01), devendo estes dados alimentar dinamicamente o algoritmo central de cálculo de risco cibernético (*Risk Score*). Ademais, a solução deve oferecer integração, via Interface de Programação de Aplicações (API) ou *plugins* homologados, com serviços de diretório institucionais (como Active Directory corporativo). Essa integração tem como finalidade habilitar o subsistema de Orquestração (SOAR) a disparar gatilhos de resposta automatizada, viabilizando ações como a imposição mandatória de redefinição de senhas, bloqueio condicional de acesso ou revogação de sessões ativas para

usuários cujas credenciais tenham sido detectadas em vazamentos classificados com alto índice de confiabilidade.

Item 03 PROTEÇÃO DE ENDPOINT (EDR/EPP/XDR) INTEGRADA
Agente unificado para proteção de estações/servidores. Deve alimentar o Item 1.

DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica estabelece os requisitos obrigatórios para a contratação de um subsistema unificado de Proteção, Detecção e Resposta em Endpoints (EDR/XDR), concebido para atuar como a principal linha de defesa ativa e sensor de telemetria nos ativos computacionais da organização. A finalidade primária deste módulo é substituir as abordagens legadas de antivírus baseadas puramente em assinaturas estáticas, implementando agentes de software avançados que operam de forma contínua em estações de trabalho e servidores físicos ou virtualizados. Este componente tem o objetivo de prover visibilidade granular sobre a execução de processos locais, prevenir a infecção por códigos maliciosos avançados, conter movimentações laterais e fornecer os artefatos técnicos necessários para a resposta a incidentes cibernéticos, atuando de forma indissociável do ecossistema central de segurança da contratante.

REQUISITOS TÉCNICOS E FUNCIONAMENTO INTERNO
O funcionamento técnico do módulo baseia-se na implantação de agentes de software leves e multiplataforma, exigindo-se compatibilidade nativa e simultânea com os sistemas operacionais da família Windows, distribuições Linux corporativas e ambientes macOS. Estes agentes devem ser projetados para operar com baixíssimo consumo de recursos computacionais (CPU e memória), garantindo que as operações de segurança não degradem a performance dos serviços de negócio. O mecanismo interno do agente deve atuar como um sensor de alta fidelidade, capaz de coletar, em tempo real, uma vasta gama de telemetria do sistema operacional, englobando a criação e o encerramento de processos, modificações em chaves de registro crítico, estabelecimento de conexões de rede ativas (entrada e saída) e alterações no sistema de arquivos. Como requisito de segurança da comunicação, toda a massa de dados coletada pelos agentes deve ser transmitida de forma estritamente criptografada para o servidor central da plataforma, onde um motor de decodificação normalizará os eventos brutos para análise imediata.

CAPACIDADES OPERACIONAIS, ANÁLISE COMPORTAMENTAL E ANTI-RANSOMWARE
Para garantir a defesa contra vetores de ataque modernos, o módulo deve ser provido de capacidades avançadas de Análise Comportamental Heurística. O motor de detecção não supervisionado deve monitorar continuamente padrões de atividade anômalos que indiquem a presença de malware sofisticado, ameaças fileless (sem arquivo) ou ataques em andamento. Como exigência operacional crítica, o sistema deve possuir mecanismos específicos para a detecção precoce e mitigação de Ransomware, identificando comportamentos inerentes a esta classe de ameaça, tais como a modificação ou criptografia massiva de arquivos em um curto espaço de tempo, tentativas de exclusão de

cópias de sombra do sistema (shadow copies) ou a injeção de código malicioso em processos legítimos do sistema operacional. Complementarmente à heurística, a solução deve incorporar um módulo de Monitoramento de Integridade de Arquivos (FIM - File Integrity Monitoring), com a capacidade de estabelecer linhas de base (baselines) comportamentais de arquivos críticos e diretórios de configuração, disparando alertas contextuais imediatos contendo a tríade investigativa ("quem, quando e o quê") sempre que houver modificações, criações ou exclusões não autorizadas.

CAPACIDADES ANALÍTICAS, INTELIGÊNCIA DE AMEAÇAS E VALIDAÇÃO DE RISCO

A fim de elevar a capacidade de detecção a um nível de estado da arte, o agente deve possuir integração automatizada com redes globais de Inteligência de Ameaças (Threat Intelligence), consumindo continuamente feeds dinâmicos de reputação de endereços IP, hashes de arquivos maliciosos e domínios de Comando e Controle (C2). Esta inteligência aplicada em tempo real deve viabilizar a identificação de Indicadores de Comprometimento (IoCs) e ameaças de dia zero (0-day) assim que observadas na rede mundial. Adicionalmente, é requisito funcional mandatório e distintivo que a solução possua um mecanismo de validação de risco de vulnerabilidades. O sistema não deve se limitar a reportar a existência de uma falha (CVE) no endpoint, devendo verificar autonomamente, em repositórios públicos e privados, a existência de códigos de exploração (exploits) armados para aquela vulnerabilidade específica. Caso confirmada a existência do exploit, a plataforma deve correlacionar criticamente este dado e disponibilizar o arquivo, script ou documento técnico associado para download seguro e análise pela equipe de defesa. Ademais, o módulo deve utilizar Inteligência Artificial Generativa para processar o volume massivo de logs do agente, traduzindo as detecções para a taxonomia da matriz MITRE ATT&CK e gerando narrativas textuais inteligíveis que resumam a cadeia do ataque e sugiram ações de remediação.

INTEGRAÇÃO OBRIGATÓRIA COM O ECOSSISTEMA E ORQUESTRAÇÃO (SOAR)

Como premissa fundamental da arquitetura unificada, este módulo de Proteção de Endpoint não poderá operar como uma ferramenta apartada (silo), sendo imperativa sua integração bidirecional e nativa com a Plataforma Unificada de Cibersegurança (Core - Item 01). Toda a telemetria, metadados de processos, alertas heurísticos e falhas de configuração coletados pelos agentes de EDR devem ser transmitidos ininterruptamente ao console central, atuando como a principal fonte de alimentação dinâmica para o algoritmo de cálculo de risco unificado (Risk Score) da organização. Sob a ótica da resposta a incidentes, os agentes instalados nos endpoints devem atuar como braços executores do subsistema de Orquestração (SOAR). Isso significa que as regras estabelecidas nos Playbooks automatizados da plataforma matriz devem ser capazes de enviar comandos remotos de execução imediata aos agentes EDR, viabilizando ações de contenção crítica, tais como o isolamento lógico da interface de rede do host comprometido, o encerramento forçado de árvores de processos maliciosos e a quarentena de arquivos suspeitos, sem a necessidade de intervenção física da equipe de suporte técnico.

MECANISMOS DE SEGURANÇA E REQUISITOS DE CONFORMIDADE
Para assegurar a resiliência do próprio mecanismo de defesa, os agentes de endpoint devem ser dotados de tecnologias de autoproteção (Anti-Tampering), impedindo que administradores locais não autorizados, scripts maliciosos ou ferramentas de bypass desativem, desinstalem ou adulterem os serviços de monitoramento do EDR. No âmbito da governança e auditoria, a solução deve prover ferramentas robustas de gestão de parque tecnológico, permitindo a exportação estruturada do inventário completo de hardware e software de todos os ativos monitorados. Por fim, o módulo deve incluir capacidades de verificação de postura (Posture Assessment), auditando continuamente a conformidade das configurações locais dos endpoints em relação a frameworks regulatórios e normativos exigidos pela instituição, emitindo relatórios de aderência a padrões como o PCI-DSS, diretrizes do NIST e requisitos técnicos de segurança exigidos pela Lei Geral de Proteção de Dados (LGPD).

ITEM 04 – SEGURANÇA DE CONTAINERS
Módulo de proteção para ambientes de conteinerização (Docker/Kubernetes) totalmente integrado à plataforma central (Item 1).

ESPECIFICAÇÃO TÉCNICA: MÓDULO DE SEGURANÇA DE CONTÊINERES E PROTEÇÃO EM TEMPO REAL (CWPP/KSPM)
DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica estabelece os parâmetros obrigatórios para a contratação de um subsistema especializado na proteção de cargas de trabalho nativas em nuvem (*Cloud Workload Protection Platform* - CWPP) e na Gestão de Postura de Segurança de Orquestradores (*Kubernetes Security Posture Management* - KSPM). A finalidade deste módulo é garantir a visibilidade, a governança e a defesa em profundidade de ambientes de conteinerização (com suporte mandatório a plataformas padrão de mercado, como Docker e Kubernetes), operando de forma contínua durante todo o ciclo de vida da aplicação. Dada a natureza efêmera, elástica e distribuída dos contêineres, este componente visa impedir que tais infraestruturas se tornem pontos cegos na arquitetura de defesa cibernética da organização, aplicando controles de segurança rigorosos desde a fase de construção e integração contínua (CI/CD) até a execução em ambiente de produção (*Runtime*).

REQUISITOS FUNCIONAIS DE ANÁLISE ESTÁTICA E GESTÃO DE POSTURA
Para atuar de forma preventiva (*Shift-Left Security*), o módulo deve possuir capacidade técnica avançada para a varredura profunda de imagens de contêineres, integrando-se nativamente aos repositórios de imagens (*Container Registries*) utilizados pela instituição. O mecanismo de análise estática deve ser capaz de inspecionar as múltiplas camadas das imagens para identificar Vulnerabilidades e Exposições Comuns (CVEs) presentes nos pacotes base do sistema operacional, além de executar a Análise de Composição de Software (SCA) para descobrir falhas estruturais em bibliotecas e dependências de código de terceiros. Complementarmente à detecção de falhas em pacotes, o subsistema deve auditar a Infraestrutura como Código (IaC), inspecionando manifestos e arquivos de configuração do Kubernetes em busca de violações de privilégio, excesso de permissões e desvios de conformidade, baseando-se

rigorosamente nas diretrizes de segurança consolidadas pelo *Center for Internet Security* (CIS Benchmarks).

CAPACIDADES OPERACIONAIS DE PROTEÇÃO EM TEMPO REAL (RUNTIME SECURITY)

A proteção das cargas de trabalho em execução (*Runtime Security*) exige que a ferramenta empregue tecnologias de instrumentação de baixo nível baseadas na interceptação de chamadas de sistema (*syscalls*) ou na utilização de tecnologias modernas de núcleo do sistema operacional, como o eBPF (*Extended Berkeley Packet Filter*). Esta abordagem arquitetural é mandatória para garantir um monitoramento de alta performance e alta fidelidade, assegurando que as operações de segurança não insiram latência prejudicial ao ambiente de produção. O motor de análise comportamental deve detectar anomalias e tentativas de exploração em tempo real, disparando alertas críticos diante de eventos não autorizados. Tais eventos incluem, obrigatoriamente, a abertura de *shells* interativos (terminais) dentro de contêineres em execução, tentativas de gravação ou modificação em diretórios sensíveis do nó hospedeiro (*host*), movimentações características de escalonamento de privilégios, execução de binários suspeitos não previstos na imagem original e o estabelecimento de conexões de rede anômalas com servidores externos ou de Comando e Controle (C2).

MECANISMOS DE SEGURANÇA E REMEDIAÇÃO AUTOMATIZADA

O subsistema de segurança de contêineres deve transcender a postura puramente passiva e analítica, suportando mecanismos ativos de bloqueio e remediação automatizada para preservar a integridade do *cluster*. Durante o estágio de implantação (*Deploy*), a solução deve atuar como um Controlador de Admissão (*Admission Controller* ou *Validating Webhook*) diretamente integrado à API do Kubernetes, detendo a autoridade técnica para impedir autonomamente a implantação de imagens que contenham vulnerabilidades de severidade crítica ou que violem as políticas de governança estabelecidas. No estágio de execução contínua (*Runtime*), caso um comportamento malicioso ou um desvio grave de política seja detectado e confirmado pelo motor heurístico, o sistema deve possuir a capacidade de intervir imediatamente no ambiente, executando ações de mitigação autônomas que incluem a pausa (*pause*) temporária do serviço, o isolamento de tráfego de rede do *pod* ou o encerramento forçado (*kill/terminate*) do contêiner comprometido, estancando assim o risco de movimentação lateral da ameaça.

INTEGRAÇÃO OBRIGATÓRIA COM O ECOSSISTEMA E ORQUESTRAÇÃO (SOAR)

Como premissa inegociável da arquitetura de segurança proposta, este módulo não poderá operar de forma isolada, sendo exigida sua integração nativa e bidirecional com a Plataforma Unificada de Cibersegurança (*Core* - Item 01). Todos os eventos de violação de *runtime*, falhas de conformidade e o inventário de imagens vulneráveis devem ser transmitidos ao console central, alimentando dinamicamente o mecanismo algorítmico de cálculo de risco cibernético (*Risk Score*) da organização. Sob a perspectiva de resposta a incidentes, os alertas gerados nos ambientes de conteinerização devem atuar como gatilhos operacionais nativos para o subsistema de Automação de Resposta (SOAR).

Essa interoperabilidade permitirá que os administradores modelem *Playbooks* complexos, onde um ataque detectado em um contêiner possa acionar, simultaneamente, o encerramento do *pod* vulnerável e o bloqueio do endereço IP do atacante no *firewall* de borda físico da instituição. Ademais, todas as detecções táticas devem ser mapeadas automaticamente para a matriz MITRE ATT&CK voltada para *Containers*.

REQUISITOS DE CONFORMIDADE E CAPACIDADES ANALÍTICAS (DFIR)
Considerando a volatilidade intrínseca dos ambientes conteinerizados, onde as instâncias são destruídas e recriadas constantemente, a plataforma deve possuir capacidades avançadas de preservação forense. Antes do encerramento de um contêiner comprometido, o módulo deve capturar artefatos técnicos essenciais (como a árvore de execução de processos, captura de pacotes de rede e metadados de acesso), canalizando essas evidências para o módulo de Perícia Digital e Resposta a Incidentes (DFIR) do console central. Para garantir a conformidade e a validade jurídica no tratamento de incidentes (art. 369 do CPC/2015), os *hashes* criptográficos referentes aos laudos de vulnerabilidades de imagens e aos registros de auditoria de intrusão em contêineres deverão ser persistidos na tecnologia de livro-razão distribuído (*Blockchain*) da plataforma *Core*, assegurando imutabilidade pericial plena frente a ameaças direcionadas à infraestrutura em nuvem.

CHAVE DE SEGURANÇA DE HARDWARE (FIDO2)
Token físico USB/NFC resistente a phishing, para autenticação dos usuários.

DISPOSITIVOS DE HARDWARE PARA AUTENTICAÇÃO MULTIFATORIAL (CHAVES FIDO2)

DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica estabelece os requisitos obrigatórios para o fornecimento de dispositivos físicos de segurança (Material Permanente), caracterizados como tokens de hardware para Autenticação Multifatorial (MFA) baseada em criptografia assimétrica. A finalidade primária destes dispositivos é atuar como uma barreira física e intransponível contra vetores modernos de engenharia social, mitigando de forma definitiva ataques de roubo de credenciais, força bruta e interceptação de sessões por meio de intermediários maliciosos (Adversary-in-the-Middle - AiTM). Estes componentes tangíveis materializam o conceito de "o que o usuário possui", ancorando a identidade digital em um ativo físico de alta segurança, sendo fundamentais para a proteção do acesso lógico a sistemas críticos, estações de trabalho e, impreterivelmente, às interfaces administrativas da Plataforma Unificada de Operações de Segurança (Item 01).

REQUISITOS TÉCNICOS E PADRÕES CRIPTOGRÁFICOS
Para garantir ampla interoperabilidade, os dispositivos ofertados devem suportar nativa e simultaneamente múltiplos protocolos de autenticação reconhecidos internacionalmente. É requisito mandatório o suporte integral ao padrão FIDO2 (incluindo as especificações WebAuthn e CTAP1/CTAP2), viabilizando fluxos de autenticação robustos sem a necessidade de senhas (Passwordless). Complementarmente, a fim de garantir suporte a sistemas corporativos legados,

os tokens devem incorporar capacidades de autenticação via Smart Card (compatível com o padrão PIV - Personal Identity Verification), bem como suportar protocolos de senhas de uso único, incluindo OATH-TOTP (Time-based One-Time Password) e HOTP (HMAC-based One-Time Password). No tange à conectividade, os dispositivos devem possuir interfaces híbridas, disponibilizando conexão física via portas USB (padrão USB-A ou USB-C, a depender do inventário da contratante) e transmissão sem fio via tecnologia NFC (Near Field Communication), permitindo a autenticação segura também em dispositivos móveis compatíveis.

REQUISITOS FÍSICOS, RESILIÊNCIA E DURABILIDADE

Considerando o caráter de uso contínuo e diário pelos servidores e administradores de TI da organização, os tokens de hardware devem ser projetados sob estritos padrões de durabilidade industrial. A estrutura física dos dispositivos deve ser confeccionada em material de alta resistência, suportando esmagamentos acidentais e impactos rotineiros sem comprometer o elemento seguro (Secure Element) interno. Adicionalmente, os componentes eletrônicos devem ser hermeticamente selados, conferindo ao dispositivo resistência à água (padrão IP68 ou equivalente) e à intrusão de poeira. É terminantemente vedado o fornecimento de dispositivos que dependam de baterias internas para seu funcionamento ou que possuam partes mecânicas móveis (como botões retráteis), eliminando assim a degradação natural por desgaste físico ou esgotamento de carga e assegurando uma vida útil prolongada do ativo.

MECANISMOS DE SEGURANÇA E PREVENÇÃO A ATAQUES (ANTI-PHISHING)

O mecanismo de funcionamento interno do dispositivo deve ser intrinsecamente resistente a campanhas de phishing direcionadas. Diferentemente de códigos SMS ou aplicativos geradores de tokens em smartphones, a autenticação via FIDO2 realizada por este hardware vincula criptograficamente o desafio de login ao domínio de origem real (Origin Binding). Caso um usuário seja induzido a acessar um site falso (com domínio visualmente similar), o token de hardware reconhecerá a divergência criptográfica e não liberará a credencial de acesso, neutralizando a ameaça de forma silenciosa. Além disso, para que qualquer operação criptográfica seja executada e transmitida ao sistema, o dispositivo deve exigir prova de presença humana, materializada através do toque físico do usuário em um sensor capacitivo localizado na superfície do token, garantindo que malwares de acesso remoto não possam acionar a chave de forma autônoma e invisível.

INTEGRAÇÃO COM A PLATAFORMA DE SEGURANÇA E GESTÃO DE IDENTIDADE (IAM)

A aplicabilidade dos dispositivos deve estar intrinsecamente alinhada à arquitetura do ecossistema tecnológico da contratante. Os tokens FIDO2 deverão integrar-se nativamente e sem fricção com as plataformas de Gerenciamento de Identidade e Acesso (IAM) corporativas, notadamente o Microsoft Active Directory (On-Premises) e o Entra ID (Azure AD), habilitando o login seguro nas estações de trabalho do domínio. De forma crítica para a segurança da gestão cibernética, o uso destas chaves de hardware será configurado como requisito obrigatório para o acesso de analistas, auditores e

administradores ao console central da Plataforma Unificada de Cibersegurança (Item 01). Esta integração garante que a camada de Controle de Acesso Baseado em Funções (RBAC) do sistema de segurança não possa ser subvertida mediante o simples comprometimento de uma senha em texto claro.

REQUISITOS DE CONFORMIDADE E SUPORTE OPERACIONAL
Os dispositivos de hardware fornecidos devem ser comprovadamente certificados pela FIDO Alliance, garantindo aderência rigorosa às especificações do protocolo global. No âmbito da sustentabilidade e governança ambiental exigidas em contratações públicas, a fabricação e composição dos materiais do token devem respeitar a diretiva RoHS (Restriction of Hazardous Substances), comprovando a ausência de substâncias altamente tóxicas. Sob a ótica de usabilidade, a operação dos dispositivos deve seguir o paradigma Plug and Play, sendo reconhecidos nativamente como dispositivos de interface humana (HID) pelos sistemas operacionais modernos (Windows 10/11, distribuições Linux e macOS), isentando a equipe de suporte técnico da organização da necessidade de instalar e gerenciar drivers proprietários complexos nas estações de trabalho dos usuários finais.

Item 06 - OPERAÇÃO DE SEGURANÇA (SOC) E SUPORTE 24X7
Monitoramento contínuo da plataforma unificada.

SERVIÇO DE OPERAÇÃO DE SEGURANÇA (SOC) E SUPORTE TÉCNICO CONTINUADO 24X7

DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica estabelece as diretrizes e os requisitos mandatórios para a contratação de Serviços Gerenciados de Segurança Cibernética, estruturados sob o formato de um Centro de Operações de Segurança (SOC - *Security Operations Center*). A finalidade primária deste serviço é prover o componente humano especializado e ininterrupto necessário para operar, gerenciar e extrair inteligência acionável da Plataforma Unificada de Cibersegurança (Item 01). Considerando que a mera aquisição de tecnologias defensivas, por mais avançadas que sejam, é insuficiente para deter adversários persistentes, este módulo de serviço atua como o braço operacional da organização. Seu objetivo é garantir a vigilância contínua do ambiente tecnológico, viabilizando a triagem de alertas, a mitigação de falsos positivos, a caça proativa a ameaças e a execução orquestrada de procedimentos de resposta a incidentes, reduzindo drasticamente as métricas de Tempo Médio de Detecção (MTTD) e Tempo Médio de Resposta (MTTR) da instituição.

CAPACIDADES OPERACIONAIS DE MONITORAMENTO E TRIAGEM
O serviço de SOC deve operar sob um regime de disponibilidade absoluta, cobrindo 24 horas por dia, 7 dias por semana e 365 dias por ano (24x7x365). A operação deve ser estruturada em um modelo de atendimento em camadas (Tiers N1, N2 e N3), garantindo o escalonamento adequado conforme a criticidade e a complexidade técnica do evento adverso. Os analistas de Nível 1 atuarão na linha de frente, realizando a triagem inicial e a qualificação do volume massivo de eventos brutos capturados pelos sensores de *Endpoint* (EDR), varreduras de vulnerabilidade e interceptações de rede, filtrando ruídos

operacionais e eliminando a fadiga de alertas. Uma vez que um evento seja classificado como um incidente real, o caso deverá ser imediatamente escalonado para o Nível 2, responsável pela contenção técnica, enquanto incidentes críticos (como tentativas de extorsão por *Ransomware* ou vazamento de dados em larga escala) envolverão especialistas de Nível 3 para a condução de análises profundas, engenharia reversa e Perícia Digital (*Digital Forensics*).

FUNCIONAMENTO TÉCNICO DE RESPOSTA A INCIDENTES E THREAT HUNTING

A equipe de operação de segurança deverá transcender a postura reativa de aguardar o acionamento de alarmes no *dashboard*. É exigência operacional a execução periódica de rotinas de Caça a Ameaças (*Threat Hunting*), utilizando algoritmos de aprendizado de máquina da plataforma e as correlações em grafos para buscar proativamente intrusões furtivas, ameaças persistentes avançadas (APTs) e movimentações laterais que não tenham acionado assinaturas estáticas de detecção. Durante a condução de um incidente, os operadores do SOC deverão utilizar obrigatoriamente a taxonomia da matriz MITRE ATT&CK para descrever o comportamento do adversário. Para a resposta, a equipe deverá acionar os fluxos de automação (*Playbooks*) predefinidos no módulo SOAR da plataforma central, executando comandos remotos de mitigação, como o isolamento lógico de interfaces de rede, a terminação de árvores de processos maliciosos e a inserção de *hashes* em listas de bloqueio globais (*blacklists*).

INTEGRAÇÃO COM OUTROS SISTEMAS E ORQUESTRAÇÃO UNIFICADA

Como requisito arquitetural e procedimental inflexível, a equipe do SOC fornecida pela contratada deverá operar exclusivamente através da interface centralizada da Plataforma Unificada de Cibersegurança (*Single Pane of Glass* - Item 01) adquirida pela instituição. É terminantemente vedada a utilização de consoles de gerenciamento desconexos ou *softwares* proprietários externos do fornecedor que fragmentem a visibilidade do ambiente e impeçam a auditoria das ações pela equipe interna da contratante. No âmbito da gestão de incidentes, os analistas do SOC deverão alimentar o módulo de *Ticketing* nativo, o qual, por sua vez, deve possuir integração bidirecional via API RESTful com o sistema de Gerenciamento de Serviços de TI (ITSM) utilizado pela organização. Essa integração síncrona garante que a equipe de infraestrutura local e a equipe do SOC externo trabalhem em uníssono, compartilhando o mesmo fluxo de informações, aprovações e cronogramas de mitigação.

REQUISITOS FUNCIONAIS DE SUPORTE TÉCNICO À PLATAFORMA (HEALTH CHECK)

Para além do monitoramento exclusivo de ameaças, o serviço continuado abrange a gestão, a manutenção e a sustentação tecnológica do próprio ecossistema de cibersegurança. A equipe técnica da contratada será responsável por realizar configurações, ajustes finos (*tuning*) de políticas de bloqueio para evitar falsos positivos que impactem as operações de negócio, e garantir a integridade de funcionamento dos agentes instalados (EDR/CWPP) em servidores legados e modernos. O escopo compreende a aplicação transparente de atualizações de segurança (*patches*), atualização de repositórios de testes de vulnerabilidade (NVTs) e o saneamento de *bugs* ou inconsistências operacionais do *Software as a Service* (SaaS). A prestação

deste suporte técnico, seja para sanar dúvidas operacionais ou corrigir falhas sistêmicas da ferramenta, será balizada por rigorosos Acordos de Nível de Serviço (SLA), com tempos de resposta e solução vinculados diretamente à severidade técnica da solicitação aberta pela contratante.

MECANISMOS DE SEGURANÇA, EVIDÊNCIAS LEGAIS E CONFORMIDADE
Tendo em vista o acesso privilegiado da equipe do SOC a dados sensíveis e aos controles vitais da infraestrutura governamental/corporativa, a operação deverá estar submetida a estritos padrões de Governança, Risco e Conformidade (GRC). Todos os analistas da contratada deverão acessar a plataforma mediante autenticação multifatorial estrita com o uso de chaves de *hardware* (FIDO2) e sob um modelo rigoroso de menor privilégio (*Role-Based Access Control* - RBAC). Durante a investigação de violações de segurança, os artefatos coletados pelo SOC (como captura de pacotes, *dumps* de memória e *logs* de acesso) deverão ser formalmente custodiados no módulo de Resposta a Incidentes (DFIR). Visando resguardar a cadeia de custódia e assegurar a validade jurídica das ações da equipe do SOC em processos litigiosos ou de fiscalização, os *hashes* criptográficos que atestam a integridade dos relatórios técnicos de encerramento de incidentes deverão ser automaticamente persistidos na tecnologia de livro-razão distribuído (*Blockchain*), impossibilitando qualquer alteração retroativa das evidências documentadas pelos operadores.

Item 07 - IMPLANTAÇÃO, INTEGRAÇÃO E TREINAMENTO OFICIAL
Setup da solução unificada, integração com legados e treinamento certificado para a equipe técnica.

SERVIÇOS ESPECIALIZADOS DE IMPLANTAÇÃO, INTEGRAÇÃO DE ARQUITETURA E TREINAMENTO OFICIAL

DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica define os parâmetros, as metodologias e os requisitos obrigatórios para a prestação de serviços técnicos especializados de implantação, configuração, integração de sistemas e transferência de conhecimento (*handover*). A finalidade central deste conjunto de serviços é operacionalizar e extrair o máximo valor tecnológico da Plataforma Unificada de Operações de Segurança (Item 01) e de seus respectivos módulos satélites (EDR, Contêineres, OSINT, Phishing e NAC). Considerando a criticidade do ambiente computacional da contratante, este serviço visa garantir que a transição tecnológica ocorra de forma fluida, sem disrupção das atividades de negócio, adaptando as funcionalidades da solução "de prateleira" (*Software as a Service*) à topologia de rede, às políticas de governança e às particularidades do parque legado da instituição, culminando na total capacitação da equipe técnica interna.

REQUISITOS TÉCNICOS DE IMPLANTAÇÃO E ASSESSMENT DE INFRAESTRUTURA
A execução dos serviços de implantação deve ser obrigatoriamente conduzida sob uma metodologia formal de gerenciamento de projetos, exigindo a designação de um gerente de projetos certificado para a condução do cronograma físico-financeiro. A fase inaugural da implantação requer a

realização de um *Assessment* (diagnóstico) profundo do ambiente tecnológico da organização, com o objetivo de mapear a superfície de ataque, identificar dependências sistêmicas e catalogar a volumetria exata de ativos e instâncias virtuais. A partir deste mapeamento, a contratada procederá com o provisionamento do ambiente em nuvem (*tenant*) e a distribuição massiva dos agentes de telemetria (EDR/XDR) nos *endpoints* e servidores. Durante esta etapa, é requisito técnico crítico a parametrização cuidadosa dos motores de varredura de vulnerabilidades, estabelecendo janelas de manutenção e perfis de *scan* customizados para garantir que a inspeção de sistemas operacionais legados (como Windows Server 2008/2012 ou distribuições Linux obsoletas) ocorra de maneira não intrusiva, evitando sobrecargas de processamento ou quedas de serviço.

INTEGRAÇÃO COM OUTROS SISTEMAS E AMBIENTES LEGADOS

Para que o conceito de "Painel Único de Vidro" se concretize, a implantação exige um esforço substancial de integração bidirecional entre a nova plataforma e o ecossistema legado da contratante. A equipe especializada deverá configurar a interoperabilidade da solução com os serviços de diretório institucionais (Microsoft Active Directory ou LDAP), viabilizando o Controle de Acesso Baseado em Funções (RBAC) e o provisionamento de autenticação forte com o uso das chaves físicas FIDO2 (Item 05). No âmbito da defesa de perímetro e resposta, é mandatória a integração nativa ou via *middleware* (utilizando APIs RESTful, SOAP ou JSON) com os *firewalls* corporativos preexistentes, permitindo o intercâmbio de inteligência e o bloqueio automatizado de endereços IP anômalos. Adicionalmente, a contratada deverá estabelecer a orquestração síncrona entre o sistema de gerenciamento de casos da plataforma de segurança e o *software* de Gerenciamento de Serviços de TI (ITSM) oficial da organização, garantindo que o ciclo de vida dos incidentes seja unificado e auditável em ambas as pontas.

CAPACIDADES OPERACIONAIS DE CUSTOMIZAÇÃO E ORQUESTRAÇÃO (SOAR)

A fase de configuração não deve se restringir às opções padrão de fábrica (*out-of-the-box*). Os arquitetos de segurança da contratada deverão modelar e implementar os painéis de visualização (*dashboards*) e os algoritmos de cálculo de risco (*Risk Score*) refletindo a exata criticidade dos diferentes grupos de ativos da instituição (exemplo: segmentando o risco de servidores de banco de dados do risco de estações de atendimento). No tange à automação, o serviço compreende o desenvolvimento e a homologação dos primeiros *Playbooks* no módulo de Orquestração, Automação e Resposta (SOAR). A equipe deverá traduzir as políticas de resposta a incidentes da organização em fluxos de trabalho lógicos que contemplem gatilhos automáticos de contenção, como o isolamento de instâncias afetadas por *Ransomware* ou a suspensão de contêineres maliciosos, testando exaustivamente estas automações em ambientes de homologação antes de sua efetivação no ambiente de produção.

REQUISITOS FUNCIONAIS DE TREINAMENTO E TRANSFERÊNCIA DE CONHECIMENTO

Para garantir a sustentabilidade e a independência operacional da instituição, o fornecimento inclui a execução de um programa de treinamento técnico oficial e

certificado. A capacitação deve ser direcionada aos administradores de rede, analistas do SOC interno e membros da equipe de governança (DPO), abordando a operação cotidiana da plataforma unificada, a análise de *logs* comportamentais, a investigação pericial e a validação de testes de *phishing*. O currículo do treinamento deve abranger a interpretação das táticas e técnicas da matriz MITRE ATT&CK evidenciadas pela ferramenta, bem como a instrução prática para a criação autônoma de novos *Playbooks* de automação e a extração de evidências imutáveis registradas na *Blockchain* da plataforma. O treinamento deverá ser ministrado integralmente no idioma português do Brasil (PT-BR), com fornecimento de documentação técnica detalhada, diagramas de arquitetura as-built (como construído) e emissão de certificados individuais de conclusão.

MECANISMOS DE SEGURANÇA DO PROJETO E REQUISITOS DE CONFORMIDADE

Toda a execução dos serviços de implantação e integração estará sujeita aos mais rigorosos preceitos de conformidade e segurança da informação. Os profissionais técnicos alocados pela contratada (arquitetos, engenheiros e especialistas em integração) deverão comprovar alta qualificação por meio de certificações reconhecidas internacionalmente (tais como CISSP, Security+, PMP) e assinar Termos de Confidencialidade (NDA) específicos, dada a exposição privilegiada à infraestrutura crítica e às vulnerabilidades governamentais durante o período de *setup*. O acesso remoto ou presencial destes profissionais ao ambiente da contratante para fins de configuração ocorrerá estritamente sob o princípio do menor privilégio, monitorado por sistemas de cofre de senhas (PAM) quando aplicável. A aceitação final dos serviços prestados estará condicionada à aprovação formal de um Caderno de Testes de Aceitação, atestando que todas as integrações, módulos e requisitos legais estipulados no processo licitatório encontram-se plenamente operacionais.

Item 08 - GESTÃO DE VULNERABILIDADES E APOIO À REMEDIAÇÃO

Serviço continuado de análise, priorização e suporte à correção de falhas (Blue Team).

SERVIÇO CONTINUADO DE GESTÃO DE VULNERABILIDADES E APOIO À REMEDIAÇÃO (BLUE TEAM)

DESCRIÇÃO CONCEITUAL E FINALIDADE

A presente especificação técnica define os requisitos obrigatórios para a contratação de serviços técnicos especializados e continuados de Gestão do Ciclo de Vida de Vulnerabilidades (*Vulnerability Management*). A finalidade primária deste serviço é preencher a lacuna operacional crônica existente entre a detecção tecnológica de falhas e a mitigação efetiva do risco, atuando como uma equipe de defesa cibernética dedicada (*Blue Team*). Em vez de apenas reportar listagens brutas geradas pelos motores de varredura da Plataforma Unificada (Item 01), este serviço visa transformar volumes massivos de dados técnicos em inteligência acionável. O objetivo central é apoiar diretamente e de forma consultiva as equipes de infraestrutura, redes e desenvolvimento de sistemas da contratante na priorização, no planejamento estratégico e na

aplicação segura de correções (*patches*) e ajustes de configuração de segurança (*hardening*).

FUNCIONAMENTO TÉCNICO DE CURADORIA E TRIAGEM

O funcionamento técnico do serviço baseia-se na curadoria analítica ininterrupta dos achados provenientes dos motores de varredura autenticada e não autenticada. Os especialistas da contratada deverão realizar a triagem minuciosa dos relatórios gerados pelo sistema, executando a eliminação metodológica de falsos positivos e a reclassificação do risco real. Esta reclassificação analítica não deve depender exclusivamente do escore base matemático do padrão CVSS (*Common Vulnerability Scoring System*), devendo incorporar obrigatoriamente o contexto arquitetural do ativo afetado — avaliando, por exemplo, se um servidor vulnerável está exposto diretamente à internet ou se encontra protegido em uma rede de gerência restrita. Além disso, a análise deverá cruzar os dados estruturais de vulnerabilidades com os *feeds* globais de Inteligência de Ameaças (*Threat Intelligence*), elevando imediatamente a criticidade de falhas que possuam *exploits* públicos ou que componham a taxonomia de ataques descrita na matriz MITRE ATT&CK.

CAPACIDADES OPERACIONAIS DE PLANEJAMENTO E APOIO À CORREÇÃO (REMEDIAÇÃO)

Como núcleo de seu escopo operacional, a equipe gerenciada deverá elaborar e fornecer, de forma estruturada e periódica, Planos de Ação de Remediação (*Action Plans*). Estes planos transcenderão o mero reporte de problemas, consolidando-se como roteiros executivos e técnicos que detalham estritamente *quais* atualizações devem ser aplicadas, *em quais* grupos de ativos e *qual* o impacto sistêmico esperado (avaliando o risco de instabilidade ou a necessidade de reinicialização de serviços críticos). Para viabilizar a execução da correção, a contratada proverá suporte técnico direto aos administradores da instituição, fornecendo *scripts* de mitigação testados, instruções precisas para a alteração de chaves de registro do sistema operacional e diretrizes para a atualização segura de bibliotecas. Quando a correção definitiva for tecnicamente inviável (especialmente em sistemas legados), a equipe deverá recomendar a adoção de controles compensatórios, como a aplicação de *patches* virtuais (*Virtual Patching*) ou a criação de regras de isolamento no módulo de Controle de Acesso à Rede (NAC).

INTEGRAÇÃO COM OUTROS SISTEMAS E CICLO DE VALIDAÇÃO (RESCAN)

A execução deste serviço deverá estar organicamente atrelada ao ecossistema tecnológico estabelecido. A equipe de gestão de vulnerabilidades operará utilizando primariamente o console centralizado da Plataforma Unificada de Cibersegurança (*Single Pane of Glass* - Item 01) para extrair os dados e fundamentar suas análises. A orquestração e a delegação das tarefas de remediação exigirão integração procedural e sistêmica com a ferramenta de Gerenciamento de Serviços de TI (ITSM) oficial da contratante, garantindo que cada pacote de correção gere um *ticket* rastreável, atrelado a Acordos de Nível de Serviço (SLA) de remediação baseados na criticidade. Após a notificação de que a equipe de infraestrutura interna aplicou as correções recomendadas, o escopo da contratada englobará a execução mandatória de varreduras de

validação (*Rescans*), atestando tecnicamente e de forma independente que a falha foi definitivamente erradicada da superfície de ataque, selando o ciclo de vida da vulnerabilidade.

CAPACIDADES ANALÍTICAS, GESTÃO DE OBSOLESCÊNCIA E ZERO-DAY
No que tange às capacidades analíticas avançadas, o serviço compreenderá a Gestão Contínua de Obsolescência Tecnológica (*End-of-Life / End-of-Support*). A equipe especializada deverá identificar e reportar proativamente sistemas operacionais, *frameworks* de desenvolvimento de *software* e ativos legados que não recebem mais suporte oficial ou atualizações de segurança de seus fabricantes, subsidiando a alta gestão governamental com mapas de risco para o planejamento orçamentário de modernização tecnológica. Em cenários de crise cibernética aguda, caracterizados pela divulgação global de vulnerabilidades críticas de dia zero (*Zero-Day*) que afetem o parque tecnológico da instituição, a equipe atuará em regime de força-tarefa, acionando protocolos emergenciais para mapear a exposição imediata do órgão, sugerir medidas temporárias de contenção de tráfego e alinhar-se ao Centro de Operações de Segurança (SOC - Item 08) para intensificar o monitoramento de IoCs até que o *patch* definitivo seja disponibilizado pela indústria.

REQUISITOS DE CONFORMIDADE E GOVERNANÇA
A prestação contínua do serviço de apoio à remediação deverá estar em estrita conformidade com as exigências de segurança e privacidade estipuladas pela Lei Geral de Proteção de Dados (LGPD) e fortemente alinhada aos controles de gestão de vulnerabilidades previstos na norma ISO/IEC 27001. A contratada será responsável por conduzir comitês técnicos periódicos com os gestores de TI e Segurança da contratante, realizando a prestação de contas (*accountability*) mediante a apresentação do avanço das métricas de correção, da evolução do *Risk Score* global e da redução efetiva da superfície de ataque corporativa. Como garantia de integridade processual, todos os relatórios de conformidade, planos de ação e cadernos de recomendação técnica emitidos pela equipe de *Blue Team* deverão ter seus respectivos *hashes* criptográficos documentados no mecanismo de imutabilidade baseada em tecnologia *Blockchain* (fornecido na plataforma base), assegurando o registro histórico irrefutável e com validade jurídica acerca das diligências adotadas pela Administração Pública na proteção de sua infraestrutura.

Item 09 - MÓDULO DE CONTROLE DE ACESSO À REDE (NAC)
Solução Zero Trust para controle de acesso (802.1x), perfilamento de IoT e Guest, 100% integrada ao Item 1.

MÓDULO DE CONTROLE DE ACESSO À REDE (NAC) E ARQUITETURA ZERO TRUST

DESCRIÇÃO CONCEITUAL E FINALIDADE
A presente especificação técnica estabelece os requisitos mandatórios para a contratação de um subsistema de Controle de Acesso à Rede (NAC - *Network Access Control*), alicerçado nos rigorosos princípios da arquitetura *Zero Trust Network Access* (ZTNA). A finalidade central deste módulo é atuar como o guardião implacável do perímetro de rede corporativo, garantindo que nenhum

dispositivo — seja ele corporativo, pessoal (BYOD), infraestrutura de Internet das Coisas (IoT) ou de visitantes — obtenha conectividade lógica aos recursos da instituição sem prévia identificação, autenticação, perfilamento e validação de conformidade. Em estrito alinhamento com a topologia de defesa em profundidade, este componente não deve atuar como uma solução isolada, mas sim como uma extensão nativa e indissociável da Plataforma Unificada de Operações de Segurança (Item 01), transmutando a visibilidade de ameaças em ações imediatas de contenção na camada de acesso físico e lógico (redes cabeadas, redes sem fio e túneis VPN).

REQUISITOS TÉCNICOS E FUNCIONAMENTO INTERNO DE AUTENTICAÇÃO E PERFILAMENTO

O funcionamento técnico do módulo deve suportar a aplicação universal do protocolo IEEE 802.1X, utilizando métodos de autenticação criptograficamente seguros (tais como EAP-TLS e PEAP) para validar a identidade de usuários e máquinas junto aos serviços de diretório institucionais (Active Directory / LDAP). Tendo em vista a vasta presença de ativos desprovidos de capacidade de autenticação complexa (como câmeras IP, impressoras de rede e sensores IoT), o subsistema deverá empregar mecanismos de *Bypass* de Autenticação por MAC (MAB) intrinsecamente combinados a um motor de Perfilamento de Dispositivos (*Device Profiling*). Este motor de perfilamento deve realizar a inspeção profunda de tráfego e metadados (analisando requisições DHCP, *banners* HTTP, pacotes SNMP e *fingerprints* de *endpoints*) para classificar o tipo de dispositivo com alta precisão e mitigar tentativas de burla baseadas na clonagem (*spoofing*) de endereços MAC, alocando o ativo dinamicamente na rede virtual (VLAN) correspondente ao seu perfil de segurança.

CAPACIDADES OPERACIONAIS DE AVALIAÇÃO DE POSTURA E GESTÃO DE VISITANTES

Para viabilizar a verdadeira premissa do *Zero Trust* ("nunca confie, sempre verifique"), o módulo deve executar a Avaliação de Postura (*Posture Assessment*) em tempo real antes de conceder autorização de acesso à rede. O sistema interrogara o *endpoint* solicitante para atestar o cumprimento das políticas de segurança corporativas, exigindo, por exemplo, que o agente de EDR (Item 03) esteja ativo e atualizado, que não existam vulnerabilidades críticas pendentes de correção e que o sistema operacional esteja devidamente homologado. Ativos reprovados na avaliação de postura deverão ser automaticamente direcionados para uma rede restrita de quarentena ou remediação. Adicionalmente, a ferramenta deverá prover capacidades operacionais avançadas para a Gestão de Visitantes (*Guest Access*), oferecendo um Portal Cativo (*Captive Portal*) plenamente customizável, suportando fluxos de autorregistro, aprovação delegada por padrinhos internos (*Sponsor Approval*) e definição estrita do ciclo de vida temporal e privilégios das contas de convidados, isolando este tráfego da rede de produção.

INTEGRAÇÃO OBRIGATÓRIA COM O ECOSSISTEMA E ORQUESTRAÇÃO (SOAR)

Como premissa arquitetural inegociável e garantidora do valor tecnológico da contratação, o módulo NAC deve ser cem por cento (100%) integrado à

Plataforma Unificada (*Core* - Item 01). O NAC deve compartilhar continuamente o contexto situacional de cada dispositivo conectado (identidade do usuário, endereço IP, endereço MAC, localização física no *switch/Access Point* e nível de conformidade) com o console central, enriquecendo o inventário dinâmico e o cálculo do *Risk Score* global. Sob a ótica da contenção automatizada, o NAC atuará como o principal braço executor de rede para o subsistema de Orquestração (SOAR). É exigência mandatória que a plataforma permita a configuração de políticas condicionais automatizadas; por exemplo, caso o motor de análise de vulnerabilidades (Item 01) detecte a exploração de um CVE crítico, ou o agente de *Endpoint* (Item 03) alerte sobre a execução de um *Ransomware*, o módulo NAC deverá receber um gatilho sistêmico (via API RESTful) e isolar de forma autônoma e imediata a porta do *switch* ou a sessão Wi-Fi do dispositivo comprometido, eliminando o lapso de tempo dependente da intervenção humana.

MECANISMOS DE SEGURANÇA E REQUISITOS DE CONFORMIDADE

A governança exercida por este módulo atende diretamente aos preceitos da Lei Geral de Proteção de Dados (LGPD) e normativos da família ISO/IEC 27000, ao garantir que o acesso lógico aos repositórios de dados sensíveis seja restrito mediante forte controle de identidade e saúde do dispositivo de acesso. Para garantir a continuidade dos serviços governamentais/corporativos, a arquitetura do NAC deve suportar implantação em Alta Disponibilidade (HA) e possuir mecanismos de tolerância a falhas (*Fail-Open/Fail-Closed*), assegurando que indisponibilidades sistêmicas não interrompam operações críticas. Por fim, para resguardar a cadeia de custódia em investigações internas ou processos de auditoria, toda alteração de política de acesso, cada evento de quarentena automatizada e todas as tentativas de conexão à rede devem gerar registros (logs) precisos. Tais registros serão canalizados para a trilha de auditoria central da plataforma (DFIR) e submetidos ao mecanismo nativo de *hash* criptográfico persistido na tecnologia de livro-razão distribuído (*Blockchain*), certificando a imutabilidade pericial plena das evidências de controle de acesso à rede.

APÊNDICE II – Escopo para Prova de Conceito (PoC)

1. PREÂMBULO E BASE LEGAL

O presente documento constitui o Apêndice II do Termo de Referência para a contratação de Solução Integrada de Cibersegurança pelo ITEC-AL, na modalidade Pregão Eletrônico, com fundamento na Lei nº 14.133/2021. Define o escopo da Prova de Conceito (PoC) exigida do licitante classificado provisoriamente em primeiro lugar, nos termos dos itens 4.77 a 4.85 do Termo de Referência. O documento foi elaborado pela equipe técnica do ITEC-AL com base nos requisitos do TR, nas normas ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-61r2 e na Lei nº 13.709/2018 (LGPD).

1.1. Fundamentação Legal e Normativa

- TR itens 4.77 a 4.85: Exigência da Prova de Conceito como condição habilitante para o licitante classificado em primeiro lugar.
- TR item 4.83: Critérios mínimos de aprovação da PoC, incluindo integração nativa entre módulos Core e Endpoint.
- TR item 4.33: Exigência de integração nativa e bidirecional via APIs RESTful para interoperabilidade com o ecossistema do ITEC-AL.
- Lei nº 14.133/2021, Art. 17, III, 'c': Validação técnica de amostras antes da adjudicação.
- Lei nº 13.709/2018 — LGPD: Controles de privacidade obrigatórios nos módulos de tratamento de dados pessoais.
- Art. 369 do CPC/2015: Validade jurídica das evidências criptograficamente assinadas e registradas em mecanismo de imutabilidade.

1.2. Objeto e Finalidade da PoC

Verificar que a solução ofertada pela licitante classificada provisoriamente em primeiro lugar não apenas declara possuir os módulos descritos no TR, mas que estes operam de forma nativamente integrada (painel único de visibilidade), com foco em: (1) detecção e visibilidade de ameaças em tempo real, (2) suporte a sistemas operacionais legados presentes no parque do ITEC-AL, (3) imutabilidade das evidências para fins de auditoria e (4) conformidade com a LGPD.

1.3. Condições de Realização

A licitante terá até 5 (cinco) dias úteis, contados da convocação formal, para realizar a montagem, configuração e demonstração do ambiente.

Local: Ambiente controlado fornecido pelo ITEC-AL ou ambiente de demonstração da licitante que replique a topologia exigida no TR.

Avaliação: Comissão técnica designada pelo ITEC-AL emitirá Parecer Técnico de Aceitabilidade ao final da sessão.

Todos os custos, incluindo, deslocamento, licenciamento temporário, infraestrutura e logística, são de inteira responsabilidade da licitante, sem ônus para a Administração (TR item 4.84).

Todas as informações acessadas durante a PoC estão sujeitas ao Termo de Confidencialidade (Apêndice VII do TR).
A sessão será facultada a todos os interessados, incluindo demais licitantes, nos termos do item 4.82 do TR.
A recusa injustificada em realizar a PoC ou a incapacidade de atender aos critérios mínimos ensejará a desclassificação da proposta, convocando-se o licitante subsequente (TR item 4.85).

2. ESCOPO TÉCNICO DOS MÓDULOS

2.1. A tabela abaixo sintetiza o escopo de verificação desta PoC, as funcionalidades listadas abaixo foram extraídas diretamente dos requisitos do Termo de Referência. A coluna "Obrigatoriedade" define o impacto da ausência da função no julgamento da PoC.

Categoria	Funcionalidade Avaliada	Referência TR	Obrigatoriedade
1. Gestão e Core	**Cockpit:** Dashboard único correlacionando todos os alertas, indicadores, vulnerabilidades, containers, dados de EDR, inventário de ativo, logs, painel de teste de carga (DDoS), Painel de campanha de phishing, sem troca de console.	Item 3.3 / 4.1.2	**Sim (Mandatório)**
1. Gestão e Core	**Risk Score Dinâmico:** Algoritmo que altera a nota de risco organizacional ao detectar ameaças nos endpoints em tempo real.	Item 3.3 / 7.1.2	**Sim (Mandatório)**
1. Gestão e Core	**Imutabilidade Blockchain:** Registro de hashes de relatórios e logs em Blockchain para validade pericial.	Item 3.3 / 7.1.6	**Sim (Mandatório)**
1. Gestão e Core	Gestão de tickets/incidentes nativa no sistema com possibilidade de integração a ferramenta de ITSM.	Item 3.3 / 7.33	**Sim (Mandatório)**
2. Proteção Endpoint	**Suporte a Sistemas Legados:** Funcionamento do agente em	Item 3.5 / 7.33.1	**Sim (Mandatório)**

	sistemas legados, como por exemplo Windows Server 2008 R2 ou 2012 (Telemetria + Scan).		
2. Proteção Endpoint	**Anti-** Detecção de criptografia e reversão (recuperação) automática de arquivos.	Item 3	**Sim (Mandatório)**
2. Proteção Endpoint	**Mapeamento MITRE ATT&CK:** Exibição automática de táticas/técnicas do framework em cada alerta.	Item 4.4.2 / 7.4.2	**Sim (Mandatório)**
3. Orquestração	**Playbooks SOAR:** Execução de fluxos automatizados de resposta (Ex: Alerta -> Bloqueio IP -> Abrir Ticket).	Item 7.1.3 / 7.4.3	**Desejável**
4. Playbook	Possibilidade de consulta aos playbooks por meio da console cockpit	Item 4.4.3 / 7.1.3	**Sim (Mandatório)**
5. Inteligência	**Dark Web Monitoring:** Detecção de credenciais do domínio @*.al.gov.br em bases de vazamentos.	Item 3.4 / Apêndice I (2)	**Sim (Mandatório)**
5. Inteligência	**OSINT/External Attack Surface:** Descoberta automatizada de subdomínios expostos vinculados ao Órgão.	Apêndice I (Item 2)	**Sim (Mandatório)**
6. Containers	**Syscall Runtime Monitoring:** Detecção de anomalias (ex: shell interno) dentro de containers em execução.	Item 7.32 / Apêndice I (4)	**Sim (Mandatório)**
7. Identidade	**Autenticação FIDO2:** Exigência de toque físico na chave de hardware para login administrativo no console.	Item 4.22.2 / 7.22.2	**Sim (Mandatório)**

8. Privacidade	**Anonimização LGPD:** Mascaramento de dados sensíveis em relatórios para usuários sem privilégios de DPO.	Item 4.55.2 / 7.23.1	**Sim (Mandatório)**
8. Privacidade	**Direito ao Esquecimento:** Busca e exclusão (purge) de logs de um titular de dados específico.	Item 4.23.2 / 7.23.2	**Sim (Mandatório)**
9. Vulnerabilidade	**Validação de Exploit:** Cruzamento de vulnerabilidades detectadas com a existência de exploit público disponível.	Apêndice I (Item 1)	**Sim (Mandatório)**
10. Interface	**Localização PT-BR:** Toda a console e manuais devem estar no idioma Português do Brasil.	Item 4.26 / 7.26	**Desejável**

2.2. **Gestão do Ciclo de Vida de Vulnerabilidades e Visibilidade de Ativos**

2.2.1. A solução deverá demonstrar a execução de varreduras automatizadas e orquestradas sobre a superfície de ataque informada pelo **ITEC-AL** no ato da PoC, abrangendo ativos computacionais heterogêneos (IPs, FQDNs e Endpoints). A avaliação consistirá na aplicação de:

2.2.2. **Scans Não Autenticados:** Para mapeamento de portas, serviços expostos e identificação de vetores de intrusão externos.

2.2.3. **Scans Autenticados (Deep Scan):** Utilizando credenciais administrativas para auditar o inventário de software, patches ausentes e configurações de *hardening* em nível de Sistema Operacional (incluindo servidores legados).

2.2.4. **Motor Analítico e Inteligência:**
A plataforma deverá classificar as vulnerabilidades detectadas rigorosamente conforme o padrão **CVSS**, calculando o risco real com base na explorabilidade técnica. A PoC exigirá a geração de **Relatórios de Inteligência Acionável**, que devem apresentar não apenas a severidade, mas o plano de remediação priorizado, discriminando ações por criticidade e impacto na continuidade dos serviços públicos estaduais.

2.3. **Análise Prospectiva de Vulnerabilidades (VAPT Automatizado)**

2.3.1. Demonstração da capacidade da ferramenta em processar uma lista dinâmica de alvos (IPs, Endpoints e URLs) fornecida pela equipe técnica do **ITEC-AL**, garantindo:

2.3.2. **Identificação de Ativos:** Descoberta automatizada de serviços e suas respectivas versões.

2.3.3. **Multimodalidade de Varredura:** Execução concomitante de varreduras autenticadas e de rede, com foco em detectar falhas de segurança sem causar negação de serviço (*DoS*) nos ativos monitorados.

2.3.4. **Priorização por Severidade:** Entrega de painel consolidado com a classificação das falhas (Critical, High, Medium, Low), fundamentado no *score* CVSS.

2.3.5. **Remediação Consultiva:** Emissão de relatórios técnicos detalhados contendo os passos precisos para a correção das falhas, scripts de mitigação e referências cruzadas (CVE/Bugtraq).

2.4. Validação de Resiliência Ofensiva (Pentest Automatizado)

2.4.1. A solução deverá demonstrar a capacidade de executar simulações de adversários e testes de intrusão automatizados sobre aplicações e infraestruturas designadas. A avaliação abrangerá metodologias de Black-box, Gray-box e White-box, focando na identificação de vetores críticos baseados no OWASP Top 10.

2.4.2. Os ataques simulados deverão incluir, obrigatoriamente, a validação de vulnerabilidades de injeção (SQL Injection), manipulação de scripts (Cross-Site Scripting - XSS), quebra de autenticação por força bruta (Brute Force) e exploração de falhas de configuração em servidores web e bancos de dados institucionais.

2.5. Testes de Estresse e Resiliência à Negação de Serviço (DDoS)

2.5.1. Demonstração de simulação de ataques de Negação de Serviço Distribuída (DDoS) em camadas de rede (L3/L4) e aplicação (L7), conduzidos em ambiente de teste isolado e controlado.

2.5.2. A avaliação focará na capacidade da solução em: (a) Identificar o aumento anômalo de tráfego em tempo real; (b) Analisar o impacto na disponibilidade dos serviços governamentais;

2.6. Simulação de Engenharia Social e Resiliência do Usuário (Anti-Phishing)

2.6.1. Demonstração do painel de gestão de campanhas simuladas de Phishing, visando mensurar a postura de segurança dos colaboradores. A ferramenta deve permitir a criação de cenários de ataque customizados (ex: falsas notificações de RH ou e-mails governamentais fraudulentos).

2.6.2. A PoC avaliará a geração de métricas de telemetria comportamental, incluindo: taxa de abertura, taxa de clique em links maliciosos, submissão de dados sensíveis e a eficácia das pílulas de treinamento (micro-learning) aplicadas imediatamente após a falha do usuário.

2.7. Custódia de Evidências, Analytics e Relatórios de Governança

2.7.1. Integridade Baseada em Blockchain: A solução deverá comprovar a geração de relatórios técnicos e gerenciais cujos hashes criptográficos (SHA-256 ou superior) sejam registrados em tecnologia Blockchain. Esta funcionalidade é mandatória para assegurar a imutabilidade pericial e a validade jurídica dos dados de segurança frente a auditorias de órgãos de controle (Art. 369 do CPC/2015).

2.7.2. Painel de Consciência Situacional: Apresentação de console administrativo intuitivo e centralizado, capaz de consolidar dados telemétricos de todos os módulos. A plataforma deverá gerar alertas

preditivos e em tempo real, correlacionando eventos de múltiplas origens e classificando-os por Risk Score organizacional.

2.7.3. Estrutura dos Alertas e Relatórios: Cada incidente ou vulnerabilidade reportada deve conter, no mínimo:

2.7.3.1. Taxonomia de Ameaças: Descrição técnica precisa da falha, preferencialmente mapeada às táticas e técnicas da Matriz MITRE ATT&CK;

2.7.3.2. Mapeamento de Impacto: Identificação clara dos ativos ou serviços governamentais críticos afetados pela exposição;

2.7.3.3. Análise de Consequências: Projeção detalhada de danos potenciais (ex: risco de exfiltração de dados sensíveis, interrupção de arrecadação estadual);

2.7.3.4. Prescrição Técnica de Remediação: Recomendações de ação objetivas, incluindo scripts de correção, comandos de hardening e patches sugeridos para a erradicação definitiva da falha.

APÊNDICE III - Matriz de Riscos

Esta matriz identifica os eventos de risco, os impactos esperados e as estratégias de mitigação e alocação de responsabilidades (entre Contratante e Contratada).

ID	Evento de Risco	Impacto (Efeito)	Probabilidade	Nível	Estratégia de Mitigação	Alocação
01	**Falha de Integração (Silos)**	Módulos (EDR, NAC, SOAR) não funcionam de forma unificada, perdendo-se o efeito de *Single Pane of Glass*.	Média	Alto	Exigir Prova de Conceito (PoC) ou Demonstração técnica das APIs funcionando conjuntamente antes da aceitação.	Contratada
02	**Incompatibilidade com Legados**	Agentes (EDR) ou Varreduras (Scanner) causam instabilidade em servidores Windows 2008/2012 ou aplicações críticas.	Alta	Alto	Estabelecer ambiente de homologação; fase de *tuning* assistido antes da aplicação em produção.	Contratada
03	**Degradação de Performance**	Agentes ou varreduras agressivas impactam a disponibilidade dos serviços de negócio.	Média	Médio	Parametrização estrita de janelas de *scan* e *throttling* de banda; uso de *agents* otimizados.	Contratada
04	**Vazamento de Dados da Plataforma**	Dados sensíveis da infraestrutura (logs, topologias) expostos indevidamente na nuvem.	Baixa	Crítico	Exigir criptografia *at rest* (AES-256) e *in transit* (TLS 1.2+); exigir conformidade SOC2/ISO27001 do fornecedor.	Contratada
05	**Alerta Falso Positivo (Fadiga SOC)**	SOC inunda a TI com alertas irrelevantes, paralisando a operação por excesso de chamados.	Alta	Alto	Obrigatoriedade de *tuning* contínuo de regras no SOAR; curadoria de alertas pelo serviço de gestão de vulnerabilidades.	Contratada
06	**Desconhecimento da Equipe Técnica**	Equipe do órgão não consegue operar a	Média	Médio	Exigir treinamento com emissão de certificado e entregáveis de	Contratada

		solução após o término do suporte de implantação.			"Arquitetura As-Built" e manuais de operação em PT-BR.	
07	**Falha de Conformidade (LGPD)**	Dados pessoais de titulares expostos na plataforma de gestão ou em relatórios de auditoria.	Baixa	Crítico	Implementação de RBAC rigoroso, mascaramento de dados (PII) e auditoria imutável via Blockchain.	Partilhada
08	**Indisponibilidade do serviço SaaS**	Plataforma fora do ar, deixando a rede sem monitoramento e resposta a incidentes.	Baixa	Alto	SLA de 99,8% de disponibilidade; exigência de redundância em Datacenters e *fail-over* geográfico.	Contratada
09	**Falha na Entrega das Chaves FIDO2**	Administradores sem acesso de segundo fator, bloqueando a gestão de segurança.	Baixa	Médio	Exigência de estoque de reserva e substituição imediata em caso de defeito; *backdoor* de emergência documentado.	Contratada
10	**Resistência cultural ao Treinamento**	Colaboradores não aderem às simulações de phishing ou ignoram os momentos de ensino.	Alta	Médio	Relatórios de performance apresentados à alta gestão; gamificação das campanhas de conscientização.	Contratante

APÊNDICE IV - ACORDO DE NÍVEL DE SERVIÇO (ANS/SLA)

1. FINALIDADE E ESCOPO
1.1. Este Acordo de Nível de Serviço estabelece os critérios objetivos para a medição da qualidade e do desempenho dos serviços prestados pela CONTRATADA no âmbito da Solução Integrada de Cibersegurança e Privacidade.
1.2. A avaliação dos indicadores será mensal e servirá de base para o dimensionamento do pagamento e a aplicação de eventuais glosas ou sanções, visando garantir a eficácia da proteção dos ativos de TIC e o cumprimento dos requisitos operacionais.

2. CLASSIFICAÇÃO DE SEVERIDADE (ATENDIMENTO DE SUPORTE E INCIDENTES)
Para fins de aplicação dos prazos de atendimento (ICP), as demandas serão classificadas conforme os níveis de severidade abaixo:

Severidade	Descrição	Prazo de Início (Resposta)	Prazo de Solução (Contorno)
CRÍTICA	Incidentes de segurança confirmados (ex: Ransomware, exfiltração ativa, DDoS massivo) ou indisponibilidade total da Plataforma Unificada.	30 minutos	24 horas
ALTA	Vulnerabilidades críticas expostas, falha em módulos principais (EDR, NAC), ou comprometimento de conta administrativa.	2 horas	2 dias úteis
NORMAL	Dúvidas operacionais, parametrização de playbooks, geração de relatórios sob demanda ou falha em subdomínios de menor criticidade.	4 horas	4 dias úteis
BAIXA	Solicitações de melhoria cosmética, dúvidas sobre manuais ou documentação técnica.	8 horas	6 dias úteis

3. INDICADORES DE MEDIÇÃO DE RESULTADO (IMR)
A) INDICADOR DE DISPONIBILIDADE DE SERVIÇO (IDS)

- Finalidade: Assegurar a continuidade das plataformas SaaS (Core, EDR, NAC, Containers).
- Mecanismo de Cálculo: IDS = (Horas de Funcionamento / Horas Totais do Mês) x 100
- Meta: ≥ 99,8%.
- Glosas (sobre o valor da mensalidade do item afetado):
  - IDS ≥ 99,8%: Pagamento Integral.
  - IDS < 99,8% até 99,0%: Glosa de 5%.
  - IDS < 99,0% até 98,0%: Glosa de 10%.
  - IDS < 98,0%: Glosa de 20% e abertura de processo sancionador.

B) INDICADOR DE CHAMADOS ATENDIDOS NO PRAZO (ICP)

- Finalidade: Medir a agilidade do SOC e do suporte técnico especializado.
- Mecanismo de Cálculo: ICP = (Chamados no Prazo / Total de Chamados) x 100

- Meta: ≥ 95%.
- Glosas (sobre o valor da mensalidade do serviço - Item 08):
    - ICP ≥ 95%: Sem desconto.
    - ICP entre 85% e 94,9%: Glosa de 1,5%.
    - ICP entre 78% e 84,9%: Glosa de 3%.
    - ICP < 72%: Multa de 1% do valor do contrato e glosa de 5% da mensalidade.

C) INDICADOR DE DISPONIBILIDADE DOS SERVIÇOS DE GERENCIAMENTO (IDSG)

- Finalidade: Medir a presença e prontidão da equipe de SOC 24x7.
- Mecanismo de Cálculo: Tempo efetivo de vigilância ativa logada no cockpit vs. tempo total do mês.
- Meta: ≥ 99%.
- Faixas de Ajuste: Segue o escalonamento de glosa de 3% a 12% conforme sua tabela de sanções para IDSG.

D) INDICADOR DE EFICÁCIA NO TRATAMENTO (IECRI)

- Finalidade: Evitar o encerramento indevido de incidentes sem a devida correção.
- Mecanismo de Cálculo: IECRI = ((Total Fechados - Total Reabertos) / Total Fechados) x 100
- Meta: ≥ 98%.
- Glosas: 1% de glosa sobre o valor da OS/Fatura para cada 0,1% abaixo da meta.

E) INDICADOR DE ATRASO NA ENTREGA (IAE)

- Finalidade: Garantir o cumprimento do cronograma de implantação e entrega de chaves FIDO2.
- Mecanismo de Cálculo: IAE = Tempo de Execução Real - Tempo Estimado na OS.
- Sanções:
    - Atraso de 1 a 29 dias: Glosa de 0,5% por dia de atraso sobre o valor do marco/OS.
    - Atraso ≥ 30 dias: Glosa de 10% do valor da etapa + 0,5% por dia, limitado a 30%.

F) INDICADOR DE SATISFAÇÃO DOS USUÁRIOS (ISU)

- Finalidade: Aferir a qualidade do atendimento consultivo da equipe de *Blue Team*.
- Meta: ≥ 80% de avaliação positiva.
- Métrica: Nota média de 1 a 5 em questionários pós-serviço (DPO/Vuln).

4. PROCEDIMENTOS DE AFERIÇÃO E ATESTO

4.1. Ferramenta de Medição: A própria Plataforma Unificada (Item 01), por meio de seus módulos de auditoria e *logs* imutáveis em *Blockchain*, será a fonte primária para extração das métricas de disponibilidade (IDS) e tempo de resposta (SOAR).

4.2. Relatório Mensal de Nível de Serviço (RNS): A CONTRATADA deverá submeter, até o 5º dia útil do mês subsequente, um relatório consolidado contendo o desempenho de todos os indicadores descritos neste Apêndice.

4.3. Verificação da Fiscalização: O Fiscal Técnico conferirá os dados do RNS confrontando-os com as evidências na plataforma. Em caso de divergência, prevalecerão os dados extraídos pela Contratante diretamente do sistema.

4.4. Aplicação de Glosas: As glosas serão calculadas pela Fiscalização Administrativa e deduzidas diretamente na Nota Fiscal do mês de referência.

5. DISPOSIÇÕES SOBRE PENALIDADES POR DESCUMPRIMENTO REINCIDENTE

5.1. A ocorrência de ICP inferior a 70% por 3 (três) meses consecutivos será considerada inexecução parcial do objeto, autorizando a Contratante a iniciar o processo de rescisão motivada.

5.2. A manipulação indevida de dados telemétricos ou *logs* visando mascarar o não cumprimento de SLAs será considerada infração grave (fraude na execução contratual), ensejando a penalidade máxima prevista na Lei 14.133/2021.

APÊNDICE V - INVENTÁRIO DE ATIVOS (BASE DE CÁLCULO)

DIMENSIONAMENTO DE INFRAESTRUTURA (QUANTITATIVO PARA CÁLCULO)

Item	Descrição	Quantidade (Números Inteiros)	Observações / Especificação
Total de Colaboradores	(Com acesso à rede/sistemas)	188	
Contas de E-mail Institucional Ativas	(Para escopo de monitoramento/proteção)	8959	
Estações de Trabalho (Endpoints)	(Desktops e Notebooks)	120	
Servidores (Físicos + Virtuais)	(Para escopo de EDR/VA/Backup)	31 – Físicos	
Máquinas Virtuais (VMs)	(Exclusivo VMs - Subconjunto do item anterior)	897 - Virtual	Hipervisores (VMware/Hyper-V/Outro):
Sistemas/Aplicações Web Críticas (URLs)	(Para escopo de Pentest/VA de Aplicações)	10 – On-premise 1-Cloud	Especificar se SaaS, On-premise ou Cloud Native.
IPs Públicos Válidos	(Para acesso a serviços/portais)	50	
Total de Domínios/Subdomínios	(Ex: .gov.br, .org)	5000	

INVENTÁRIO DE ATIVOS E REDE (DIMENSIONAMENTO TÉCNICO)

Item	QTD Estimada	Fabricante/Modelo (Se relevante)	Criti. (Alta/Média/Baixa)	Observações
Firewalls	4	2 - Fortigate 3300E 2 - Fortigate 2200E		
Switches Gerenciáveis	13	2 - FortiSwitch 1024D 5 - FortiSwitch 548D 6 - FortiSwitch 124E		
Access Points	8	8 - AP-431F-PROFILE		
Instâncias de Bancos de Dados	260			MariaDB / 306 GB MySQL / 18,310 TB Oracle / 53,71 TB Postgresql 13,20 TB SQL Server 23 TB

Storages / Servidores de Arquivos (File Servers)	1			Windows /1 TB
Usuários no Active Directory (AD)	188			
VPN Usuários Ativas (Licenças)	1127			
Câmeras/Dispositivos IoT	70			

APÊNDICE VI - Modelo de Ordem de Serviço (OS)

ORDEM DE SERVIÇO — CONTRATO DE CIBERSEGURANÇA

Contratação de Solução Integrada de Cibersegurança — Lei nº 14.133/2021

1. IDENTIFICAÇÃO DA ORDEM DE SERVIÇO

Nº da OS:	*OS-____/20__*	**Data de Emissão:**	*____/____/20__*
Contrato nº:	*___/20__*	**Vigência do Contrato:**	*__/__/20__ a __/__/20__*
Processo Adm.:	*xxxxx.xxxxxx/xxxx-xx*	**Tipo de OS:**	*( ) Implantação ( ) Serviço Contínuo ( ) Corretiva ( ) Evolutiva*

2. PARTES ENVOLVIDAS

CONTRATANTE			
Órgão:	Instituto de Tecnologia do Estado de Alagoas — ITEC-AL	**CNPJ:**	*xx.xxx.xxx/xxxx-xx*
Gestor do Contrato:	*[Nome completo / matrícula]*	**Cargo:**	*[Cargo]*
Fiscal Técnico:	*[Nome completo / matrícula]*	**Contato:**	*[e-mail / ramal]*

CONTRATADA			
Razão Social:	*[Razão Social da Empresa]*	**CNPJ:**	*xx.xxx.xxx/xxxx-xx*
Preposto:	*[Nome do Preposto]*	**Cargo:**	*[Cargo]*
Telefone / E-mail:	*[Telefone] / [e-mail@empresa.com.br]*	**Ticket ITSM:**	*[Nº do chamado]*

3. OBJETO E ESCOPO DA ORDEM DE SERVIÇO

Objeto:	*[Descrever de forma clara e objetiva o serviço ou atividade demandada]*
Item(ns) do Contrato:	( ) Item 01 — Plataforma Core ( ) Item 02 — OSINT/EASM ( ) Item 03 — EDR/XDR ( ) Item 04 — Containers ( ) Item 05 — FIDO2 ( ) Item 06 — SOC 24x7 ( ) Item 07 — Implantação ( ) Item 08 — Gestão Vuln. ( ) Item 09 — NAC

Justificativa:	*[Descrever o motivo técnico ou operacional que originou a demanda]*
Criticidade:	( ) CRÍTICA — Impacto imediato em produção ( ) ALTA — Risco elevado ( ) NORMAL — Operacional ( ) BAIXA — Melhoria
Documentos Relacionados:	*[Nº de incidentes, relatórios, RNS, alertas do SOC ou decisões formais que embasam esta OS]*

4. RELAÇÃO DE ATIVIDADES / SERVIÇOS DEMANDADOS

⚠ *Detalhar cada atividade em linha separada. Itens marcados com (*) são obrigatórios para OS de implantação.*

#	Descrição da Atividade	Unidade	Qtd. Est.	Prazo (dias)	Perfil Técnico
1	*[Atividade 1 — ex.: Instalação de agentes EDR em servidores Windows]*	Hora Técnica	___	___	Perfil 6
2	*[Atividade 2 — ex.: Configuração de políticas NAC para dispositivos IoT]*	Hora Técnica	___	___	Perfil 6
3	*[Atividade 3 — ex.: Elaboração de Playbook SOAR para contenção de Ransomware]*	Hora Técnica	___	___	Perfil 3
4	*[Atividade 4]*	Hora Técnica	___	___	___
5	*[Atividade 5]*	Hora Técnica	___	___	___

5. PRAZOS E CRONOGRAMA DE EXECUÇÃO

Data de Início:	*____/____/20__*	**Data de Conclusão (estimada):**	*____/____/20__*
Prazo Total (dias corridos):	*___ dias*	**Horário de Execução:**	( ) Horário Comercial (08h–18h) ( ) Fora do Horário ( ) 24x7
Janela de Manutenção (se houver):	*[Data/hora acordada para intervenções que possam causar indisponibilidade]*		

Observações de Prazo:	*[Ex.: prorrogação permitida mediante justificativa formal aceita pelo Fiscal Técnico]*

6. CRITÉRIOS DE ACEITAÇÃO E ENTREGÁVEIS

⚠ *Todos os entregáveis abaixo devem ser formalmente atestados pelo Fiscal Técnico para fins de recebimento provisório e definitivo (art. 140 da Lei nº 14.133/2021).*

#	Entregável / Critério de Aceite	Prazo de Entrega	Status
1	*[Relatório técnico de execução das atividades com evidências (prints, logs, outputs)]*	Até ___ dias após execução	( ) Pendente ( ) Entregue ( ) Aprovado
2	*[Documentação as-built atualizada (se houver alteração de arquitetura)]*	Até ___ dias após execução	( ) Pendente ( ) Entregue ( ) Aprovado
3	*[Rescan de validação (quando aplicável — itens de remediação)]*	Até ___ dias após correção	( ) Pendente ( ) Entregue ( ) Aprovado
4	*[Atualização da base de conhecimento / playbooks impactados]*	Até ___ dias após execução	( ) Pendente ( ) Entregue ( ) Aprovado
5	*[Demonstração funcional ao Fiscal Técnico (para OS de implantação/configuração)]*	Na data de conclusão	( ) Pendente ( ) Entregue ( ) Aprovado

7. ACORDO DE NÍVEL DE SERVIÇO (SLA) APLICÁVEL A ESTA OS

Severidade	Prazo de Resposta	Prazo de Solução
CRÍTICA	30 minutos	24 horas
ALTA	2 horas	2 dias úteis
NORMAL	4 horas	4 dias úteis
BAIXA	8 horas	6 dias úteis

Severidade desta OS:	( ) CRÍTICA ( ) ALTA ( ) NORMAL ( ) BAIXA

Prazo de Resposta (SLA):	*[Preencher conforme severidade marcada acima]*
Prazo de Solução (SLA):	*[Preencher conforme severidade marcada acima]*

8. APURAÇÃO DO INDICADOR DE ATRASO NA ENTREGA (IAE)

⚠ O IAE será calculado pelo Fiscal Técnico ao encerrar esta OS. Atrasos injustificados resultam em glosa conforme Seção 9 do TR.

Tempo Estimado (TEST):	*[___ dias corridos, conforme item 5 desta OS]*	
Tempo de Execução Real (TEX):	*[A preencher na data de aceite pelo Fiscal Técnico]*	
IAE = TEX – TEST:	**IAE ≤ 0:** Pagamento integral | **1 ≤ IAE < 30:** Glosa 0,5%/dia | **IAE ≥ 30:** Glosa 10% + 0,5%/dia (lim. 30%) + multa 2%	

9. DISPOSIÇÕES DE SEGURANÇA DA INFORMAÇÃO E SIGILO

A execução desta Ordem de Serviço estará condicionada ao cumprimento integral das obrigações de sigilo e segurança previstas no Contrato, neste Termo de Referência e nos Termos de Ciência e Confidencialidade assinados pela Contratada, em especial:

- Todos os profissionais alocados para esta OS devem ter Termo de Ciência e Sigilo (NDA) assinado e arquivado nos autos do processo administrativo.
- É vedado o acesso a sistemas, dados ou configurações além do estritamente necessário para a execução do escopo desta OS (princípio do menor privilégio).
- Qualquer incidente de segurança detectado durante a execução desta OS deve ser comunicado imediatamente ao Fiscal Técnico, independentemente da relação com o escopo contratado.
- Toda ação executada nos sistemas da Contratante deverá ser registrada no histórico do chamado (ITSM) para fins de auditoria forense e conformidade com a LGPD.
- É vedada a extração ou cópia de dados da Contratante para dispositivos ou ambientes externos sem autorização formal prévia e por escrito do Gestor do Contrato.

10. RECURSOS, ACESSOS E RESPONSABILIDADES

#	Recurso / Acesso Necessário	Responsável pela Disponibilização	Status
1	*[Acesso VPN / credencial de serviço para integração]*	**CONTRATANTE**	( ) Disponível ( ) Pendente
2	*[Janela de manutenção aprovada no Change Management]*	**CONTRATANTE**	( ) Aprovada ( ) Pendente
3	*[Ambiente de homologação/sandbox para testes prévios]*	**CONTRATANTE**	( ) Disponível ( ) Não aplicável
4	*[Licenças adicionais ou módulos a serem ativados pelo fabricante]*	**CONTRATADA**	( ) Disponível ( ) Pendente
5	*[Profissional técnico certificado conforme perfil exigido no TR, item 4.44]*	**CONTRATADA**	( ) Alocado ( ) Pendente

11. EMISSÃO E RECEBIMENTO DA ORDEM DE SERVIÇO

EMITIDA PELA CONTRATANTE	RECEBIDA PELA CONTRATADA
_____ *[Nome do Fiscal Técnico]* Fiscal Técnico do Contrato — ITEC-AL Data: ____/____/20__	_____ *[Nome do Preposto da Contratada]* Preposto — [Razão Social] Data: ____/____/20__

12. TERMO DE RECEBIMENTO PROVISÓRIO

Data do Recebimento Provisório:	*____/____/20__*
Observações do Fiscal Técnico:	*[Descrever eventuais pendências ou inconformidades identificadas no recebimento provisório]*
Observações do Fiscal Administrativo:	*[Ex.: verificação de regularidade fiscal, certidões, documentação trabalhista]*
Resultado:	( ) Recebido sem ressalvas ( ) Recebido com pendências (ver observações) ( ) Rejeitado

FISCAL TÉCNICO	FISCAL ADMINISTRATIVO
_____ *[Nome / Matrícula]* Data: ____/____/20__	_____ *[Nome / Matrícula]* Data: ____/____/20__

13. TERMO DE RECEBIMENTO DEFINITIVO

Data do Recebimento Definitivo:	____/____/20__ (até 15 dias corridos após o Recebimento Provisório — art. 140 Lei nº 14.133/2021)
IAE Apurado:	*[___ dias] | Glosa resultante: R$ _____ (ou: Sem glosa — IAE ≤ 0)*
Valor a Faturar (OS):	*R$ _____ (valor apurado após eventuais deduções de glosa)*
Ateste para Pagamento:	( ) Autorizado integralmente ( ) Autorizado parcialmente — ver ressalvas ( ) Não autorizado

GESTOR DO CONTRATO — ATESTE DEFINITIVO
_____ *[Nome completo / Matrícula do Gestor do Contrato]* Gestor do Contrato — ITEC-AL Data: ____/____/20__

APÊNDICE VII - Termo de Ciência e Compromisso de Sigilo (NDA)

TERMO DE CIÊNCIA, CONFIDENCIALIDADE E COMPROMISSO DE SIGILO

Contratação de Solução Integrada de Cibersegurança — Lei nº 14.133/2021

1. QUALIFICAÇÃO DAS PARTES

CONTRATANTE	
Órgão:	Instituto de Tecnologia do Estado de Alagoas — ITEC-AL
CNPJ:	*xx.xxx.xxx/xxxx-xx*
Representante Legal:	*[Nome / Cargo / Matrícula]*

CONTRATADA	
Razão Social:	*[Razão Social da Empresa]*
CNPJ:	*xx.xxx.xxx/xxxx-xx*
Representante Legal:	*[Nome / CPF / Cargo]*
Endereço Completo:	*[Rua, nº, Cidade, UF, CEP]*
DPO / Encarregado LGPD:	*[Nome e e-mail do DPO da Contratada]*

2. OBJETO E FUNDAMENTO LEGAL

O presente Termo tem por objeto estabelecer as obrigações de confidencialidade, sigilo e proteção de informações sensíveis às quais se sujeitam a Contratada e todos os profissionais por ela alocados para execução do Contrato de Solução Integrada de Cibersegurança firmado com o ITEC-AL, nos termos da Lei nº 14.133/2021, da Lei nº 13.709/2018 (LGPD) e das cláusulas contratuais pertinentes.

Este instrumento é condição prévia e obrigatória para o início da execução dos serviços, conforme exigência do item 4.46.2 do Termo de Referência. A assinatura deve ocorrer antes do primeiro acesso físico ou lógico a quaisquer sistemas, ambientes ou informações do ITEC-AL.

3. DEFINIÇÕES

Para os fins deste Termo, aplicam-se as seguintes definições:

- Informação Confidencial: toda informação técnica, operacional, estratégica, financeira ou jurídica relativa à infraestrutura de TIC do ITEC-

AL, incluindo topologias de rede, endereços IP, credenciais de acesso, vulnerabilidades identificadas, logs de segurança, dados pessoais de servidores e cidadãos, configurações de sistemas e quaisquer dados acessados ou gerados durante a execução contratual;

- Profissional Vinculado: todo empregado, colaborador, subcontratado, estagiário ou consultor da Contratada que, em razão do contrato, tenha acesso direto ou indireto a Informações Confidenciais;
- Incidente de Privacidade: qualquer acesso não autorizado, vazamento, divulgação indevida, destruição, alteração, extravio ou tratamento irregular de Informação Confidencial ou de dados pessoais;
- Controlador e Operador: conforme definições do art. 5º, VI e VII, da Lei nº 13.709/2018 (LGPD).

4. OBRIGAÇÕES DA CONTRATADA E DOS PROFISSIONAIS VINCULADOS

A Contratada obriga-se, por si e por todos os seus Profissionais Vinculados, a:

- Manter sigilo absoluto sobre todas as Informações Confidenciais acessadas durante ou após a vigência do contrato, pelo prazo de 5 (cinco) anos após o encerramento da relação contratual, ou por prazo superior quando exigido por lei específica;
- Utilizar as Informações Confidenciais exclusivamente para os fins de execução do objeto contratual, sendo expressamente vedado o uso para benefício próprio, de terceiros ou para finalidades não previstas neste instrumento;
- Não reproduzir, copiar, transmitir, divulgar, publicar ou compartilhar, por qualquer meio, Informações Confidenciais sem autorização prévia e expressa do Gestor do Contrato do ITEC-AL;
- Adotar medidas técnicas e organizacionais adequadas para proteger as Informações Confidenciais contra acesso não autorizado, em padrão equivalente ao exigido pela norma ISO/IEC 27001;
- Comunicar imediatamente ao Fiscal Técnico do ITEC-AL — prazo máximo de 2 horas após ciência do fato — qualquer suspeita ou ocorrência de Incidente de Privacidade ou violação de sigilo, com relatório de causa, extensão e medidas de contenção adotadas;
- Ao término do contrato ou quando solicitado, devolver ou destruir de forma segura (sanitização certificada, conforme NIST SP 800-88) todos os suportes que contenham Informações Confidenciais, apresentando Certificado de Destruição de Dados;
- Exigir que todos os Profissionais Vinculados assinem o Apêndice A deste Termo (Ciência Individual) antes do primeiro acesso a sistemas ou informações do ITEC-AL.

5. VEDAÇÕES ESPECÍFICAS — INFORMAÇÕES DE CIBERSEGURANÇA

⚠ *As vedações abaixo são de cumprimento especialmente rigoroso, dada a natureza crítica das informações de segurança cibernética.*

É expressamente vedado à Contratada e a qualquer Profissional Vinculado:

- Divulgar a terceiros, em qualquer hipótese, vulnerabilidades identificadas nos sistemas do ITEC-AL, configurações de firewalls, topologias de rede internas ou quaisquer informações que possam subsidiar ataques cibernéticos;
- Utilizar dados, credenciais ou acessos obtidos durante a execução contratual após o término do vínculo contratual, ainda que para fins defensivos;
- Publicar, em meios acadêmicos, conferências, redes sociais ou blogs, informações derivadas desta execução contratual que identifiquem o ITEC-AL, suas vulnerabilidades ou arquitetura de segurança;
- Utilizar dados coletados (logs, telemetria, evidências forenses) para alimentar modelos de IA proprietários da Contratada ou para benchmarking comercial com outros clientes;
- Realizar, por conta própria ou a pedido de terceiros, qualquer teste de intrusão, varredura de vulnerabilidades ou simulação de ataque fora do escopo expressamente autorizado nas Ordens de Serviço.

6. TRATAMENTO DE DADOS PESSOAIS — LGPD

Na qualidade de Operadora de Dados (art. 5º, VII, LGPD), a Contratada compromete-se a:

- Tratar os dados pessoais acessados estritamente conforme as instruções do ITEC-AL (Controladora), não realizando qualquer operação que extrapole o escopo do contrato;
- Implementar criptografia AES-256 para dados em repouso e TLS 1.3 para dados em trânsito, controle de acesso por perfil (RBAC) e pseudonimização sempre que tecnicamente viável;
- Comunicar ao ITEC-AL, em até 24 horas, qualquer Incidente de Privacidade com dados pessoais que possa acarretar risco aos titulares, subsidiando a notificação à ANPD prevista no art. 48 da LGPD;
- Não transferir dados pessoais para países sem proteção equivalente à LGPD, salvo mediante autorização expressa do ITEC-AL nas hipóteses do art. 33 da LGPD;
- Ao término do contrato, excluir ou devolver todos os dados pessoais tratados, apresentando comprovante de sanitização certificada no prazo de 30 dias.

7. RESPONSABILIDADE CIVIL, PENAL E CONTRATUAL

O descumprimento de quaisquer obrigações deste Termo sujeitará a Contratada e/ou o Profissional Vinculado, de forma cumulativa:

- Responsabilidade civil pela reparação integral dos danos causados ao ITEC-AL, aos titulares de dados afetados e a terceiros prejudicados, nos termos do art. 927 do Código Civil;

- Penalidades contratuais previstas na Seção 9 do Termo de Referência, incluindo multa de até 20% do valor total e declaração de inidoneidade;
- Sanções administrativas da ANPD de até 2% do faturamento anual da Contratada, limitadas a R$ 50.000.000,00 por infração (art. 52, LGPD);
- Responsabilidade penal do profissional infrator nas hipóteses dos arts. 153, 154-A e 325 do Código Penal;
- Rescisão imediata do contrato por inexecução grave e comunicação ao CEIS/CNEP (art. 161, Lei nº 14.133/2021).

8. DISPOSIÇÕES GERAIS

- Este Termo não é transmissível, não podendo ser cedido a terceiros sem autorização expressa e por escrito do ITEC-AL.
- Exceções à obrigação de sigilo somente serão admitidas mediante autorização prévia por escrito do ITEC-AL, ou quando determinadas por autoridade judicial ou administrativa competente, hipótese em que a Contratada notificará imediatamente o ITEC-AL.
- As obrigações de sigilo sobrevivem à extinção do contrato pelo prazo mínimo de 5 anos, ressalvadas disposições legais que estabeleçam prazo superior.
- Fica eleito o Foro da Comarca de Maceió/AL para dirimir eventuais litígios, renunciando-se a qualquer outro.

9. ASSINATURAS — CONTRATADA (PESSOA JURÍDICA)

Ao assinar, o representante legal declara ter lido, compreendido e concordado integralmente com este Termo, responsabilizando-se pelo cumprimento das obrigações por si e por todos os Profissionais Vinculados.

_____ *[Nome do Representante Legal da Contratada]* Representante Legal — [Razão Social] Data: ____/____/20__	_____ *[Nome do Representante do ITEC-AL]* Gestor do Contrato — ITEC-AL Data: ____/____/20__

APÊNDICE A — TERMO DE CIÊNCIA INDIVIDUAL DO PROFISSIONAL VINCULADO

(A ser assinado por cada profissional antes do primeiro acesso a sistemas ou informações do ITEC-AL)

Nome Completo:	*[Nome completo do profissional]*
CPF:	___.___.___-__
Cargo / Função:	*[Cargo na Contratada]*
Perfil Técnico (TR):	( ) Perfil 1 — SOC ( ) Perfil 2 — Gestão ( ) Perfil 3 — DFIR ( ) Perfil 4 — Vuln. ( ) Perfil 5 — Pentest ( ) Perfil 6 — Arquiteto
Contrato vinculado:	*Contrato nº ___/20__ — ITEC-AL*
Data de início do acesso:	____/____/20__

Eu, profissional identificado acima, DECLARO que:

- Li e compreendi integralmente o Termo de Ciência, Confidencialidade e Compromisso de Sigilo firmado entre a empresa em que trabalho e o ITEC-AL;
- Tenho plena ciência de que terei acesso a informações sensíveis, sigilosas e estratégicas da infraestrutura de segurança cibernética do ITEC-AL;
- Comprometo-me a não divulgar, reproduzir, compartilhar ou utilizar quaisquer Informações Confidenciais para fins além dos estritamente necessários à execução do meu trabalho;
- Reconheço que o descumprimento das obrigações de sigilo poderá acarretar responsabilidade civil, penal e administrativa, conforme legislação vigente;
- Esta obrigação de sigilo persiste pelo prazo de 5 anos após o término do meu vínculo com o contrato.

_____ *[Assinatura do Profissional Vinculado]* CPF: ___.___.___-__ Data: ____/____/20__	_____ *[Testemunha — Preposto da Contratada]* Cargo / CPF Data: ____/____/20__

APÊNDICE VIII - Modelo de Relatório Mensal de Nível de Serviço (RNS)

RELATÓRIO MENSAL DE NÍVEL DE SERVIÇO — RNS
Contratação de Solução Integrada de Cibersegurança — Lei nº 14.133/2021

1. IDENTIFICAÇÃO DO RELATÓRIO

Nº do RNS:	*RNS-____/20__*	Mês/Ano de Referência:	*___/20__*
Contrato nº:	*___/20__*	Data de Emissão:	*____/____/20__*
Contratada:	*[Razão Social]*	Preposto:	*[Nome / e-mail]*
Fiscal Técnico:	*[Nome / Matrícula]*	Período de Apuração:	*01/___/20__ a 31/___/20__*

2. QUADRO-RESUMO EXECUTIVO

⚠ *Este quadro serve como base para o ateste de pagamento. O Fiscal Técnico deve preencher após conferência dos dados do sistema.*

DESEMPENHO GERAL DO PERÍODO			
Incidentes Detectados:	___	Incidentes Críticos (P1):	___
MTTR Médio do Período:	*[___ h]*	Chamados em Aberto:	___
Total de Glosas Apuradas:	*R$ _____*	Valor a Faturar (Líquido):	*R$ _____*
Postura de Risco:	*[Melhorou / Manteve / Piorou — justificar]*		
Resultado Geral:	( ) APROVADO — Pagamento integral ( ) APROVADO COM GLOSAS — ver Seção 3 ( ) REPROVADO — Processo sancionador		

3. APURAÇÃO DOS INDICADORES DE MEDIÇÃO DE RESULTADO (IMR)

ID	Indicador	Meta Contratual	Apurado	Status	Glosa (R$)
IDS	Disponibilidade da Plataforma SaaS Core	≥ 99,8%	____%	✅ ATINGIDA	R$ 0,00
ICP	Chamados Atendidos no Prazo (SOC/Suporte)	≥ 95%	____%	✅ ATINGIDA	R$ 0,00
IDSG	Disponibilidade SOC 24x7	≥ 99%	____%	✅ ATINGIDA	R$ 0,00

IECRI	Taxa de Resolução Sem Reabertura	≥ 98%	____%	✅ ATINGIDA	R$ 0,00
ISU	Satisfação dos Usuários (NPS Pós-Atend.)	≥ 80%	____%	✅ ATINGIDA	R$ 0,00
IAE	Atraso na Entrega de Ordens de Serviço	= 0 dias	___ *dias*	✅ ATINGIDA	R$ 0,00
TOTAL GLOSA		*[Cálculo conforme fórmula IMR do TR, Seção 8]*			R$ _____

4. OPERAÇÃO DO SOC — INCIDENTES E THREAT HUNTING

#	Descrição do Incidente	Severidade	Detecção	MTTR	Status / Resultado
01	*[Ex.: Movimento lateral detectado — T1021.002 (MITRE ATT&CK)]*	CRÍTICA	__/__	___ h	Encerrado
02	*[Ex.: Campanha de phishing identificada — 42 usuários expostos]*	ALTA	__/__	___ h	Encerrado
03	*[Ex.: CVE-20xx-xxxx explorada em servidor de aplicação]*	CRÍTICA	__/__	___ h	Em Remediação
04	*[Acrescentar linhas conforme ocorrências do período]*	—	—	—	—

Sessões de Threat Hunting:	*[Nº de sessões] — descrever escopo resumido*
Playbooks SOAR acionados:	*[Nº de acionamentos] — listar playbooks e resultados*
Taxa de Falsos Positivos (FP%):	*[___% — meta: < 5%]*

5. GESTÃO DE VULNERABILIDADES — PAINEL DE REMEDIAÇÃO

Severidade	Abertas (ant.)	Novas	Remediadas	Pendentes > 30d	SLA Rem. (%)
CRÍTICA	___	___	___	___	___%

ALTA	___	___	___	___	___%
MÉDIA	___	___	___	___	___%
BAIXA	___	___	___	___	___%
TOTAL	___	___	___	___	___%

Top 3 Vuln. Críticas Pendentes:	*[CVE-ID] — [Sistema afetado] — [Motivo do atraso na correção]*
Rescans realizados:	*[Nº] — Taxa de confirmação de remediação: ___%*

6. CONFORMIDADE — LGPD, NAC E ATIVOS

Item de Conformidade	Meta	Apurado	Status
Ativos sem agente EDR (Item 03)	≤ 2% do parque	___%	( ) OK ( ) NOK
Administradores com FIDO2 ativo (Item 05)	100%	___%	( ) OK ( ) NOK
Dispositivos não identificados no NAC (Item 09)	≤ 1% da rede	___%	( ) OK ( ) NOK
Incidentes de privacidade reportados no prazo (24h)	100%	___%	( ) OK ( ) NOK
Variação do Risk Score mensal	Redução ou manutenção	___ *pts*	( ) OK ( ) NOK

7. CHAVES FIDO2 (ITEM 05)

Total fornecidas:	38 unidades	Ativas no período:	___
Com defeito / substituídas:	___	Em estoque de reserva:	___
Destinação logística reversa:	*[Comprovante de coleta ecológica: Sim / Não / N.A.]*		

8. ANÁLISE EXECUTIVA E RECOMENDAÇÕES

[Espaço reservado para análise narrativa do Fiscal Técnico: avaliação qualitativa da execução, riscos identificados, tendências observadas e recomendações para o próximo período. Mínimo de 5 linhas.]

9. VALIDAÇÃO E ATESTE PARA PAGAMENTO

⚠ *O ateste do Gestor neste RNS autoriza a Fiscal Administrativa a processar a liquidação da fatura mensal, deduzidas as glosas da Seção 3.*

ELABORADO — CONTRATADA	VERIFICADO — FISCAL TÉCNICO	ATESTADO — GESTOR DO CONTRATO
_____ *[Preposto da Contratada]* Data: __/__/20__	_____ *[Fiscal Técnico / Matr.]* Data: __/__/20__	_____ *[Gestor do Contrato / Matr.]* Data: __/__/20__

APÊNDICE IX - DECLARAÇÃO DE ADEQUAÇÃO À LGPD E COMPROMISSO DE TRATAMENTO SEGURO DE DADOS PESSOAIS

Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais

1. IDENTIFICAÇÃO DO DECLARANTE

Razão Social:	*[Razão Social da Contratada]*
CNPJ:	*xx.xxx.xxx/xxxx-xx*
Representante Legal:	*[Nome / CPF / Cargo]*
Endereço da Sede:	*[Rua, nº, Cidade, UF, CEP]*
DPO / Encarregado de Dados:	*[Nome completo / e-mail de contato do DPO]*
Contrato a que se refere:	*Contrato nº ___/20__ — ITEC-AL — Solução Integrada de Cibersegurança*

2. DECLARAÇÕES DE CONFORMIDADE

A empresa acima identificada, na qualidade de OPERADORA DE DADOS (art. 5º, VII, LGPD), sob as penas da lei, DECLARA que:

I. **POSSUI PROGRAMA CORPORATIVO DE PROTEÇÃO DE DADOS PESSOAIS**

Implementou e mantém Programa de Conformidade com a LGPD (Privacy by Design e Privacy by Default), abrangendo políticas internas, procedimentos operacionais, controles técnicos e treinamento regular de equipe para o tratamento lícito e seguro de dados pessoais.

II. **TRATA DADOS PESSOAIS SOMENTE NAS HIPÓTESES LEGAIS DA LGPD**

O tratamento de dados pessoais de titulares identificados ou identificáveis — incluindo servidores públicos, cidadãos e usuários dos sistemas do ITEC-AL — será realizado exclusivamente com base nas hipóteses de licitude dos arts. 7º e 11 da LGPD aplicáveis ao contexto contratual, especialmente o cumprimento de obrigação legal e o exercício regular de direitos em processo contratual.

III. **ADOTA MEDIDAS TÉCNICAS E ORGANIZACIONAIS DE SEGURANÇA**

Adota, no mínimo, as seguintes medidas:

- Criptografia AES-256 para dados em repouso (at rest) e TLS 1.3 para dados em trânsito (in transit);
- Controle de Acesso Baseado em Funções (RBAC) com autenticação multifatorial via FIDO2 para acessos administrativos;
- Registros imutáveis de auditoria (audit log protegido por hash), impedindo alteração retroativa;
- Pseudonimização e anonimização de dados pessoais sempre que tecnicamente viável, especialmente em ambientes de teste e análises forenses;
- Processo formal de Avaliação de Impacto à Proteção de Dados (RIPD/DPIA) para operações de alto risco;

- Segregação lógica completa entre ambientes de clientes distintos (isolamento de tenants);
- Política de retenção com prazos definidos e processo de eliminação segura ao término da finalidade.

IV. **COMUNICARÁ INCIDENTES NO PRAZO LEGAL (24 HORAS)**

Compromete-se a comunicar ao ITEC-AL, em até 24 horas após ciência do fato, qualquer incidente de segurança com dados pessoais que possa acarretar risco aos titulares, com informações sobre natureza dos dados afetados, quantidade de titulares, medidas de contenção e prazo de eliminação dos riscos, conforme art. 48 da LGPD e Resolução CD/ANPD nº 2/2022.

V. **ATENDERÁ AOS DIREITOS DOS TITULARES DE DADOS**

Garantirá ao ITEC-AL todos os meios para atendimento das solicitações de titulares nos termos do art. 18 da LGPD — confirmação, acesso, retificação, portabilidade, oposição, eliminação e revogação — no prazo máximo de 15 dias da requisição.

VI. **NÃO REALIZARÁ TRANSFERÊNCIA INTERNACIONAL SEM AUTORIZAÇÃO**

Não transferirá dados pessoais do ITEC-AL para países ou organismos internacionais sem grau de proteção equivalente à LGPD, exceto mediante autorização prévia e escrita do ITEC-AL, somente nas hipóteses do art. 33 da LGPD.

VII. **GARANTIRÁ DEVOLUÇÃO E ELIMINAÇÃO DOS DADOS AO TÉRMINO**

Ao término da vigência ou em caso de rescisão, devolverá todos os dados em formato estruturado e legível e procederá com a exclusão definitiva (sanitização certificada conforme NIST SP 800-88), apresentando Certificado de Destruição de Dados no prazo de 30 dias.

VIII. **ESTÁ SUJEITA ÀS SANÇÕES DA LGPD E DO CONTRATO**

Tem plena ciência de que o descumprimento sujeitará a Contratada, cumulativamente, às penalidades contratuais, às sanções da ANPD (art. 52 LGPD — até R$ 50.000.000,00 por infração) e à responsabilidade civil pelos danos causados a titulares (art. 42 LGPD).

3. SUBOPERADORES E INFRAESTRUTURA DE NUVEM

Caso a Contratada utilize subcontratados ou provedores de nuvem (suboperadores) para processamento de dados do ITEC-AL, declara que:

- Todos os suboperadores estão contratualmente vinculados a obrigações de proteção de dados equivalentes às previstas neste instrumento;
- Os suboperadores foram submetidos a due diligence de privacidade e segurança antes de receberem acesso a dados do ITEC-AL;
- A Contratada responde perante o ITEC-AL por todo e qualquer ato dos suboperadores que resulte em violação da LGPD ou das cláusulas de privacidade do contrato (art. 39, LGPD).

Provedor de Nuvem / Suboperador:	*[Nome do provedor de nuvem / datacenter utilizado]*
País / Região dos Servidores:	*[Brasil — Região: ___] ou [País: ___ — Mecanismo de transferência: ___]*

Certificações de Segurança:	( ) ISO 27001 ( ) SOC 2 Tipo II ( ) PCI-DSS ( ) Outro: ___

4. ASSINATURA E VIGÊNCIA

A presente declaração é firmada sob as penas da lei, sendo válida por toda a vigência do contrato e por mais 5 anos após seu término. Integra o processo administrativo como documento hábil de comprovação de conformidade com a LGPD para fins de auditoria interna, fiscalização pelos órgãos de controle e eventuais processos sancionatórios perante a ANPD.

_____ *[Nome do Representante Legal da Contratada]* Representante Legal — CPF: ___.___.___-__ Data: ____/____/20__	_____ *[Nome do DPO / Encarregado de Dados]* DPO — CPF: ___.___.___-__ Data: ____/____/20__

⚠ *Esta declaração deve ser reapresentada a cada renovação contratual e sempre que houver alteração relevante nos processos de tratamento de dados da Contratada.*

APÊNDICE X – Modelo de Proposta de Preços

PROPOSTA COMERCIAL
Pregão Eletrônico nº ___/20__ — Solução Integrada de Cibersegurança — ITEC-AL

1. IDENTIFICAÇÃO DO PROPONENTE

Razão Social:	*[Razão Social]*
CNPJ:	*xx.xxx.xxx/xxxx-xx*
Endereço Completo:	*[Rua, nº, Cidade, UF, CEP]*
Representante Legal:	*[Nome / CPF / Cargo]*
Telefone / E-mail:	*[Telefone] / [e-mail comercial]*
Dados Bancários:	*[Banco] / Ag. [____] / CC [_____] — para fins de pagamento*
Validade da Proposta:	60 (sessenta) dias corridos, contados da data de abertura da sessão do Pregão Eletrônico.

2. PROPOSTA DE PREÇOS — ITENS DO OBJETO

⚠ *Preencher os campos destacados. Os valores devem incluir todos os tributos, encargos, custos operacionais e lucro. Os totais são calculados na Planilha de Composição de Custos (Apêndice XI), que acompanha obrigatoriamente esta proposta.*

Item	CATSER	Descrição Resumida	Unidade de Medida	Qtd.	Valor Unit. (R$)	Total Item (R$)
01	27162	Plataforma Unificada de Cibersegurança (Core)	Lic. Anual / Ativo	1.430	*R$* _____	*R$* _____
02	27162	Inteligência e Proteção de Marca (OSINT/EASM)	Ass. Anual / Dom.	17.499	*R$* _____	*R$* _____
03	27162	Proteção de Endpoint (EDR/XDR)	Lic. Anual / Endpt.	1.430	*R$* _____	*R$* _____

04	27162	Segurança de Containers (CS/KSPM)	Lic. Anual / Node	11	*R$* _____	*R$* _____
05	46639	Chaves de Hardware FIDO2	Unidade	38	*R$* _____	*R$* _____
06	20605	Operação SOC e Suporte 24x7	Mês	12	*R$* _____	*R$* _____
07	16217	Implantação, Integração e Treinamento	Hora Técnica	600	*R$* _____	*R$* _____
08	5238	Gestão de Vulnerabilidades e Apoio à Remediação	Mês	12	*R$* _____	*R$* _____
09	27049	Controle de Acesso à Rede (NAC)	Lic. Anual / Disp.	2.250	*R$* _____	*R$* _____
VALOR GLOBAL TOTAL (12 meses):					**R$** _____	

Por extenso:
_____
_____

3. DECLARAÇÕES OBRIGATÓRIAS

Ao apresentar esta proposta, o proponente DECLARA expressamente que:

1. Os preços propostos incluem todos os custos diretos e indiretos, tributos federais, estaduais e municipais (PIS, COFINS, CSLL, IRPJ, ISS/ICMS conforme aplicável), encargos trabalhistas, viagens, hospedagem, seguros, lucro e demais despesas para a plena execução do objeto, não cabendo remuneração adicional de qualquer natureza;
2. Tomou pleno conhecimento do Edital, Termo de Referência, Apêndices e Matriz de Riscos (Apêndice III), aceitando integralmente as condições de execução e a alocação de riscos neles prevista;
3. A empresa mantém todas as condições de habilitação exigidas no Edital e comprometendo-se a informar imediatamente qualquer alteração que implique perda dessas condições durante a vigência do contrato;
4. Possui — ou contratará previamente ao início da execução — os profissionais com as certificações exigidas no item 4.44 do Termo de Referência, e que as informações curriculares e de certificação são fidedignas;
5. Instalará escritório operacional na Região Nordeste do Brasil no prazo máximo de 60 dias da assinatura do contrato, conforme item 4.105 do Termo de Referência;

6. Não mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigentes ou agentes públicos do ITEC-AL que atuem na contratação ou fiscalização;
7. Aceita os critérios de medição, fórmulas de glosa e apuração do IMR previstos na Seção 8 do Termo de Referência e no Apêndice IV (ANS/SLA).

4. ASSINATURA

Por ser expressão da verdade e para que produza seus legais efeitos, assino a presente proposta.

_____ *[Nome do Representante Legal]* [Cargo] — CNPJ: xx.xxx.xxx/xxxx-xx Data: ____/____/20__	_____ *[Local], ____/____/20__* Data: ____/____/20__

Proposta enviada exclusivamente via sistema de Pregão Eletrônico

INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS

Estudo Técnico Preliminar 4/2026

1. Informações Básicas

Número do processo: E:41506.0000000158/2026

2. Descrição da necessidade

O Instituto de Tecnologia em Informática e Informação do Estado de Alagoas – ITEC - Instituto de Tecnologia em Informática e Informação do Estado de Alagoas, exerce papel estratégico na gestão, operação e suporte da infraestrutura tecnológica que sustenta os sistemas, portais institucionais e serviços digitais utilizados pelos órgãos e entidades da Administração Pública Estadual.

No contexto atual de transformação digital da administração pública, a dependência de sistemas informatizados, plataformas digitais e infraestrutura de rede tornou-se elemento central para a prestação de serviços públicos à população. Nesse cenário, a segurança da informação e a proteção contra ameaças cibernéticas passam a ser requisitos fundamentais para garantir a continuidade dos serviços governamentais, a integridade das informações institucionais e a proteção de dados sensíveis.

Nos últimos anos, a intensificação de ataques cibernéticos direcionados a órgãos governamentais tem evidenciado a necessidade de adoção de mecanismos avançados de proteção e monitoramento contínuo da infraestrutura tecnológica. Incidentes de segurança envolvendo tentativas de invasão e indisponibilidade de portais governamentais demonstram que ambientes digitais institucionais estão sujeitos a ameaças constantes, capazes de comprometer a disponibilidade de serviços essenciais, além de expor informações estratégicas da administração pública.

Nesse contexto, o ITEC – Instituto de Tecnologia em Informática e Informação do Estado de Alagoas, na condição de órgão responsável pela governança, gestão e operação da infraestrutura tecnológica que sustenta os sistemas e serviços digitais da Administração Pública Estadual, possui a necessidade institucional de fortalecer sua capacidade de prevenção, detecção, monitoramento e resposta a incidentes de segurança da informação em todo o ambiente tecnológico sob sua responsabilidade.

Considerando a complexidade e a amplitude do parque tecnológico administrado pelo Instituto, que envolve aplicações web, ambientes baseados em contêineres, orquestração por Kubernetes, pods, servidores e estações de trabalho, além da infraestrutura de suporte aos portais e sistemas governamentais, torna-se necessária a implementação de mecanismos estruturados e contínuos de gestão de vulnerabilidades, capazes de identificar, analisar e tratar riscos de segurança de forma sistemática.

Adicionalmente, o ITEC necessita estruturar e ampliar sua camada de segurança da informação, de forma a garantir maior proteção dos ativos tecnológicos do Estado e assegurar a adoção de boas práticas e padrões reconhecidos de segurança da informação, alinhados a referenciais nacionais e internacionais, tais como a ISO/IEC 27001, a Lei Geral de Proteção de Dados Pessoais (LGPD), a Política Nacional de Cibersegurança (PNCiber) e a Estratégia Nacional de Cibersegurança (E-Ciber).

Diante desse cenário, identifica-se a necessidade institucional de elevar o nível de maturidade de sua gestão de segurança da informação, aprimorar os processos de identificação e mitigação de vulnerabilidades e fortalecer a proteção da infraestrutura tecnológica que suporta os serviços digitais do Governo do Estado de Alagoas.

Outro aspecto relevante refere-se à necessidade de garantir conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que diz respeito à proteção de dados pessoais tratados pelos sistemas governamentais hospedados ou gerenciados pelo Instituto. A implementação de mecanismos robustos de segurança da informação contribui diretamente para a redução de riscos associados a vazamentos de dados, acessos indevidos e outras ameaças que possam comprometer a privacidade dos cidadãos.

Portanto, a necessidade do ITEC consiste em assegurar que o ambiente tecnológico sob sua gestão esteja resiliente e devidamente protegido contra ameaças cibernéticas, contribuindo para a continuidade dos serviços governamentais, a proteção das informações institucionais e a segurança dos dados da sociedade, preservando a confiança da população nas plataformas digitais do Estado.

3. Área requisitante

Área Requisitante	Responsável

4. Necessidades de Negócio

Considerando as atribuições institucionais do ITEC – Instituto de Tecnologia em Informática e Informação do Estado de Alagoas, responsáveis pela gestão, operação e sustentação da infraestrutura tecnológica que suporta sistemas, redes, portais e serviços digitais da Administração Pública Estadual, identificam-se lacunas operacionais e riscos estratégicos que precisam ser mitigados para assegurar a perenidade dos serviços públicos digitais.

Tais necessidades decorrem da crescente dependência dos órgãos estaduais de plataformas digitais para a execução de suas atividades, bem como da ampliação da superfície de exposição a ameaças cibernéticas que podem comprometer a disponibilidade, integridade e confidencialidade das informações institucionais e dos serviços públicos digitais.

Para o cumprimento de sua missão e a preservação da confiança dos cidadãos nas instituições estaduais, o ITEC apresenta as seguintes necessidades de negócio:

1.2.1 Garantir a continuidade dos serviços digitais governamentais

Os sistemas, portais e plataformas digitais utilizados pelos órgãos da Administração Pública Estadual são essenciais para o funcionamento das atividades administrativas e para o atendimento à população. Dessa forma, torna-se necessário assegurar a disponibilidade e a resiliência desses serviços diante de falhas de segurança, incidentes cibernéticos ou exploração de vulnerabilidades tecnológicas.

1.2.2. Proteger os ativos de informação da Administração Pública

O ambiente tecnológico gerenciado pelo ITEC concentra um grande volume de informações institucionais e dados sensíveis utilizados pelos órgãos estaduais. Assim, existe a necessidade de garantir a proteção desses ativos contra acessos não autorizados, vazamentos de dados, manipulação indevida de informações e outras ameaças que possam comprometer a integridade e a confidencialidade das informações públicas.

1.2.3. Fortalecer a capacidade institucional de prevenção e resposta a incidentes de segurança

Diante da evolução e da crescente sofisticação das ameaças cibernéticas, torna-se necessário fortalecer a capacidade institucional de identificar vulnerabilidades, detectar atividades suspeitas e responder de forma eficiente a incidentes de segurança que possam afetar a infraestrutura tecnológica e os serviços digitais do Estado.

1.2.4. Elevar o nível de maturidade em segurança da informação

A complexidade do ambiente tecnológico administrado pelo Instituto exige o aprimoramento contínuo das práticas de governança e gestão de segurança da informação, com maior capacidade de identificação, avaliação e tratamento de riscos associados à infraestrutura digital do Estado.

1.2.5. Atender às diretrizes e políticas nacionais de segurança cibernética

Há necessidade de fortalecer a estrutura de segurança da informação de forma alinhada às diretrizes e estratégias nacionais voltadas à proteção do espaço cibernético brasileiro, promovendo o desenvolvimento de capacidades institucionais de proteção digital no âmbito da administração pública.

1.2.6. Garantir conformidade com a legislação de proteção de dados

Considerando que diversos sistemas e plataformas digitais sob gestão do Instituto realizam tratamento de dados pessoais, torna-se necessário garantir que o ambiente tecnológico possua mecanismos adequados para proteção dessas informações, contribuindo para a conformidade com as obrigações estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2.7. Redução da Superfície de Exposição e Mitigação de Riscos Críticos

O ITEC necessita eliminar a atual fragmentação na visibilidade de ativos, garantindo que vulnerabilidades em sistemas críticos sejam identificadas e tratadas antes que resultem em incidentes de alto impacto financeiro, interrupção de serviços essenciais ou danos à imagem do Governo Estadual.

O suprimento dessas necessidades é vital para a sustentabilidade da estratégia de Governo Digital de Alagoas, garantindo que a modernização administrativa seja acompanhada por um ambiente de resiliência e confiança digital.

5. Necessidades Tecnológicas

Considerando a crescente dependência da Administração Pública de sistemas digitais, infraestrutura de rede e plataformas tecnológicas para execução de suas atividades institucionais, torna-se necessário identificar soluções tecnológicas capazes de fortalecer a segurança da informação e a proteção da infraestrutura digital do Estado.

Nesse contexto, foram identificadas as seguintes **necessidades tecnológicas a serem atendidas pela solução a ser contratada**, visando garantir maior segurança, disponibilidade e confiabilidade do ambiente tecnológico administrado pelo ITEC - Instituto de Tecnologia em Informática e Informação do Estado de Alagoas.

Monitoramento contínuo do ambiente tecnológico

A solução deverá possibilitar o monitoramento contínuo dos ativos tecnológicos, incluindo redes, servidores, aplicações e demais componentes da infraestrutura de tecnologia da informação, com o objetivo de identificar comportamentos anômalos, tentativas de acesso indevido e outras atividades que possam representar risco à segurança do ambiente digital.

Esse monitoramento deverá permitir a identificação rápida de eventos de segurança e a geração de alertas que possibilitem a adoção de medidas preventivas e corretivas.

Identificação e gestão de vulnerabilidades

A solução deverá disponibilizar mecanismos capazes de identificar vulnerabilidades existentes na infraestrutura tecnológica, permitindo a análise de riscos e a adoção de medidas para mitigação de falhas de segurança.

Nesse sentido, espera-se que a solução permita:

- Realização de varreduras periódicas no ambiente tecnológico;
- Identificação de falhas de segurança em sistemas e dispositivos;
- Classificação de vulnerabilidades conforme níveis de criticidade;
- Apoio na priorização de ações corretivas.

Detecção de ameaças e incidentes de segurança

A solução deverá possuir recursos capazes de detectar possíveis ameaças cibernéticas e incidentes de segurança que possam comprometer a integridade, confidencialidade ou disponibilidade das informações institucionais.

Essa capacidade deverá permitir a identificação de comportamentos suspeitos e padrões de ataque, contribuindo para uma resposta mais ágil diante de incidentes que possam afetar o ambiente tecnológico.

Consolidação e análise de registros de eventos (logs)

Considerando o elevado volume de registros gerados pelos sistemas e dispositivos tecnológicos, torna-se necessária a adoção de solução capaz de consolidar e analisar esses registros de forma centralizada.

Essa funcionalidade permitirá:

- Centralização de registros de eventos de segurança;
- Análise correlacionada de informações provenientes de diferentes fontes;
- Identificação de padrões de comportamento suspeitos;
- Apoio às atividades de investigação de incidentes.

Disponibilização de relatórios e indicadores de segurança

A solução deverá possibilitar a geração de relatórios técnicos e gerenciais que permitam acompanhar o nível de segurança do ambiente tecnológico, incluindo indicadores relacionados a vulnerabilidades identificadas, eventos de segurança registrados e incidentes detectados.

Essas informações são importantes para apoiar o processo de gestão de riscos e tomada de decisões estratégicas relacionadas à segurança da informação.

Integração com a infraestrutura tecnológica existente

A solução deverá possuir capacidade de integração com os sistemas, redes e equipamentos já utilizados pela Administração Pública Estadual, permitindo sua utilização de forma compatível com o ambiente tecnológico existente.

Essa integração é essencial para garantir a eficiência das atividades de monitoramento e análise de segurança da informação.

Modelo tecnológico da solução

Considerando as tendências atuais de mercado e a necessidade de atualização constante das tecnologias de segurança digital, torna-se desejável que a solução adotada seja disponibilizada em modelo que permita atualização contínua, escalabilidade e otimização da gestão tecnológica.

Esse modelo possibilita maior eficiência operacional, redução da necessidade de infraestrutura local e acesso a tecnologias atualizadas de proteção contra ameaças cibernéticas.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Além das necessidades de negócio e tecnológicas previamente identificadas, a solução de Tecnologia da Informação e Comunicação a ser contratada deverá atender a requisitos adicionais considerados essenciais para garantir a adequada execução dos serviços, a eficiência operacional da solução e a mitigação de riscos associados à segurança da infraestrutura digital administrada pelo ITEC - Instituto de Tecnologia em Informática e Informação do Estado de Alagoas.

Nesse sentido, considera-se necessário que a solução contemple condições estruturais, operacionais e logísticas capazes de assegurar a pronta resposta a incidentes de segurança da informação e o suporte técnico adequado às atividades de implantação, operação e manutenção da solução.

Presença regional para suporte técnico e operação

Considera-se imprescindível, para a adequada execução dos serviços, especialmente no que se refere ao suporte técnico presencial, à coordenação de equipes de campo e à gestão de ativos físicos relacionados à solução de segurança da informação, que a empresa contratada possua ou venha a instalar **estrutura administrativa e técnica na Região Nordeste do Brasil**.

A presença regional visa garantir maior agilidade no atendimento de demandas operacionais, redução de tempo de deslocamento para atendimento presencial e maior proximidade institucional com a Administração Pública contratante.

Estrutura operacional da unidade regional

A unidade regional deverá funcionar como ponto de apoio técnico e administrativo para a execução dos serviços contratados, podendo desempenhar, entre outras, as seguintes funções:

- servir como **ponto de contato regional** entre a Administração e a contratada para assuntos operacionais e de fiscalização contratual;
- atuar como **base de apoio para equipes técnicas responsáveis pela gestão de vulnerabilidades e atividades operacionais de segurança da informação**;
- apoiar a coordenação das equipes envolvidas na operação do monitoramento de segurança e nas atividades de implantação da solução;
- possibilitar suporte logístico às atividades técnicas que eventualmente demandem presença física.

Essa estrutura contribuirá para assegurar maior eficiência na execução dos serviços e maior capacidade de resposta diante de eventuais incidentes que demandem atuação presencial especializada.

Infraestrutura mínima da unidade regional

A unidade regional deverá dispor de infraestrutura mínima que permita o adequado suporte às atividades relacionadas à execução do contrato, incluindo:

- endereço físico formalmente estabelecido para recebimento de comunicações administrativas;
- estrutura básica para suporte às equipes técnicas responsáveis pela implantação e operação da solução;
- espaço adequado para guarda e controle de equipamentos de segurança ou dispositivos eventualmente utilizados na execução dos serviços;
- possibilidade de utilização do espaço para reuniões técnicas, alinhamentos operacionais e reuniões periódicas de acompanhamento contratual.

Prazo para comprovação da estrutura regional

Caso a empresa contratada ainda não possua unidade estabelecida na região no momento da contratação, deverá providenciar sua instalação e plena operacionalização no prazo máximo de **60 (sessenta) dias corridos**, contados a partir da assinatura do contrato ou da emissão da Ordem de Início de Serviço.

Para fins de comprovação da estrutura operacional, deverão ser apresentados à fiscalização contratual documentos que evidenciem a existência e funcionamento da unidade regional, tais como:

- comprovante de endereço da unidade;
- documentação ou autorização de funcionamento, quando aplicável;
- identificação dos profissionais responsáveis pelo atendimento regional.

Justificativa da exigência

A exigência de presença regional fundamenta-se na necessidade de garantir **prontidão operacional, capacidade de resposta rápida a incidentes e suporte técnico adequado à infraestrutura tecnológica crítica da Administração Pública**.

A proximidade geográfica da equipe técnica contribui para reduzir riscos associados à indisponibilidade de serviços digitais, possibilitando maior eficiência na coordenação de atividades técnicas e no atendimento de situações emergenciais relacionadas à segurança da informação.

Além disso, a existência de ponto de contato regional fortalece a governança contratual, permitindo maior interação entre a Administração Pública e a contratada, bem como maior efetividade no acompanhamento e fiscalização da execução dos serviços.

A exigência de estrutura regional encontra respaldo na jurisprudência do Tribunal de Contas da União, que admite a previsão de requisitos relacionados à infraestrutura operacional da contratada quando demonstrada sua pertinência para a adequada execução do objeto contratual, conforme entendimento

consolidado nos Acórdão 1214/2013 – Plenário (TCU), Acórdão 2622/2013 – Plenário (TCU) e Acórdão 1632/2012 – Plenário (TCU), os quais reconhecem a possibilidade de exigência de estrutura técnica ou logística quando necessária à eficiência da execução contratual e devidamente justificada no processo de contratação.

7. Estimativa da demanda - quantidade de bens e serviços

A definição dos quantitativos da solução integrada de cibersegurança foi realizada com base em **levantamento do ambiente tecnológico**, **identificação dos ativos a serem protegidos**, **análise do perfil de uso da infraestrutura institucional**, **projeção de crescimento do ambiente** e **aplicação de margem de segurança operacional**, com o objetivo de assegurar cobertura suficiente durante a vigência contratual.

A metodologia adotada observou as seguintes etapas:

a) levantamento preliminar dos ativos computacionais, usuários, dispositivos de rede e serviços digitais do ambiente institucional;

b) identificação dos componentes da solução necessários à proteção do ambiente de TIC; **c)** dimensionamento dos quantitativos por item, de acordo com a métrica de licenciamento ou unidade de consumo aplicável;

d) aplicação de margem técnica, quando necessária, para absorver crescimento do ambiente, substituições, expansões e contingências operacionais.

Com base nessa metodologia, foram definidos os quantitativos a seguir.

Plataforma Unificada de Cibersegurança (Core)

A estimativa para a plataforma central de cibersegurança considerou o total de ativos computacionais e ativos de infraestrutura relevantes para monitoramento e correlação de eventos de segurança.

Base de levantamento

- 120 estações de trabalho;
- 31 servidores físicos;
- 897 máquinas virtuais;
- estimativa de 200 ativos de rede e segurança com geração de telemetria e eventos;
- margem para crescimento vegetativo e inclusão de novos ativos durante a vigência.

Memória de cálculo

Ativos computacionais: 120 + 31 + 897 = **1.048 ativos**

Ativos de rede e segurança: **200 ativos**

Subtotal: 1.048 + 200 = **1.248 ativos**

Margem técnica e operacional para expansão, contingência e arredondamento contratual:
aproximadamente 14,6%

Quantitativo estimado

1.430 licenças anuais por ativo

Inteligência e Proteção de Marca (OSINT/EASM)

A estimativa deste item considerou a necessidade de monitoramento da superfície externa de exposição digital da instituição, abrangendo domínios, subdomínios e endereços de correio eletrônico associados à organização.

Base de levantamento

- 1 domínio institucional principal;
- 5.000 subdomínios mapeados/estimados;
- 8.959 contas de e-mail institucionais;
- margem para expansão do ambiente de exposição digital, novos subdomínios, aliases, contas institucionais e ativos correlatos monitoráveis.

Memória de cálculo

Domínio principal: **1**

Subdomínios: **5.000**

E-mails institucionais: **8.959**

Subtotal: 1 + 5.000 + 8.959 = **13.960 ativos de exposição**

Margem técnica para crescimento, variação de inventário, ativos correlacionados e arredondamento contratual: **aproximadamente 25,3%**

Quantitativo estimado 17.499 unidades de assinatura anual por domínio/e-mail

Proteção de Endpoint (EDR/XDR)

A estimativa deste item considerou os endpoints e ativos computacionais passíveis de instalação de agentes ou mecanismos equivalentes de proteção avançada.

Base de levantamento

- 120 estações de trabalho;
- 31 servidores físicos;
- 897 máquinas virtuais;
- estimativa de crescimento do parque de endpoints e servidores protegidos ao longo da vigência contratual;
- reserva para substituições, novas ativações e contingência operacional.

Memória de cálculo

Base atual de endpoints e servidores: 120 + 31 + 897 = **1.048 ativos**

Margem técnica para expansão, contingência e padronização contratual: **aproximadamente 36,5%**

Quantitativo estimado 1.430 licenças anuais por endpoint

Segurança de Web e Containers (CS/KSPM)

A estimativa para segurança de containers e postura de segurança em workloads foi definida com base em cenário de adoção seletiva e progressiva de ambientes containerizados e cargas expostas na camada web, considerando a realidade atual do ambiente e sua evolução previsível.

Base de levantamento

- existência predominante de ambiente virtualizado tradicional;
- previsão de uso de containers em serviços críticos, pipelines, homologação, desenvolvimento e possíveis clusters reduzidos;
- adoção de quantitativo focalizado em nodes/hosts estratégicos, compatível com estágio atual de maturidade tecnológica do ambiente.

Metodologia

Em vez de replicar o quantitativo total do ambiente virtual, foi adotado critério de **dimensionamento seletivo**, concentrando licenciamento sobre hosts /nodes efetivamente destinados a workloads containerizados ou sujeitos à gestão de postura de segurança específica.

Quantitativo estimado 11 licenças anuais por node

Chaves de Hardware (FIDO2)

A estimativa considerou a necessidade de autenticação forte para perfis críticos e privilegiados, sem adoção universal para todos os usuários.

Base de levantamento

- 188 colaboradores;
- priorização de perfis com maior criticidade, tais como:
    - administradores de rede e segurança;
    - equipe técnica de TIC;
    - gestores e diretores;
    - usuários com acesso privilegiado;
    - operadores de sistemas críticos e financeiros;
- previsão de estoque técnico para reposição, contingência e novas designações.

Memória de cálculo

Cobertura focal para perfis críticos e privilegiados, acrescida de reserva técnica:
quantitativo estimado de **38 unidades**

Quantitativo estimado 38 unidades

Operação de Segurança (SOC) e Suporte 24x7

A estimativa deste item decorre da natureza continuada do serviço, que deve ser prestado de forma ininterrupta ao longo da vigência contratual.

Metodologia

Por se tratar de serviço contínuo de monitoramento, triagem, análise e suporte especializado, a unidade de medida adotada corresponde à prestação mensal do serviço.

Quantitativo estimado 12 meses

Implantação, Integração e Treinamento

A estimativa de horas técnicas foi calculada com base na complexidade de implantação da solução, necessidade de integração com o ambiente existente e capacitação da equipe.

Premissas consideradas

- instalação e parametrização inicial da plataforma;
- integração com diretórios, ativos de rede, firewalls, logs e ambientes legados;
- configuração de regras, políticas, conectores e painéis;
- apoio à ativação dos módulos contratados;
- treinamento técnico-operacional da equipe responsável;
- ajustes assistidos pós-implantação.

Memória de cálculo

Foi adotado quantitativo global de **600 horas técnicas**, entendido como suficiente para:

- implantação inicial;
- integrações prioritárias;
- ajustes operacionais;
- treinamento e transferência de conhecimento.

Quantitativo estimado 600 horas técnicas

Gestão de Vulnerabilidades e Apoio à Remediação

A estimativa decorre da natureza continuada do serviço de identificação, classificação, tratamento e acompanhamento de vulnerabilidades no ambiente tecnológico.

Metodologia

Por se tratar de serviço prestado de forma recorrente, com acompanhamento contínuo do ambiente e apoio técnico à remediação, a unidade de medida adotada corresponde à prestação mensal.

Quantitativo estimado 12 meses

Controle de Acesso à Rede (NAC)

A estimativa para NAC considerou todos os dispositivos com potencial de autenticação, autorização, postura ou controle de acesso à rede corporativa, incluindo acessos locais e remotos.

Base de levantamento

- 188 usuários com, em média, 2 dispositivos principais (notebook + celular):
  188 × 2 = **376 dispositivos**
- 120 estações fixas;
- 70 dispositivos IoT/câmeras;
- 1.127 usuários/acessos vinculados a VPN ou acesso remoto;
- margem para visitantes, dispositivos temporários, ativos não inventariados e expansão da rede.

Memória de cálculo

Dispositivos móveis e notebooks: **376**

Estações fixas: **120**

IoT/câmeras: **70**

VPN/acesso remoto: **1.127**

Subtotal: 376 + 120 + 70 + 1.127 = **1.693 dispositivos**

Margem técnica e operacional para crescimento, visitantes, contingência e arredondamento contratual: **aproximadamente 32,9%**

Quantitativo estimado 2.250 licenças anuais por dispositivo

Quadro consolidado da metodologia de estimativa

Item	Especificação	CATSER /CATMAT	Unidade	Base metodológica	Quantitativo
1	Plataforma Unificada de Cibersegurança (Core)	27502	Licença anual/ativo	Ativos computacionais + ativos de rede + margem operacional	1.430
2	Inteligência e Proteção de Marca (OSINT/EASM)	27502	Assinatura anual	Domínio + subdomínios + e-mails + margem de expansão	17.499
3	Proteção de Endpoint (EDR/XDR)	27502	Licença anual/endpoint	Endpoints e servidores + margem de crescimento	1.430
4	Segurança de Web e Containers (CS /KSPM)	27502	Licença anual/node	Nodes estratégicos para workloads containerizados e camada web	11
5	Chaves de Hardware (FIDO2)	485464	Unidade	Perfis críticos + usuários privilegiados + reserva técnica	38
6	Operação de Segurança (SOC) e Suporte 24x7	26999	Mês	Serviço contínuo durante a vigência contratual	12
7	Implantação, Integração e Treinamento	3840	Hora técnica	Estimativa de esforço técnico de implantação e capacitação	600
8	Gestão de Vulnerabilidades e Apoio à Remediação	27014	Mês	Serviço continuado durante a vigência contratual	12
9	Controle de Acesso à Rede (NAC)	27502	Licença anual/dispositivo	Dispositivos locais e remotos + margem operacional	2.250

8. Levantamento de soluções

Análise das soluções disponíveis no mercado

Com base em levantamento técnico e análise de práticas adotadas em organizações públicas e privadas, foram identificadas três alternativas principais para atendimento da necessidade institucional.

Solução 1 – Aquisição de licenças de softwares especializados

Essa alternativa consiste na aquisição de licenças de softwares de segurança da informação, incluindo ferramentas voltadas para:

- gestão de vulnerabilidades;
- monitoramento de eventos de segurança;
- proteção de endpoints;
- análise de incidentes;
- apoio à governança de tecnologia da informação.

Nesse modelo, o ITEC seria responsável por:

- implantar as ferramentas adquiridas;
- administrar a infraestrutura tecnológica necessária;
- realizar monitoramento contínuo dos eventos de segurança;
- conduzir análises técnicas e respostas a incidentes cibernéticos.

Embora esse modelo proporcione maior autonomia operacional, ele exige a existência de equipe técnica altamente especializada e permanentemente atualizada, capaz de acompanhar a evolução das ameaças digitais e das tecnologias de proteção.

Adicionalmente, a aquisição isolada de softwares tende a gerar ambiente tecnológico fragmentado, exigindo contratações complementares para suporte, integração de sistemas e atualização tecnológica, o que pode elevar a complexidade de gestão e os custos operacionais ao longo do tempo.

Solução 2 – Desenvolvimento interno da plataforma pelo ITEC

Outra alternativa considerada consiste no desenvolvimento interno de plataforma de governança de segurança da informação e gestão de vulnerabilidades pelo próprio ITEC, utilizando recursos tecnológicos e equipe técnica da instituição.

Esse modelo permitiria maior controle sobre os processos de desenvolvimento, bem como a customização das funcionalidades da solução de acordo com as necessidades específicas da organização.

Entretanto, o desenvolvimento de plataforma própria de segurança cibernética envolve elevada complexidade técnica, exigindo conhecimentos especializados em áreas como:

- engenharia de segurança da informação;
- monitoramento de eventos de segurança (SIEM);
- detecção e resposta a incidentes (EDR/XDR);
- análise de inteligência de ameaças;
- arquitetura de segurança em ambientes híbridos e em nuvem.

Além disso, seria necessário estabelecer estrutura permanente de desenvolvimento, manutenção e atualização da plataforma, considerando a constante evolução das técnicas de ataque cibernético e das tecnologias de defesa digital.

Esse cenário demandaria investimentos significativos em recursos humanos especializados, infraestrutura tecnológica e atualização contínua da solução, podendo comprometer a eficiência operacional e desviar o foco institucional das atividades estratégicas do Instituto.

Solução 3 – Contratação de solução integrada com serviços especializados

A terceira alternativa consiste na contratação de solução integrada de cibersegurança em modelo SaaS (Software as a Service) associada à prestação de serviços especializados.

Esse modelo contempla:

- fornecimento de plataforma integrada de segurança da informação;
- monitoramento contínuo de eventos de segurança (SOC 24x7);
- gestão contínua de vulnerabilidades;
- detecção e resposta a incidentes cibernéticos;
- geração de relatórios técnicos e indicadores de segurança;
- apoio à adequação à Lei Geral de Proteção de Dados;

- capacitação da equipe técnica do Instituto.

Nesse modelo, a empresa contratada assume a responsabilidade pela operação da solução, atualização tecnológica, monitoramento do ambiente e suporte especializado, garantindo que a organização tenha acesso permanente a tecnologias atualizadas e a profissionais especializados em segurança cibernética.

Essa abordagem permite maior escalabilidade da solução, redução da dependência de recursos internos altamente especializados e maior eficiência na gestão dos riscos tecnológicos.

9. Análise comparativa de soluções

Comparativo entre as soluções avaliadas

Critério	Solução 1 – Aquisição de Softwares	Solução 2 – Desenvolvimento Interno	Solução 3 – Serviços Especializados
Natureza da solução	Aquisição de ferramentas	Desenvolvimento próprio	Plataforma + serviços especializados
Investimento inicial	Médio	Alto	Reduzido
Necessidade de equipe especializada	Alta	Muito alta	Moderada
Atualização tecnológica	Dependente de novas aquisições	Responsabilidade interna	Incluída no serviço
Monitoramento contínuo	Limitado	Dependente de estrutura interna	Contínuo (SOC 24x7)
Escalabilidade	Limitada	Dependente da capacidade interna	Alta
Tempo de implantação	Médio	Alto	Reduzido
Risco de obsolescência	Médio	Alto	Baixo
Complexidade operacional	Alta	Muito alta	Moderada

Avaliação Comparativa (Benchmarking)

Contratações similares realizadas por outros órgãos

A análise de contratações realizadas por órgãos da Administração Pública evidencia tendência crescente de adoção de soluções integradas de segurança da informação e governança digital, incluindo:

Órgão	Objeto	Modalidade
Defensoria Pública do Espírito Santo	Licenciamento de solução corporativa de segurança (XDR)	Pregão Eletrônico
DETRAN – ES	Plataforma de segurança da informação e adequação à LGPD	Pregão Eletrônico

https://pncp.gov.br/app/editais/29115474000160/2025/239

https://detran.es.gov.br/pregoes-eletronicos

https://pncp.gov.br/app/editais/00671513000124/2024/39

No contexto das contratações de soluções de Tecnologia da Informação e Comunicação (TIC), especialmente aquelas relacionadas à segurança da informação e à gestão de serviços tecnológicos, a Administração Pública pode adotar diferentes **modelos de contratação**, conforme a natureza do objeto, o grau de complexidade da solução e o nível de maturidade institucional.

A **Instrução Normativa SGD/ME nº 94/2022**, que dispõe sobre o processo de contratação de soluções de TIC no âmbito da Administração Pública Federal, estabelece que a escolha do modelo de contratação deve observar critérios de **eficiência, economicidade, mensuração objetiva dos resultados e mitigação de riscos contratuais**, devendo ser precedida de análise comparativa entre as alternativas disponíveis.

A partir do levantamento de práticas adotadas em contratações similares realizadas por órgãos públicos, bem como da análise das características da solução pretendida, foram identificados os seguintes **modelos de contratação aplicáveis** ao objeto:

I – Contratação por alocação de profissionais especializados

Nesse modelo, a empresa contratada disponibiliza profissionais especializados para atuação direta nas atividades técnicas relacionadas à solução de TIC, permanecendo estes alocados nas dependências do órgão ou atuando remotamente conforme a necessidade institucional.

Embora esse modelo possa proporcionar flexibilidade operacional, ele tende a aproximar-se de uma **contratação de mão de obra**, o que pode gerar riscos de descaracterização do objeto e dificuldades na mensuração objetiva dos resultados entregues.

O **Tribunal de Contas da União (TCU)** tem reiteradamente orientado que contratações de TIC devem priorizar modelos baseados em **resultados mensuráveis e entregas claramente definidas**, evitando estruturas contratuais centradas exclusivamente na disponibilização de profissionais.

II – Contratação por entregáveis técnicos

Nesse modelo, a remuneração da contratada está vinculada à **entrega de produtos ou resultados previamente definidos**, tais como relatórios técnicos, análises de segurança, diagnósticos de vulnerabilidade, implantação de ferramentas ou execução de serviços específicos.

Esse formato permite maior controle sobre as entregas contratuais e facilita o processo de fiscalização, uma vez que os produtos são previamente especificados e possuem critérios objetivos de aceitação.

Contudo, em soluções que exigem **monitoramento contínuo e operação permanente**, como no caso de serviços de cibersegurança, esse modelo pode apresentar limitações, pois não contempla de forma adequada atividades operacionais recorrentes e de natureza contínua.

III – Contratação com remuneração fixa associada a Acordos de Nível de Serviço (ANS)

Nesse modelo, amplamente adotado em contratações de serviços de TIC, a empresa contratada é remunerada mediante valor fixo periódico, condicionado ao cumprimento de **Acordos de Nível de Serviço (ANS)** previamente estabelecidos.

Os ANS definem indicadores de desempenho e parâmetros mínimos de qualidade que devem ser observados durante a execução contratual, tais como:

- tempo de resposta a incidentes;
- disponibilidade da plataforma;
- tempo de tratamento de vulnerabilidades;
- periodicidade de relatórios técnicos;
- níveis de atendimento e suporte.

Esse modelo está alinhado às recomendações da **IN SGD/ME nº 94/2022**, que orienta que os contratos de TIC devem estabelecer **indicadores de desempenho e mecanismos objetivos de avaliação da qualidade dos serviços prestados**.

IV – Contratação sob demanda (pay-per-use)

Nesse modelo, a remuneração da contratada ocorre de acordo com a **quantidade de serviços efetivamente utilizados ou executados**, podendo envolver métricas como número de incidentes analisados, quantidade de análises realizadas ou volume de dados processados.

Embora apresente flexibilidade contratual, esse formato pode gerar **imprevisibilidade orçamentária**, além de dificultar o planejamento financeiro da Administração Pública, especialmente em serviços críticos que demandam disponibilidade permanente.

Avaliação dos modelos de contratação

Considerando as características da solução pretendida, que envolve **monitoramento contínuo de segurança da informação, gestão de vulnerabilidades, resposta a incidentes e suporte técnico especializado**, procedeu-se à análise comparativa dos modelos de contratação identificados.

Verificou-se que o modelo baseado exclusivamente na **alocação de profissionais** não se mostra adequado ao objeto, uma vez que o foco da contratação deve estar nos **resultados e níveis de serviço prestados**, e não na simples disponibilização de mão de obra técnica.

Da mesma forma, o modelo baseado exclusivamente em **entregáveis pontuais** apresenta limitações para soluções que demandam operação contínua e acompanhamento permanente do ambiente tecnológico institucional.

Por sua vez, o modelo de **remuneração fixa associada a Acordos de Nível de Serviço (ANS)** apresenta maior aderência às necessidades institucionais, pois permite:

- estabelecer indicadores objetivos de desempenho;
- garantir previsibilidade orçamentária;
- assegurar a continuidade dos serviços;
- vincular o pagamento ao cumprimento de metas e padrões de qualidade.

Além disso, esse modelo está alinhado às boas práticas de governança de tecnologia da informação, bem como às orientações dos órgãos de controle, que recomendam que contratos de TIC possuam **mecanismos claros de mensuração de desempenho e qualidade dos serviços prestados**.

Conclusão da análise de modelos de contratação

Com base na avaliação realizada, conclui-se que o modelo mais adequado para a contratação da solução pretendida consiste na **prestação de serviços especializados de cibersegurança, associada ao fornecimento de plataforma tecnológica em modelo SaaS, com remuneração periódica vinculada ao cumprimento de Acordos de Nível de Serviço (ANS)**.

Essa abordagem permite à Administração Pública obter uma solução completa e integrada, contemplando não apenas a disponibilização de ferramentas tecnológicas, mas também a operação especializada dos serviços, o monitoramento contínuo do ambiente digital e o suporte técnico necessário para mitigação de riscos cibernéticos.

Adicionalmente, o modelo proposto contribui para:

- otimização dos recursos públicos;
- redução da necessidade de investimentos em infraestrutura própria;
- acesso contínuo a tecnologias atualizadas;

fortalecimento da governança de segurança da informação.

10. Registro de soluções consideradas inviáveis

Durante a elaboração deste Estudo Técnico Preliminar foram avaliadas diferentes alternativas tecnológicas com potencial para atendimento das necessidades institucionais relacionadas à segurança da informação, proteção de ativos digitais e fortalecimento da governança de tecnologia da informação no âmbito do **ITEC – Instituto de Tecnologia em Informática e Informação**.

A análise dessas alternativas considerou critérios técnicos, operacionais e econômicos, tais como capacidade de atendimento das necessidades institucionais, maturidade tecnológica, viabilidade de implantação, necessidade de recursos internos, riscos operacionais e sustentabilidade da solução ao longo do tempo.

Como resultado dessa avaliação, algumas alternativas foram consideradas **inviáveis ou inadequadas** para atendimento das necessidades institucionais, conforme descrito a seguir.

Aquisição isolada de ferramentas de segurança da informação

Uma das alternativas analisadas consistiu na aquisição de ferramentas isoladas de segurança da informação, como soluções independentes de antivírus corporativo, monitoramento de eventos, gestão de vulnerabilidades e proteção de rede.

Entretanto, verificou-se que essa abordagem resultaria em um ambiente tecnológico fragmentado, composto por múltiplas ferramentas com diferentes arquiteturas e padrões de integração, o que poderia aumentar significativamente a complexidade de gestão e operação da solução.

Além disso, a operação eficiente dessas ferramentas exigiria a manutenção de equipe técnica altamente especializada para realizar atividades como:

- integração entre sistemas de segurança;
- monitoramento contínuo de eventos;
- análise de incidentes cibernéticos;
- atualização permanente das ferramentas de proteção.

Considerando as limitações de recursos humanos especializados e os custos operacionais associados à gestão de múltiplas ferramentas isoladas, concluiu-se que essa alternativa não se mostra adequada para o atendimento das necessidades institucionais do Instituto.

Desenvolvimento interno de plataforma própria de cibersegurança

Outra alternativa analisada consistiu no desenvolvimento interno de uma plataforma própria de segurança da informação pelo próprio **ITEC**, utilizando recursos tecnológicos e equipe técnica da instituição.

Embora essa alternativa pudesse proporcionar maior autonomia institucional e possibilidade de customização da solução, verificou-se que o desenvolvimento de plataforma própria de cibersegurança envolve elevado grau de complexidade técnica, exigindo competências especializadas em áreas como:

- engenharia de segurança da informação;
- monitoramento de eventos de segurança (SIEM);
- detecção e resposta a incidentes (EDR/XDR);
- inteligência de ameaças cibernéticas;
- proteção de ambientes virtualizados e em nuvem.

Além disso, o desenvolvimento e manutenção de solução própria demandariam investimentos significativos em infraestrutura tecnológica e recursos humanos especializados, bem como atualização permanente da plataforma para acompanhar a evolução das ameaças cibernéticas.

Outro fator relevante refere-se ao **tempo necessário para desenvolvimento, testes e implantação da solução**, o que poderia comprometer a capacidade institucional de responder de forma tempestiva aos riscos associados à segurança da informação.

Diante desses fatores, concluiu-se que essa alternativa apresenta **elevado risco operacional e baixa relação custo-benefício**, sendo considerada inviável no contexto da presente contratação.

Após análise das alternativas avaliadas, verificou-se que as soluções descritas neste capítulo não apresentam viabilidade técnica, operacional ou econômica para atendimento das necessidades institucionais do **ITEC – Instituto de Tecnologia em Informática e Informação**.

Diante disso, optou-se pela adoção de solução baseada na **contratação de plataforma integrada de cibersegurança associada à prestação de serviços especializados**, modelo que se mostrou mais adequado para garantir proteção efetiva dos ativos digitais institucionais, atualização tecnológica contínua e maior eficiência na gestão da segurança da informação.

11. Análise comparativa de custos (TCO)

Conforme exigido pelo art. 11, inciso III, da Instrução Normativa SGD/ME nº 94/2022, procedeu-se à comparação dos custos totais de propriedade (Total Cost of Ownership — TCO) para as soluções tecnicamente viáveis identificadas neste Estudo Técnico Preliminar.

Das três alternativas analisadas no Capítulo 3, apenas a Solução 3 — Contratação de Solução Integrada com Serviços Especializados — foi considerada tecnicamente viável para atendimento das necessidades institucionais, conforme demonstrado na análise comparativa dos Capítulos 3.8 e 3.13. As demais alternativas (Solução 1 e Solução 2) foram registradas como inviáveis no Capítulo 4, razão pela qual não integram a análise de TCO.

Metodologia de cálculo

O TCO da solução viável foi calculado considerando os seguintes componentes de custo ao longo de 12 (doze) meses, prazo de vigência inicial do contrato:

a) custos diretos de licenciamento e fornecimento;

b) custos de serviços continuados (valor mensal × 12 meses);

c) custos de implantação, integração e treinamento (horas técnicas);

d) custos administrativos e de fiscalização estimados (pessoal interno dedicado à gestão contratual).

Item	Especificação	CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unit Mensal/ Unidade	Media	Valor Estimado	Órgão	Links de acesso
1	Plataforma Unificada de Cibersegurança (Core)	27502	Licença Anual/ Ativo	1.430	R$ 1.132,02 R$ 1.937,50	R$ 1.534,76	R$ 2.194.704,77	170607 - CENTRO DE SERVIÇOS COMPARTILHADOS 171510 - MUNICÍPIO DE BENTO GONÇALVES	https://pncp.gov.br/app/editais/00489828000155/2025/475 https://pncp.gov.br/app/editais/87849923000109/2026/29
2	Inteligência e Proteção de Marca (OSINT/EASM)	27502	Assinatura Anual (Por Dominio e e-mail)	17.499	R$ 1.942,44 R$ 1.250,00	R$ 1.596,22	R$ 27.932.253,78	MUNICIPIO DE MANGARATIBA MUNICIPIO DE CONTENDA	https://pncp.gov.br/app/editais/29138310000159/2026/31 https://pncp.gov.br/app/editais/76105519000104/2025/142
3	Proteção de Endpoint (EDR/ XDR)	27502	Licença Anual/ Endpoint	1.430	R$ 573,81	R$ 573,81	R$ 820.553,07	TRIBUNAL DE CONTAS DO ESTADO PARA	https://pncp.gov.br/app/editais/04976700000177/2024/95
4	Segurança de Web e Containers (CS/KSPM)	27502	Licença Anual/ Node	11	R$ 50.848,56 R$ 27.642,72	R$ 39.245,64	R$ 431.702,04	SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTAO MUNICIPIO DE MANGARATIBA	https://pncp.gov.br/app/editais/05461142000170/2026/7 https://pncp.gov.br/app/editais/29138310000159/2026/31
5	Chaves de Hardware (FIDO 2)	6682	Unidade	38	R$ 639,99 R$ 755,22	R$ 697,61	R$ 26.508,99	TRIBUNAL SUPERIOR DO TRABALHO MINISTERIO DA FAZENDA	https://pncp.gov.br/app/editais/00509968000148/2025/4625 https://pncp.gov.br/app/editais/00394460000141/2024/2109
6	Operação de Segurança (SOC) e Suporte 24x7	26999	Mês	12	R$ 2.578,71 R$ 1.250,00	R$ 1.914,36	R$ 22.972,26	MUNICIPIO DE BENTO GONCALVES MUNICIPIO DE BRUSQUE	https://pregaobanrisul.com.br/editais/0001_2026/lote/1546798 https://pncp.gov.br/app/editais/83102343000194/2025/22
7	Implantação, Integração e Treinamento	3840	Hora Técnica	600	R$ 800,00 R$ 1.297,00	R$ 1.048,50	R$ 629.100,00	FUNDACAO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL GENCIA NACIONAL DE ENERGIA ELETRICA - ANEEL	https://pncp.gov.br/app/editais/15461510000133/2025/21 https://pncp.gov.br/app/editais/02270669000129/2025/71
8	Gestão de Vulnerabilidades e Apoio à Remediação	27014	Mês	12	R$ 1.290.028,61 R$ 972.933,46	R$ 1.131.481,04	R$ 13.577.772,42	FUNDACAO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL GENCIA NACIONAL DE ENERGIA ELETRICA - ANEEL	https://pncp.gov.br/app/editais/15461510000133/2025/21 https://pncp.gov.br/app/editais/02270669000129/2025/71
9	Controle de Acesso à Rede (NAC)	27502	Licença Anual/ Disp.	2.250	5.643,00 4641,84	R$ 5.142,42	R$ 11.570.445,00	SECRETARIA DE ESTADO DA SAUDE TRIBUNAL SUPERIOR ELEITORAL	https://pncp.gov.br/app/editais/27080605000196/2025/878 https://pncp.gov.br/app/editais/00509018000113/2024/4149
						Total	R$ 57.206.012,33		

Fontes das estimativas de preço: pesquisa de preços realizada em conformidade com a Instrução Normativa SEGES/ME nº 65/2021, com base em contratações similares através de busca no PNCP, conforme documentação anexa ao processo de contratação.

Conclusão

Com base nos dados acima, conclui-se que a Solução 3 representa o menor TCO tecnicamente viável para a Administração, pois elimina a necessidade de investimento em infraestrutura própria, incorpora a atualização tecnológica contínua no custo do serviço e dispensa a manutenção de equipe interna altamente especializada.

12. Descrição da solução de TIC a ser contratada

A solução de TIC consiste na prestação de serviços continuados de Segurança Cibernética Gerenciada, estruturada por meio de uma plataforma unificada de Defesa Ativa, Visibilidade e Segurança Ofensiva. A solução integra, em um ecossistema coeso, tecnologias de proteção de endpoints (EDR/XDR), gerenciamento de vulnerabilidades, inteligência de ameaças externas (OSINT/Dark Web) e controle de acesso a rede (Zero Trust), visando garantir a resiliência da infraestrutura tecnológica, a detecção preditiva de vetores de ataque, a contenção automatizada de incidentes e a proteção de dados críticos. O ciclo de vida do objeto abrange desde o licenciamento de software na modalidade Software as a Service (SaaS), a implantação técnica e a parametrização em ambientes legados, até a operação assistida por um Centro de Operações de Segurança (SOC) especializado 24x7 e o suporte contínuo à remediação de falhas.

Plataforma Unificada de Gestão e Governança (Core)

A plataforma atua como o eixo central de gerenciamento, consolidando dados telemétricos provenientes de todas as camadas defensivas da organização, endpoints, nuvem e contêineres. Sua finalidade é prover uma visão holística e unificada do risco cibernético organizacional por meio de um Risk Score dinâmico, facilitando a governança e o atendimento aos requisitos de auditoria e conformidade. O sistema consolida a gestão de ativos e permite a orquestração de respostas a incidentes (SOAR) e a guarda de evidências com integridade baseada em Blockchain, conferindo validade técnica e jurídica aos relatórios gerados, em conformidade com o Art. 369 do Código de Processo Civil.

Inteligência, Defesa Ativa e Segurança Ofensiva

O ciclo de vida da solução prevê, ainda, uma camada de inteligência e validação contínua, a proteção contra ameaças externas e o monitoramento da Dark Web (OSINT) estendem o perímetro de segurança para além da rede física, enquanto a segurança de contêineres garante que a modernização tecnológica não abra novas brechas em ambientes de nuvem. O controle de acesso (NAC) atua na borda física e lógica, aplicando os princípios Zero Trust para restringir o acesso a dispositivos IoT e visitantes, enquanto as chaves de hardware (FIDO2) elevam a segurança da identidade corporativa, eliminando o risco de phishing nos acessos administrativos. A segurança ofensiva (Pentest automatizado e DDoS) promove o teste de estresse contínuo da resiliência dos serviços, permitindo que a organização corrija falhas antes da exploração por agentes maliciosos.

Gestão do Ciclo de Vida da Vulnerabilidade e Resposta (SOC/Blue Team)

A solução compreende a operação humana integrada, garantindo que a tecnologia contratada seja operada por especialistas de segurança, o serviço de SOC realiza o monitoramento ininterrupto e a triagem de alertas, enquanto o serviço de gestão de vulnerabilidades atua no lifecycle preventivo (análise, priorização e apoio técnico à correção). Esta abordagem garante que a organização não apenas detete uma vulnerabilidade ou invasão, mas possua a capacidade técnica para operacionalizar o patching, a mitigação de riscos e a validação posterior do ambiente (Rescan), fechando o ciclo de detecção-resposta-correção.

Implantação, Integração e Capacitação

Para assegurar a sustentabilidade da contratação, o ciclo de vida do objeto contempla serviços especializados de implantação e transferência de conhecimento, esta fase garante a integração técnica com o legado tecnológico da contratante, assegurando que sistemas operacionais obsoletos e infraestruturas críticas não percam visibilidade ou segurança durante a adoção da nova plataforma. O treinamento oficial certificado, integrado ao suporte técnico continuado, capacita a equipe da instituição na operação das ferramentas de defesa, na escrita de playbooks de automação e na governança da privacidade de dados, assegurando a independência do órgão na gestão do ecossistema de segurança cibernética a longo prazo.

Normativos aplicáveis ao objeto

A presente contratação observa o conjunto de normas legais, regulamentares e orientações técnicas que disciplinam a gestão pública, as contratações administrativas e a governança de tecnologia da informação no âmbito da Administração Pública.

A identificação desses normativos tem como objetivo assegurar que a solução a ser contratada esteja em conformidade com os princípios da legalidade, eficiência, economicidade e transparência, além de garantir aderência às boas práticas de segurança da informação e proteção de dados.

Nesse contexto, destacam-se os seguintes normativos aplicáveis ao objeto da contratação.

Legislação de contratações públicas

A contratação será conduzida em conformidade com a **Lei nº 14.133/2021**, que estabelece normas gerais de licitação e contratação para a Administração Pública, definindo princípios, procedimentos e instrumentos destinados a assegurar a seleção da proposta mais vantajosa para a Administração.

Essa legislação estabelece diretrizes para o planejamento das contratações públicas, incluindo a obrigatoriedade da elaboração de estudos técnicos preliminares, análise de riscos, definição de requisitos e justificativa da solução escolhida, bem como mecanismos de governança e gestão contratual.

Normas de contratação de soluções de TIC

No que se refere especificamente à contratação de soluções de Tecnologia da Informação e Comunicação (TIC), o presente processo observa as diretrizes estabelecidas pela **Instrução Normativa SGD/ME nº 94/2022**, que dispõe sobre o processo de contratação de soluções de TIC no âmbito da Administração Pública Federal, estabelecendo diretrizes para o planejamento, seleção de fornecedores, gestão contratual e avaliação de desempenho das soluções tecnológicas contratadas.

Essas normas reforçam a necessidade de planejamento adequado das contratações de TIC, priorizando a seleção de soluções tecnológicas capazes de gerar resultados mensuráveis e assegurar maior eficiência na gestão dos recursos públicos.

Normas de proteção de dados pessoais

Considerando que a solução a ser contratada envolve o tratamento e a proteção de dados institucionais e possivelmente dados pessoais, a contratação deve observar as disposições da **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Essa legislação estabelece princípios e regras para o tratamento de dados pessoais, aplicáveis tanto a órgãos públicos quanto a entidades privadas, incluindo diretrizes relacionadas à segurança da informação, governança de dados e proteção da privacidade.

Nesse contexto, a solução tecnológica deverá contemplar mecanismos que contribuam para a proteção dos dados sob responsabilidade institucional, reduzindo riscos de vazamentos, acessos não autorizados ou incidentes de segurança da informação.

Política Nacional de Segurança da Informação

A gestão da segurança da informação na Administração Pública também observa as diretrizes estabelecidas pelo **Decreto nº 9.637/2018**, que institui a Política Nacional de Segurança da Informação.

Esse normativo estabelece princípios, objetivos e instrumentos voltados à proteção das informações estratégicas do Estado brasileiro, bem como à promoção de práticas de segurança da informação nas instituições públicas.

Entre suas diretrizes destacam-se a gestão de riscos, a proteção de ativos de informação e o fortalecimento das capacidades institucionais de prevenção e resposta a incidentes de segurança.

Política Nacional de Cibersegurança

A contratação também se fundamenta nas diretrizes estabelecidas pelo **Decreto nº 11.856/2023**, que institui a **Política Nacional de Cibersegurança (PNCiber)**.

Esse decreto estabelece princípios, objetivos e diretrizes voltados ao fortalecimento da segurança cibernética no país, promovendo a proteção das infraestruturas digitais e a mitigação de riscos associados a ameaças cibernéticas.

Entre seus principais objetivos destacam-se:

- fortalecer a capacidade nacional de prevenção, detecção e resposta a incidentes cibernéticos;
- promover a proteção de infraestruturas críticas de informação;
- incentivar a adoção de boas práticas de segurança cibernética no setor público;
- ampliar a resiliência dos sistemas digitais utilizados pela Administração Pública.

Nesse contexto, a adoção de soluções tecnológicas voltadas ao monitoramento de segurança, gestão de vulnerabilidades e resposta a incidentes cibernéticos está diretamente alinhada às diretrizes estabelecidas por essa política pública.

Governança da Política Nacional de Cibersegurança

Complementarmente, a governança e a coordenação da Política Nacional de Cibersegurança foram regulamentadas pelo **Decreto nº 12.573/2024**, que estabelece mecanismos institucionais voltados à implementação e ao acompanhamento das ações de segurança cibernética no país.

Esse normativo reforça a necessidade de fortalecimento das estruturas institucionais de segurança digital, incentivando a adoção de mecanismos de proteção tecnológica, monitoramento de riscos cibernéticos e desenvolvimento de capacidades organizacionais voltadas à gestão da segurança da informação.

Normativos institucionais e estaduais

No âmbito institucional e da administração pública estadual, a contratação também observa as diretrizes estabelecidas pelos **Decretos Estaduais nº 103.660 e nº 103.659**, que tratam da organização institucional e das competências relacionadas à gestão de tecnologia da informação, governança digital e segurança da informação no âmbito do Estado de Alagoas.

Esses normativos estabelecem diretrizes para a modernização da gestão pública por meio da transformação digital, fortalecendo o papel do **ITEC – Instituto de Tecnologia em Informática e Informação** na coordenação, implementação e gestão das soluções tecnológicas utilizadas pela Administração Pública Estadual.

Nesse contexto, a adoção de soluções estruturadas de segurança da informação e cibersegurança contribui diretamente para o cumprimento das competências institucionais atribuídas ao Instituto e para o fortalecimento da infraestrutura digital do Estado.

Normas e boas práticas internacionais

Além dos normativos legais e regulamentares aplicáveis, a solução deverá observar boas práticas amplamente reconhecidas na área de segurança da informação e governança de tecnologia da informação, incluindo referenciais como:

- **ISO/IEC 27001** – Sistema de Gestão de Segurança da Informação;
- **ISO/IEC 27002** – Código de boas práticas para controles de segurança da informação;
- **NIST Cybersecurity Framework** – Estrutura de referência para gestão de riscos cibernéticos;
- **COBIT** – Estrutura de governança e gestão de tecnologia da informação;

ITIL – Conjunto de boas práticas para gestão de serviços de tecnologia da informação.

Requisitos do objeto

Código CATSER (descrição e unidade de medida)

Item	Especificação	CATSER /CATMAT	Métrica ou Unidade de Medida
1	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Plataforma Unificada de Cibersegurança (Core)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual/Ativo
2	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Inteligência e Proteção de Marca (OSINT/EASM)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Assinatura Anual (Por Dominio e e-mail)
3	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Proteção de Endpoint (EDR/XDR)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual/Endpoint
	Descrição CATSER:		**Unidade de medida CATSER:**

4	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Segurança de Web e Containers (CS/KSPM)	27502	Unidade **Unidade de Medida complementar:** Licença Anual/Node
5	**Descrição CATMAT:** Módulo Eletrônico Tipo: Token Modelo: Chip Criptográfico Uso: Usb Aplicação: Armazenamento De Certificado Digital Características Adicionais: Homologado Para Chaves: Tipo Rsa 2048 Bits; Certif **Descrição complementar:** Chaves de Hardware (FIDO2)	485464	**Unidade de medida CATMAT:** Unidade
6	**Descrição CATSER:** Serviços de Gerenciamento de Redes de Tecnologia da Informação e Comunicação (TIC) **Descrição complementar:** Operação de Segurança (SOC) e Suporte 24x7	26999	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Mês
7	**Descrição CATSER:** Treinamento Informática - Sistema / Software **Descrição complementar:** Implantação, Integração e Treinamento	3840	**Unidade de medida CATSER:** Hora **Unidade de Medida complementar:** Hora Técnica
8	**Descrição CATSER:** Serviços de Gerenciamento de Infraestrutura de Tecnologia da Informação e Comunicação (TIC) **Descrição complementar:** Gestão de Vulnerabilidades e Apoio à Remediação	27014	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Mês
9	**Descrição CATSER:** Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software **Descrição complementar:** Controle de Acesso à Rede (NAC)	27502	**Unidade de medida CATSER:** Unidade **Unidade de Medida complementar:** Licença Anual/Disp.

Justificativa da descrição e unidade de medida complementar

Considerando a insuficiência da Descrição ou Unidade de Medida dos códigos CATSER utilizados, há necessidade da exigência das seguintes especificações técnicas complementares, que, compatíveis com a Descrição ou Unidade de Medida dos códigos CATSER utilizados, não apresentam divergência ou dissociação:

Em relação aos itens de Software (CATSER 27502)

Descrição Complementar: Plataforma Core, OSINT/EASM, EDR/XDR, CS/KSPM e NAC.

Unidade de Medida Complementar: Ativo, Domínio/E-mail, Node e Dispositivo.

O código 27502 refere-se genericamente a "Locação de Software". Contudo, a segurança da informação exige ferramentas com finalidades distintas e tecnicamente divergentes (proteção de endpoint vs. inteligência de marca). A especificação complementar é indispensável para definir o escopo de proteção e a volumetria da licença, uma vez que a precificação de mercado varia drasticamente conforme o objeto protegido (um "Node" de container possui complexidade e custo distintos de um "Dispositivo" de rede).

Em relação ao item de Hardware (CATMAT 485464)

Descrição Complementar: Chaves de Hardware (FIDO2).

O código 485464 abrange qualquer "Módulo Eletrônico". A especificação do padrão FIDO2 é essencial para garantir a interoperabilidade com sistemas modernos de autenticação sem senha (passwordless) e atender aos requisitos de MFA (Autenticação de Múltiplos Fatores) de alta segurança, impedindo a aquisição de hardware obsoleto ou proprietário.

Em relação aos itens de Serviços Gerenciados (CATSER 26999 e 27014)

Descrição Complementar: Operação de Segurança (SOC) 24x7 e Gestão de Vulnerabilidades.

Os códigos de gerenciamento de TIC são amplos. A descrição complementar assegura que o serviço contratado inclua o monitoramento contínuo (24x7), crítico para a resiliência contra ataques cibernéticos que ocorrem fora do horário comercial, e a proatividade na remediação de falhas, diferenciando o suporte técnico comum da inteligência de defesa cibernética.

Em relação ao Treinamento e Implantação (CATSER 3840)

Descrição Complementar: Implantação, Integração e Treinamento.

Unidade de Medida Complementar: Hora Técnica.

O CATSER 3840 foca estritamente no treinamento. A inclusão da "Implantação e Integração" como descrição complementar justifica-se pela necessidade de que o software seja configurado e integrado ao ecossistema de TI existente por profissionais certificados, garantindo que as licenças adquiridas sejam plenamente operacionais desde o primeiro dia de vigência.

Natureza do objeto

De engenharia

Com base nas disposições tanto da Lei Federal nº 5.194, de 1966, quanto da Lei Federal nº 6.496, de 1977, além das Resoluções do Conselho Federal de Engenharia e Agronomia (CONFEA), inclusive Resolução CONFEA nº 218, de 1973, o objeto da contratação não consiste em serviço de engenharia.

Comum

O objeto da contratação é comum, visto poderem seus padrões de desempenho e qualidade ser objetivamente definidos por meio de especificações usuais no mercado.

Execução continuada

O objeto da contratação consiste na prestação de serviços especializados de cibersegurança e proteção do ambiente tecnológico institucional, incluindo monitoramento contínuo de eventos de segurança, gestão de vulnerabilidades, resposta a incidentes cibernéticos e suporte técnico especializado. Trata-se de atividade que deve ser executada de forma **continuada e ininterrupta**, considerando a natureza permanente das operações tecnológicas realizadas pelo **ITEC – Instituto de Tecnologia em Informática e Informação**.

A execução continuada do serviço justifica-se pelos seguintes aspectos:

Habitualidade

A habitualidade do serviço decorre do fato de que as atividades relacionadas à segurança da informação e à proteção da infraestrutura digital institucional são realizadas de forma permanente e contínua no ambiente tecnológico do Instituto.

Os sistemas corporativos, plataformas digitais, serviços de rede e demais recursos tecnológicos utilizados pela Administração Pública operam continuamente para viabilizar a execução das atividades administrativas e a prestação de serviços digitais aos órgãos e entidades atendidos pelo ITEC.

Nesse contexto, o monitoramento da segurança do ambiente tecnológico, a identificação de vulnerabilidades, a análise de eventos de segurança e a mitigação de riscos cibernéticos constituem atividades permanentes e inerentes à gestão da infraestrutura de tecnologia da informação.

Considerando que as ameaças cibernéticas se manifestam de forma constante e evolutiva, a adoção de mecanismos de monitoramento e proteção deve ocorrer de forma contínua, não sendo suficiente a realização de ações pontuais ou eventuais de segurança da informação.

Dessa forma, a prestação do serviço de segurança cibernética deve ocorrer de maneira permanente, acompanhando o funcionamento ininterrupto dos sistemas e serviços digitais mantidos pelo Instituto.

Essencialidade

A essencialidade do serviço decorre da importância estratégica da segurança da informação para a proteção dos ativos digitais institucionais e para a continuidade das atividades administrativas suportadas pela infraestrutura tecnológica do ITEC.

A paralisação ou interrupção dos serviços de monitoramento de segurança e gestão de vulnerabilidades poderia comprometer significativamente a capacidade institucional de identificar e responder a incidentes cibernéticos, aumentando o risco de ocorrência de eventos como:

- ataques cibernéticos;
- vazamento de dados institucionais ou pessoais;
- comprometimento da integridade dos sistemas corporativos;
- indisponibilidade de serviços digitais utilizados pela Administração Pública.

Além disso, a ausência de monitoramento contínuo do ambiente tecnológico pode dificultar a detecção tempestiva de vulnerabilidades e ameaças, expondo os sistemas institucionais a riscos operacionais, legais e reputacionais.

Nesse sentido, a prestação continuada dos serviços de cibersegurança é fundamental para assegurar a proteção da infraestrutura digital institucional, garantir a continuidade dos serviços tecnológicos e preservar a integridade, confidencialidade e disponibilidade das informações sob responsabilidade do Instituto.

Diante disso, conclui-se que os serviços objeto da presente contratação possuem **natureza continuada**, uma vez que atendem necessidades permanentes da Administração Pública e são essenciais para o funcionamento regular das atividades institucionais e para a segurança do ambiente tecnológico.

Regime de dedicação exclusiva de mão de obra

Considerando os requisitos exigidos para a execução contratual, o objeto da contratação não consiste em serviço com regime de dedicação exclusiva de mão de obra (MDO). A solução contratada baseia-se na prestação de resultados mensuráveis, aferidos por Acordos de Nível de Serviço (ANS) e Instrumento de Medição de Resultado (IMR), com os profissionais da Contratada operando de forma remota e sem exclusividade de dedicação às dependências da Contratante, ressalvadas as atividades presenciais previstas no Plano de Implantação e nas Ordens de Serviço específicas.

Regime de execução do serviço

O regime de execução contratual será de **Execução Indireta**, sob o regime de Empreitada por Preço Unitário, conforme o art. 6º, inciso XXI, alínea "c", da Lei nº 14.133/2021, dada a natureza de prestação de serviços continuados de TI, onde o pagamento será aferido pela efetiva disponibilidade da plataforma e dos serviços gerenciados, conforme os indicadores definidos no IMR.

Prazo de vigência

A contratação do serviço continuado terá prazo de vigência inicial de 12 (doze) meses, contados a partir da data de sua assinatura, podendo ser prorrogada por períodos sucessivos até o limite de 120 (cento e vinte) meses, conforme o art. 108 da Lei nº 14.133/2021, mediante comprovação de vantagem e desempenho satisfatório.

Qualificação econômico-financeira

De acordo com a área do objeto da contratação e o porte das empresas que nela atuam, considerando a existência de maior risco para a Administração, em função da complexidade e do vulto da contratação, há necessidade da exigência de patrimônio líquido mínimo para habilitação.

O percentual de patrimônio líquido mínimo exigido será de 10% (dez por cento) do valor estimado da contratação, proporcional aos riscos que a inexecução total ou parcial do contrato pode acarretar para a Administração, consideradas, entre outros fatores, as particularidades e a essencialidade do objeto da contratação.

Capacidade técnico-operacional

Para fins de qualificação técnico-operacional, a licitante deverá comprovar aptidão para o desempenho de atividade pertinente e compatível com o objeto da contratação, mediante apresentação de atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprovem:

— Características: prestação de serviços de segurança cibernética gerenciada envolvendo, cumulativamente, monitoramento contínuo de eventos de segurança (SOC), gestão de vulnerabilidades e proteção de endpoints (EDR/XDR) em ambientes corporativos com infraestrutura híbrida (física e virtualizada);

— Quantidades: cobertura mínima de 35% (trinta e cinco por cento) do quantitativo contratado de 1.430 licenças, garantindo a proporcionalidade sem restringir indevidamente a competitividade;

A exigência de prestação de serviços envolvendo simultaneamente SOC e EDR justifica-se pela integração funcional entre esses componentes no objeto licitado: a operação do SOC sem visibilidade de endpoint (EDR) não demonstra capacidade equivalente ao objeto; da mesma forma, o licenciamento isolado de EDR sem a operação do SOC não comprova a aptidão para o serviço continuado exigido.

Capacidade técnico-profissional

Considerando a necessidade de qualificação profissional específica dos profissionais responsáveis pela execução do objeto da contratação, definem-se suas parcelas de maior relevância e valor significativo, para efeito de anotação ou registro de responsabilidade técnica.

A licitante deverá comprovar possuir em seu quadro permanente (ou mediante contrato de prestação de serviços/compromisso de contratação futura), profissionais de nível superior, detentores das certificações internacionais abaixo elencadas. Estes profissionais serão considerados "Equipe-Chave" e sua alocação, bem como eventuais substituições, deverão ser submetidas à prévia aprovação da Contratante.

Perfil técnico	Denominação	Certificações de referência (mínimo 1 por perfil)
Perfil 1	Analista de Segurança Cibernética (SOC)	CompTIA Security+; CySA+ ou GSEC
Perfil 2	Gerente de Projetos (Implantação)	PMP ou CSM (Scrum Master)
Perfil 3	Analista de SOC Nível 3 (DFIR)	CompTIA CySA+; ECSA ou GCIH
Perfil 4	Especialista em Gestão de Vulnerabilidades	ISO 27001 Foundation; CompTIA Security+ ou GPEN
Perfil 5	Especialista em Testes de Intrusão (Red Team)	OSCP; CEH Practical ou eJPT
Perfil 6	Arquiteto de Soluções de Segurança	CISSP; AWS Certified Security – Specialty ou Azure Security Engineer

Os serviços técnicos especializados deverão ser prestados por profissionais devidamente qualificados e certificados, garantindo a excelência na execução das atividades de privacidade, segurança ofensiva, SOC e gestão de projetos. A Contratada deverá comprovar a disponibilidade da equipe técnica conforme os perfis abaixo, sendo que a apresentação destas comprovações é condição obrigatória para a Qualificação Técnica da licitante.

Perfil 1: Analista de Segurança Cibernética (Residente/SOC)

Atribuição: Operação do SOC, triagem de incidentes, análise de logs e uso da Plataforma (Item 01).

Formação: Curso superior completo em TIC ou Engenharia.

Certificação Obrigatória (pelo menos uma): CompTIA Security+; CySA+ (Cybersecurity Analyst); ou GSEC (GIAC Security Essentials).

Perfil 2: Gerente de Projetos (Gestão de Implantação)

Atribuição: Gestão do cronograma, interface com a Contratante e condução do kick-off e aceite.

Formação: Curso superior completo em TI ou área correlata.

Certificação Obrigatória: PMP (Project Management Professional) ou certificação Scrum Master (CSM) se metodologia ágil for adotada.

Perfil 3: Analista de SOC Nível 3 (Investigação e DFIR)

Atribuição: Investigação de incidentes críticos, perícia digital (DFIR) e orquestração (SOAR).

Formação: Curso superior completo em TI.

Certificação Obrigatória (pelo menos uma): CompTIA CySA+; ECSA (EC-Council Certified Security Analyst); ou GCIH (GIAC Certified Incident Handler).

Perfil 4: Especialista em Gestão de Vulnerabilidades (Blue Team)

Atribuição: Análise de vulnerabilidades, curadoria de patches e gestão de obsolescência tecnológica.

Formação: Curso superior completo em TI ou área correlata.

Certificação Obrigatória (pelo menos uma): Information Security Foundation (ISO 27001); ou CompTIA Security+; ou GPEN (GIAC Penetration Tester).

Perfil 5: Especialista em Testes de Intrusão (Pentester/Red Team)

Atribuição: Execução de testes de intrusão, validação da resiliência dos sistemas (DDoS) e auditoria de segurança ofensiva.

Certificação Obrigatória (pelo menos uma): OSCP (Offensive Security Certified Professional); ou CEH (EC-Council Certified Ethical Hacker) versão Practical; ou eJPT (eLearnSecurity Junior Penetration Tester).

Perfil 6: Arquiteto de Soluções de Segurança (Integração e Hardening)

Atribuição: Setup técnico, integração de APIs, integração com AD/LDAP, hardening de sistemas e arquitetura em nuvem.

Formação: Curso superior completo em TI ou área correlata.

Certificação Obrigatória (pelo menos uma): CISSP (Certified Information Systems Security Professional); ou certificações avançadas de nuvem (AWS Certified Security – Specialty ou Azure Security Engineer Associate).

Instalações e aparelhamento

De acordo com o objeto da contratação, e em conformidade legal com o artigo 67, inciso III, há necessidade de que a Contratada apresente declaração formal da disponibilidade, no momento da execução contratual, das seguintes instalações e aparelhamento:

a) infraestrutura de datacenter ou ambiente de nuvem certificado (ISO 27001, SOC 2 Tipo II ou equivalente) onde a plataforma SaaS estará hospedada, com disponibilidade mínima de 99,8% ao mês;

b) Centro de Operações de Segurança (SOC) com operação 24x7x365, com capacidade de monitoramento simultâneo e equipe técnica disponível para atendimento de incidentes críticos no prazo estabelecido no item de requisitos temporais deste instrumento;

c) unidade administrativa ou técnica na Região Nordeste do Brasil, conforme condições estabelecidas neste instrumento.

A comprovação das condições acima será exigida na fase de habilitação técnica, por meio de declaração do fabricante ou prestador de serviços de nuvem, atestado de operação do SOC e documentação comprobatória da estrutura regional, nos termos do item de demais requisitos para a escolha da solução.

Justificativa Técnica da Necessidade e Essencialidade das Exigências

A exigência dos requisitos de instalações e aparelhamento acima descritos fundamenta-se na natureza estratégica e na alta criticidade do objeto, sendo indispensável para assegurar a execução contratual sem riscos à continuidade dos serviços públicos estaduais.

1. Da Certificação da Infraestrutura (Datacenter/Nuvem): A exigência de certificações como ISO 27001 e SOC 2 não configura restrição à competitividade, mas sim uma salvaguarda mínima de conformidade com o Art. 46 da LGPD. Uma vez que a plataforma processará dados telemétricos, logs de servidores críticos e inventário de vulnerabilidades do Estado, a ausência de controles auditados de segurança física e lógica no datacenter do fornecedor representaria um risco inaceitável de vazamento de informações sensíveis e comprometimento da soberania de dados da Administração Pública.

2. Da Operacionalidade do SOC 24x7: O cenário atual de ameaças cibernéticas, notadamente ataques de Ransomware e Exfiltração de Dados, demonstra que incidentes ocorrem majoritariamente fora do horário comercial. A exigência de uma estrutura de SOC 24x7x365 é um requisito de prontidão operacional. Sem o aparelhamento humano e tecnológico capaz de reagir em minutos a uma anomalia detectada pelo EDR ou pelo NAC, o investimento em licenças de software tornar-se-ia inócuo, pois a tecnologia isolada, sem monitoramento especializado, não é capaz de conter proativamente o avanço de um invasor na rede estadual.

3. Da Presença Regional (Região Nordeste): A exigência de estrutura na Região Nordeste justifica-se pelo Princípio da Eficiência e pela Prontidão Logística. A solução contratada envolve componentes físicos (Item 05 - Chaves FIDO2) e suporte à implantação e remediação (Blue Team) que podem demandar intervenções presenciais em cenários de falhas críticas de conectividade ou substituição urgente de hardware. A proximidade geográfica reduz drasticamente o Tempo Médio de Resposta (MTTR) e facilita a governança contratual, permitindo reuniões técnicas de alinhamento e auditorias de conformidade in loco sem os custos e a latência de deslocamentos interestaduais complexos. Tal exigência encontra amparo na jurisprudência do Tribunal de Contas da União, que admite requisitos de estrutura logística quando estes são essenciais para a garantia da execução e agilidade do atendimento técnico.

Desta forma, os requisitos de instalações e aparelhamento aqui estipulados são necessários, suficientes e proporcionais ao vulto da contratação, visando exclusivamente a mitigação de riscos operacionais e a proteção da infraestrutura digital que sustenta os serviços essenciais ao cidadão alagoano.

Obrigações da contratada

De acordo com o objeto da contratação, não há necessidade da exigência de obrigações específicas da contratada, sendo adequadas e suficientes aquelas previstas na minuta padronizada pela PGE/AL.

Classificação Brasileira de Ocupações (CBO)

De acordo com o objeto da contratação, as categorias profissionais que serão empregadas na execução do serviço enquadram-se na Classificação Brasileira de Ocupações (CBO) da seguinte forma:

Perfil	**Denominação CBO**	**Código CBO**
Analista de Segurança Cibernética (SOC)	Analista de segurança da informação	2124-05
Gerente de Projetos	Gerente de projetos de tecnologia da informação	1425-10
Analista SOC N3 / DFIR	Analista de segurança da informação	2124-05
Especialista em Vulnerabilidades	Analista de segurança da informação	2124-05
Especialista em Testes de Intrusão	Analista de segurança da informação — Pentest	2124-05

Vistoria

A vistoria nas instalações do local de execução do serviço poderá ser realizada de segunda a sexta-feira, das 08 horas às 18 horas.

De acordo com o objeto da contratação, não há necessidade da indicação de outras instruções específicas sobre a vistoria, sendo adequadas e suficientes aquelas previstas na minuta padronizada pela PGE/AL.

Deslocamentos e hospedagem

De acordo com o objeto da contratação, não há necessidade de deslocamentos e hospedagem dos profissionais que serão empregadas na execução do serviço.

Uniformes, materiais e equipamentos

De acordo com o objeto da contratação, não há necessidade de indicar uniformes, materiais e equipamentos específico a serem disponibilizados em favor da Administração.

Participação de cooperativa

De acordo com o objeto da contratação e considerado o modo como é usualmente executado no mercado em geral, não será aceita cooperativa para a sua prestação, tendo em vista a necessidade de subordinação jurídica entre os profissionais e a empresa contratada, a exigência de pessoalidade na alocação da equipe técnica especializada (perfis certificados individualizados, conforme capítulo 7.44) e a habitualidade do serviço, características que são incompatíveis com a execução por cooperados em regime de autonomia ou rodízio.

Modelo de execução do objeto

A execução do objeto da contratação seguirá a seguinte dinâmica:

Condições de execução

A execução do objeto seguirá a metodologia de Gestão Continuada de Segurança, fundamentada no ciclo PDCA (Plan-Do-Check-Act), assegurando que as tecnologias, os processos e a equipe técnica da Contratada operem em alinhamento constante com a realidade da infraestrutura da Contratante.

O início dos serviços dar-se-á em até 15 (quinze) dias corridos contados da assinatura do contrato, com a realização imediata da Reunião de Kick-off e a formalização do Plano de Implantação.

Etapas de Execução:

Etapa I (Diagnóstico e Setup): Realização do Assessment da superfície de ataque, provisionamento do tenant SaaS, integração com sistemas legados, Active Directory e firewalls existentes.

Etapa II (Implantação e Hardening): Instalação dos agentes (EDR/XDR), configuração dos sensores de rede e validação das políticas de segurança nos contêineres e ativos.

Etapa III (Operação Assistida e Treinamento): Realização de workshops práticos, treinamento da equipe técnica e validação dos Playbooks de resposta automatizada (SOAR).

Etapa IV (Operação Continuada e Monitoramento): Início da vigência do SOC 24x7, gestão de vulnerabilidades, suporte à remediação (Blue Team) e testes de segurança ofensiva recorrentes.

Local e horário da prestação dos serviços

A Plataforma SaaS e o monitoramento centralizado (SOC) serão acessados remotamente pelos analistas da Contratada.

As atividades de consultoria, reunião de alinhamento e suporte presencial serão realizadas, quando necessário, no escritório regional da Contratada na Região Nordeste ou nas dependências da Contratante, conforme demanda formalizada em Ordem de Serviço (OS).

O suporte remoto estará disponível em regime 24x7x365 para incidentes críticos, e em horário comercial (08:00h às 18:00h) para solicitações administrativas e suporte evolutivo.

Rotinas a serem cumpridas

A Contratada deverá manter um Painel de Gestão de Incidentes atualizado, integrado ao ITSM da Contratante, onde constarão todas as demandas abertas e o status de remediação de cada vulnerabilidade mapeada.

Reuniões de gestão serão realizadas mensalmente para validação do nível de serviço (SLA), revisão da postura de risco e apresentação de novos riscos identificados pelo módulo de inteligência (OSINT/Dark Web).

Materiais a serem disponibilizados

Para a perfeita execução dos serviços, a Contratada fornecerá toda a infraestrutura lógica (plataforma SaaS, chaves de autenticação FIDO2, scripts de remediação e manuais técnicos) necessária para a execução do serviço. A Contratante fornecerá os acessos logísticos (rede/VPN) e os ativos para a instalação dos sensores de monitoramento

Formas de transferência de conhecimento

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

O processo de transferência de conhecimento ocorrerá durante toda a execução contratual, com ênfase nos primeiros 90 dias, visando a independência da equipe interna.

Ao final da vigência contratual (ou rescisão), a Contratada deverá apresentar um Relatório de Handover, contendo o estado atual do parque, as principais vulnerabilidades pendentes, o inventário de assets e o espelhamento de todas as configurações de playbooks e políticas de segurança para que a Contratante possa assumir a operação ou transferi-la a um novo parceiro.

Procedimentos de transição e finalização do contrato

Com antecedência mínima de 90 (noventa) dias do término da vigência contratual, ou em caso de rescisão antecipada, a Contratada deverá iniciar o Plano de Transição de Saída (Exit Strategy), visando a continuidade ininterrupta da segurança cibernética da Contratante.

Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

Entrega de toda a documentação técnica atualizada, incluindo topologias de rede, scripts de remediação, bibliotecas de Playbooks (SOAR) desenvolvidas, e manuais operacionais (runbooks).

A Contratada deverá exportar e entregar todos os logs, evidências forenses coletadas, relatórios, inventários de assets e políticas de segurança configuradas em formatos abertos e legíveis (JSON, CSV, PDF ou XML), garantindo a portabilidade integral da operação para a Contratante ou para um novo fornecedor.

Realização de sessões de transferência de conhecimento assistida com a equipe técnica da Contratante (ou do novo fornecedor), documentando o estado atual dos ativos, os riscos remanescentes, as pendências de patches e as configurações dos sensores de monitoramento.

Realização da desativação do serviço dos agentes (EDR/CWPP), revogação de acessos privilegiados (RBAC) e a exclusão definitiva dos dados da Contratante no ambiente da Contratada, mediante emissão de Certificado de Destruição e Sanitização de Dados.

Durante todo o período de transição de saída, a Contratada permanece integralmente responsável pela prestação do serviço, incluindo o monitoramento do SOC e a resposta a incidentes, não sendo permitida a degradação do nível de serviço (SLA) alegando o encerramento do contrato.

Quantidade mínima de serviços para comparação e controle

Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo.

Mecanismos formais de comunicação

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

I. Ordem de Serviço;
II. Ata de Reunião;
III. Ofício;
IV. Sistema de abertura de chamados;
V. E-mails e Cartas;

Em situações de emergência (vazamentos críticos ou ataques de Ransomware), será ativado o canal de comunicação direto entre o Plantão SOC da Contratada e o Gestor de Segurança da Contratante (linha dedicada/telefonia).

Manutenção de Sigilo e Normas de Segurança

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.

O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação.

Subcontratação

É permitida a subcontratação parcial do objeto desta licitação, até o limite de 25% (vinte e cinco por cento) do valor total do contrato, desde que a empresa subcontratada possua capacidade técnica e operacional compatível com a parcela que lhe será delegada, devendo tal condição ser previamente comunicada e autorizada pela Contratante.

É vedada a subcontratação da parcela principal do objeto, definida como o fornecimento da Plataforma Unificada de Cibersegurança (Item 01) e a gestão estratégica do contrato (Core Platform), uma vez que a responsabilidade pela integração sistêmica e pela unidade da solução (cockpit) deve ser de inteira responsabilidade da Contratada principal.

É vedada a subcontratação integral de qualquer dos itens obrigatórios desta contratação, sob pena de inexecução contratual.

Das Parcelas Passíveis de Subcontratação:

Poderão ser subcontratadas as seguintes atividades de apoio técnico especializado, desde que a Contratada comprove a qualificação técnica dos subcontratados:

Serviços de suporte técnico local ou auxílio à implantação física;

Execução de Testes de Intrusão (Pentest) especializados, caso a Contratada não possua Red Team interno próprio.

Em qualquer hipótese de subcontratação, permanece a responsabilidade integral e exclusiva da Contratada pela perfeita execução contratual. Caberá à Contratada realizar a supervisão, a coordenação e a garantia da qualidade das atividades dos subcontratados, respondendo perante a Contratante pelo rigoroso cumprimento das obrigações contratuais, inclusive quanto à confidencialidade e segurança dos dados.

A subcontratação depende de autorização prévia e formal da Contratante, a quem incumbe avaliar se o subcontratado preenche os requisitos de capacidade técnica necessários para a execução da parcela. A Contratada deverá apresentar a documentação que comprove a qualificação do subcontratado (currículos, certificações e histórico de serviços similares), que será submetida à avaliação da equipe de fiscalização e anexada aos autos do processo.

É vedada a subcontratação de pessoa física ou jurídica se esta mantiver vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização/gestão do contrato, bem como parentes até o terceiro grau.

Prazo de execução

O objeto da contratação terá prazo de execução contado, do efetivo recebimento da Ordem de Início de Serviços (OIS), até a expiração do prazo de vigência contratual e seguirá o seguinte cronograma físico-financeiro:

Etapa	**Descrição da Atividade / Marco (Evento)**	**Prazo (Dias Corridos)**
01	Kick-off, Plano de Implantação e Assessment	Até o 15º dia
02	Ativação SaaS (Core, EDR, OSINT) e Integração AD/Firewall	Até o 30º dia
03	Deploy Completo dos Agentes e Parametrização	Até o 45º dia
04	Treinamento Técnico e Operacional (Handover)	Até o 60º dia
05	Homologação da PoC de Resposta e Relatório Final	Até o 75º dia
06	Início da Operação SOC 24x7 e Gestão de Vuln.	A partir do 1º dia

Aceitação de consórcio

Será permitida a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei nº 14.133/2021, devendo ser observado:

a) apresentação de compromisso público ou particular de constituição de consórcio, subscrito pelas consorciadas;

b) indicação da empresa líder, responsável pela representação do consórcio perante a Administração;

c) apresentação, por cada consorciada, dos documentos de habilitação exigidos no edital;

d) responsabilidade solidária das empresas consorciadas pelos atos praticados durante a licitação e execução contratual;

e) vedação de participação de empresa consorciada, na mesma licitação, em mais de um consórcio ou isoladamente.

Modelo de gestão do contrato e critérios de medição e pagamento

MODELO DE GESTÃO DO CONTRATO

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.

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.

As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

O Contratado deverá enviar preposto da empresa no local da execução do objeto somente quando solicitado. A solicitação de comparecimento do preposto deve ocorrer com 03 (três) dias úteis de antecedência.

O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que o Contratado designará outro para o exercício da atividade.

Reunião Inicial

Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

A pauta desta reunião observará, pelo menos:

Presença do representante legal da contratada, que apresentará o seu preposto;

Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste ETP.

Rotinas de Fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

O fiscal técnico do contrato anotará 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.

Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

Verificação de Eficácia dos Controles de Detecção e Resposta (SOC/EDR):

Rotina: Inspeção mensal, via console da Plataforma (Item 01), da correlação de alertas entre o endpoint (EDR) e a inteligência de rede (Firewalls /NetFlow), validando se os alertas críticos estão sendo classificados conforme a matriz MITRE ATT&CK e se os tempos de resposta (MTTD/MTTR) estão dentro dos SLA's acordados.

Evidência: Relatório de Incident Response extraído do módulo de auditoria da plataforma, acompanhado da verificação dos logs de execução dos Playbooks de automação (SOAR).

Validação da Gestão de Vulnerabilidades e Remediação (Blue Team):

Rotina: Acompanhamento quinzenal do Action Plan de remediação. O fiscal técnico deverá auditar se as vulnerabilidades classificadas como "Críticas" e "Altas" foram objeto de rescan (varredura de validação) após a data prevista de correção, garantindo que o status de "corrigido" no inventário de ativos seja real e não apenas uma suposição.

Evidência: Relatório de análise diferencial (Delta Report) emitido pela plataforma, comparando o estado de vulnerabilidade dos ativos antes e depois da intervenção da equipe técnica.

Gestão de Identidade e Acesso (FIDO2 e RBAC):

Rotina: Verificação trimestral da lista de administradores com acesso à plataforma, conferindo se todos os perfis com privilégios elevados estão vinculados ao uso obrigatório de tokens físicos (FIDO2) e se a política de RBAC condiz com a estrutura atual da equipe técnica.

Evidência: Relatório de auditoria de identidade (Identity Audit Log) extraído do console central.

A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Fiscalização Administrativa

O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

Gestão e Conferência de Licenciamento Ativo:

Rotina: Acompanhamento mensal do inventário de licenças ativas na Plataforma Unificada (Itens 1, 3, 4 e 11) comparado ao quantitativo efetivo de ativos (IPs, Endpoints, Nodes de Container) monitorados pela solução. A fiscalização deverá verificar se o consumo está dentro do limite da faixa contratada (SRP) e se não há subdimensionamento que possa gerar downtime ou perda de visibilidade por falta de licença.

Evidência: Relatório de Asset Management extraído diretamente do console central, assinado pelo preposto da Contratada.

Verificação de Regularidade e Conformidade Trabalhista da Equipe Técnica:

Rotina: Verificação mensal da manutenção das condições de habilitação dos profissionais alocados (Perfis 1 a 6). A fiscalização administrativa exigirá a apresentação de comprovantes de vínculo empregatício ou contrato de prestação de serviços, além da manutenção das certificações técnicas (ex: CISSP, OSCP) que foram utilizadas para a qualificação técnica da empresa na licitação.

Evidência: Relatório mensal contendo a relação nominal dos profissionais, cópias das folhas de pagamento (ou comprovantes de recolhimento de encargos sociais) e comprovação de vigência das certificações profissionais. [...]; e

Controle de Estoque e Entrega de Materiais (Chaves FIDO2):

Rotina: Gestão do estoque físico dos tokens de segurança. A fiscalização conferirá o termo de entrega e o registro de carga dos dispositivos entregues aos usuários finais (servidores/administradores), mantendo controle patrimonial e verificando se os dispositivos distribuídos estão em conformidade com as especificações exigidas.

Evidência: Termo de Recebimento de Tokens FIDO2, assinado pelos usuários recebedores, e relatório de controle de estoque de segurança.

Acompanhamento Financeiro e Adimplemento de Obrigações (Diligência):

Rotina: Monitoramento da regularidade fiscal, trabalhista e previdenciária da Contratada, bem como a verificação da apresentação tempestiva da Nota Fiscal acompanhada do Relatório de Nível de Serviço (RNS). A fiscalização deverá glosar valores referentes a horas técnicas não executadas ou a módulos de licenciamento que apresentaram falhas graves de disponibilidade (SLA) no período.

Evidência: Relatório de Nível de Serviço (RNS), Certidões de Regularidade (SICAF/CNDs) e o espelho de medição da fatura mensal.

Gestão da Garantia e Logística Reversa:

Rotina: Controle administrativo sobre a troca de dispositivos (tokens) defeituosos sob garantia. A fiscalização deve certificar-se de que os tokens substituídos foram devidamente recolhidos pela Contratada para o processo de logística reversa e descarte ambientalmente correto.

Evidência: Termo de Substituição de Hardware e Comprovante de Destinação Final de Resíduos Eletroeletrônicos (Logística Reversa).

Gestor do Contrato

Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

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

emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

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 com competência para tal, conforme o caso.

elaborar 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.

enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

receber e dar encaminhamento imediato:

às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), que vincula a parcela do pagamento à qualidade e ao desempenho da solução contratada. O pagamento será realizado mensalmente, proporcionalmente aos itens efetivamente disponibilizados e aos níveis de serviço atingidos.

Quadro de Indicadores de Nível de Serviço (IMR):

A medição da qualidade dos serviços de SOC, Gestão de Vulnerabilidades e Sustentação da Plataforma seguirá os indicadores abaixo, cuja inobservância implicará em glosa proporcional no faturamento mensal:

Indicador	Descrição	Meta Aceitável	Glosa (% do Faturamento)
Disponibilidade (SaaS)	Uptime da Plataforma Core (Item 01)	≥ 99,8%	5% a 20% (conforme gravidade)
IAP (Tempo de Resposta)	Atendimento a chamados/incidentes (SOC)	≥ 95% dentro do prazo	2% a 10%
Qualidade da Remediação	Falhas críticas não remediadas após 30 dias	≤ 5% do total	5%
Conformidade (Inventário)	Ativos sem agente ou sem monitoramento	≤ 2% do total	2%

Indicador de Atraso na Entrega (IAE)

Finalidade	Medir o tempo de atraso na entrega dos produtos ou serviços constantes na Ordem de Serviço (OS).
Meta a cumprir	IAE <= 0 (A meta definida visa garantir a entrega dos produtos ou serviços constantes nas OS dentro do prazo previsto.)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS.
Periodicidade	Para cada OS encerrada
Instrumento de medição	OS e/ou Termo de Recebimento Provisório (TRP)
Mecanismo de cálculo (%)	**IAE = TEX - TEST** Onde: IAE - Indicador de Atraso na Entrega; TEX - Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos serviços da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeite a entrega, o prazo de execução da OS continua a correr, findando-se apenas quando a Contratada entregar os produtos da OS e haja aceitação por parte do fiscal técnico; TEST - Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência.
Início da vigência	A partir da emissão da OS
Sanções/faixas de ajuste	IAE <= 0: Pagamento integral da OS; IAE >= 1 e < 30: Aplicar-se-á glosa de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso; IAE >= 30: Aplicar-se-á glosa de 10% sobre o valor da OS ou fração em atraso acrescido de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso limitado em 30% sobre o valor da OS, bem como multa de 2% sobre o valor do contrato.

Observações	--

b) Indicador de Chamados atendidos dentro do Prazo (ICP)

Finalidade	Assegurar que os chamados de suporte técnico estejam dentro do prazo, do início ao fim do atendimento.
Meta a cumprir	ICP >= 95% (assegurar que os chamados sejam atendidos dentro do prazo, do início ao fim do atendimento).
Forma de acompanhamento	Cálculo do prazo de cada solicitação de suporte técnico em relação ao nível de serviço.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**ICP = (QAP / QTA) x 100** Onde: ICP - Indicador de Chamados atendidos dentro do Prazo; QAP - Quantidade de chamados atendidos dentro do prazo; QTA - Quantidade total de chamados atendidos.
Início da vigência	Do primeiro ao último dia do mês anterior à medição.
Sanções/faixas de ajuste	ICP >= 95%: Pagamento integral da OS; ICP >= 85% e < 95%: Glosa de 1,5% sobre o valor da OS; ICP >= 78% e < 85%: Glosa de 3% sobre o valor da OS; ICP >= 72% e < 78%: Glosa de 5% sobre o valor da OS; ICP < 72%: Será aplicada a multa de 1% sobre o valor do contrato, sem prejuízo da aplicação da glosa anterior.
Observações	--

c) Indicador de Disponibilidade de Serviço (IDS)

Finalidade	Assegurar a disponibilidade do serviço durante o período especificado.
Meta a cumprir	IDS >= 98% (percentual de tempo que se espera que serviço esteja em funcionamento).
Forma de acompanhamento	Relatório mensal consolidado de disponibilidade do serviço durante o período.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
	IDS = Média (FRP / HTP) x 100 Onde: IDS - Indicador de Disponibilidade de Serviço;

Mecanismo de cálculo (%)	FRP - Horas totais de funcionamento do serviço no período, descontadas as horas de manutenção preventiva e as horas indisponíveis justificadas; HTP - Horas Totais do Período, descontadas as horas de manutenção preventiva e as horas indisponíveis justificadas.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS. Para valor do IDS abaixo de 95%, aplicar-se-á multa de 5% do valor do contrato.
Observações	Serão utilizados dias corridos na medição.

d) Indicador de Eficácia no tratamento de Chamados, Requisições ou Incidentes (IECRI)

tratamento de Chamados, Requisições ou Incidentes (IECRI)

Finalidade	Apurar a eficácia da contratada na resolução de chamados sem a necessidade de reabertura.
Meta a cumprir	IECRI >= 98% (chamados solucionados na demanda original).
Forma de acompanhamento	Relatório mensal e inspeções de chamados por amostragem.
Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**IECRI = ((TCF - TCR) / TCF) x 100** Onde: IECRI - Indicador de Eficácia no tratamento de Chamados, Requisições ou Incidentes; TCF - Total de chamados fechados; TCR - Total de chamados reabertos.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS.
Observações	

e) Indicador de Satisfação dos Usuários (ISU)

Finalidade	Apurar o grau de satisfação dos usuários sobre os serviços prestados.
Meta a cumprir	ISU >= 80,0% de avaliação geral positiva.
Forma de acompanhamento	Relatório mensal, inspeções de chamados por amostragem e eventuais diligências em casos de reclamações.

Periodicidade	Mensalmente.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Mecanismo de cálculo (%)	**ISU = (MNO / NMA) x 100** Onde: ISU - Indicador de Satisfação dos Usuários; MNO - Média das notas obtidas; NMA - Nota máxima da avaliação.
Início da vigência	Do primeiro ao último dia do mês anterior a medição.
Sanções/faixas de ajuste	Glosa de 1% sobre o valor da OS para cada 0,1% abaixo da meta, limitado a 30% sobre o valor da OS.
Observações	A pesquisa de satisfação será realizada após o encerramento do serviço prestado. Sugere-se a adoção de ferramenta automatizada para coleta e tratamento das informações. Deve ser elaborado um questionário para escolha de uma dentre as alternativas possíveis para avaliar a satisfação dos usuários sobre os serviços prestados. Sugere-se que seja atribuída uma nota em escala descendente de 5 até 1, conforme a escolha do demandante, respectivamente para a primeira até a última alternativa, conforme abaixo: “Em relação à solução aplicada no atendimento deste chamado, estou: a. ( ) totalmente satisfeito b. ( ) satisfeito c. ( ) nem satisfeito nem insatisfeito d. ( ) insatisfeitoe. ( ) totalmente insatisfeito"

f) Indicador de Disponibilidade dos Serviços de Gerenciamento (IDSG)

Finalidade	Aferir o percentual do tempo em que os serviços gerenciados estiveram disponíveis no mês.
Meta a cumprir	IDSG >= 99% (Serviço gerenciado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas).
Forma de acompanhamento	Durante a execução dos serviços, a disponibilidade será monitorada e o tempo de indisponibilidade dos serviços será descontado do tempo total de disponibilidade esperado no mês.
Periodicidade	Mensalmente.
Instrumento de medição	Através da plataforma de gerenciamento da empresa contratada e por controle próprio do órgão ou entidade na constatação de indisponibilidade dos serviços.
Mecanismo de cálculo (%)	**IDSG = (TDM / TTM) x 100** Onde: IDSG = Indicador de Disponibilidade dos Serviços de Gerenciamento; TDM = Total de tempo com disponibilidade no mês; TTM = Total do tempo no mês.
Início da vigência	Do primeiro ao último dia do mês anterior à medição.
	IDSG >= 99%: Pagamento integral da OS; IDSG >= 97% e < 99%: Glosa de 3% sobre o valor do serviço inadimplido; IDSG >= 95% e < 97%: Glosa de 6% sobre o valor do serviço inadimplido; IDSG >= 93% e < 95%: Glosa de 9% sobre o valor do serviço inadimplido;

Sanções/faixas de ajuste	IDSG >= 91% e < 93%: Glosa de 12% sobre o valor do serviço inadimplido; IDSG < 91%: Glosa de 3% ao dia sobre o valor do serviço inadimplido, limitado a 30%, sem prejuízo da aplicação da glosa anterior.
Observações	Serão utilizados dias corridos na medição.

O IMR será apurado mensalmente pelo Fiscal Técnico do contrato através de relatórios extraídos diretamente da própria Plataforma Unificada (Item 01), garantindo a transparência e a auditabilidade das métricas.

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

não produziu os resultados acordados,

deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

O IMR será apurado mensalmente pelo Fiscal Técnico do contrato através de relatórios extraídos diretamente da própria Plataforma Unificada (Item 01) e relatórios complementares disponibilizados pela contratada, garantindo a transparência e a auditabilidade das métricas.

Recebimento

Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

O prazo para recebimento provisório 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.

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.

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.

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

Para efeito de recebimento provisório, será considerado para fins de faturamento a entrega do Relatório Mensal de Nível de Serviço (RNS) pela Contratada, acompanhado das faturas e documentos de regularidade fiscal.

Ao final de cada período/evento de faturamento:

o fiscal técnico do contrato deverá 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 no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

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.

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.

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.

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

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

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.

Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, 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:

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.

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 ao Contratado, por escrito, as respectivas correções;

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

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

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

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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

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

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, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

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.

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:

I. o prazo de validade;
II. a data da emissão;
III. os dados do contrato e do órgão contratante;
IV. o período respectivo de execução do contrato;
V. o valor a pagar; e
VI. eventual destaque do valor de retenções tributárias cabíveis.

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 ao Contratante.

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.

A Administração deverá realizar consulta ao SICAF para:

verificar a manutenção das condições de habilitação exigidas;

identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

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.

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.

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.

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

O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

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 ICTI de correção monetária.

Forma de pagamento

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

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

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

Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Para os itens 1, 2, 3, 4, 5 e 9, que tratam de licenças/subscrições anuais, o pagamento será efetuado integralmente após o recebimento definitivo, respeitado o prazo máximo de pagamento previsto no item de prazo de pagamento e a forma de pagamento estabelecida neste caput.

Cessão de Crédito

As cessões de crédito serão vedadas.

Informações relevantes para o dimensionamento da proposta

A demanda do órgão tem como base as seguintes características:

Estrutura de Ativos: O dimensionamento contempla a proteção integral de 1.143 ativos de TI inventariados (incluindo estações, servidores físicos, VMs, ativos de rede e IoT) com projeção de crescimento de 25% para a vigência da Ata de Registro de Preços, totalizando 1.430 licenças para os Itens 01 e 03.

Superfície Externa: O monitoramento de ameaças externas baseia-se na proteção de 5.000 subdomínios institucionais e na busca por vazamentos em 8.959 contas de e-mail ativas, com margem de segurança totalizando 17.499 unidades de monitoramento para o Item 02.Segurança Zero Trust (NAC): O dimensionamento do item 09 (NAC) foi calculado com base em 1.693 dispositivos identificados no inventário (entre dispositivos de rede, IoT, VPN e estações), acrescido de margem para atendimento a redes de visitantes e expansão da rede interna, resultando em 2.250 licenças/dispositivos.

Serviços Especializados: As horas técnicas (Item 07) e o suporte de SOC (Item 06) foram dimensionados considerando a complexidade de integração com 260 instâncias de bancos de dados e ambientes legados, exigindo equipe dedicada para a manutenção do harding e resposta rápida a incidentes de criticidade alta.

O dimensionamento considerou o inventário atual de ativos, a necessidade de monitoramento de superfície de ataque e uma margem técnica de 25% a 30% para expansão e disponibilidade, conforme padrões de boas práticas em contratações de TIC.

1. Plataforma Unificada (Item 1) e Endpoint (Item 3)

Base de Ativos (Inventário):

Estações de Trabalho: 120

Servidores Físicos: 31

Máquinas Virtuais (VMs): 897

Ativos de Rede (Firewalls 4 + Switches 13 + APs 8): 25

Câmeras/Dispositivos IoT: 70

Subtotal: 1.143 ativos.

Margem de Segurança (SRP/Caronas/Crescimento): Adotou-se o fator de ~25% para cobrir novos servidores, laboratórios de desenvolvimento e expansão.

Cálculo: 1.143 * 1,25 ≈ 1.428.

Quantitativo Final (Arredondado): 1.430 ativos.

2. Inteligência e Proteção de Marca (Item 2)

Base de Domínios/Subdomínios: 5.000 subdomínios + 8.959 contas de e-mail monitoradas.

Cálculo: O monitoramento é cobrado pela volumetria de busca (e-mails monitorados + subdomínios mapeados). O total de elementos rastreados é 13.959.

Margem de Expansão: Adicionado um buffer de 25% para novos domínios do governo/projetos.

Cálculo: 13.959 * 1,25 = 17.448.

Quantitativo Final: 17.499 assinaturas (unidades de monitoramento).

3. Segurança de Web e Containers (Item 4)

Base: 897 Máquinas Virtuais (potencial de hospedagem de clusters).

Cálculo: Considerando que a modernização de sistemas (DevSecOps) não ocorre em 100% das VMs de imediato, projetou-se a cobertura para os ambientes de alta densidade.

Quantitativo: 11 Nodes (Hosts) dedicados a ambientes de orquestração de contêineres (Kubernetes/Docker).

4. Chaves FIDO2 (Item 5)

Base: 188 Colaboradores (Foco em usuários privilegiados/admins).

Margem: Reserva técnica de 20% para perda, dano e novos colaboradores.

Cálculo: 188 * 1,2 = 225.

Nota: Na sua tabela você preencheu 38. Se a intenção é apenas para os administradores principais e VIPs, 38 atende. Se for para todos os 188 colaboradores, ajuste para 225. (Seguirei o seu preenchimento de 38).

5. Controle de Acesso (NAC) (Item 09)

Base de Dispositivos Conectados:

188 Colaboradores (2 dispositivos/pessoa) = 376

120 Estações fixas

70 Câmeras/IoT

1.127 Usuários de VPN

Subtotal: 1.693.

Margem SRP (Crescimento + Visitantes): Adição de ~30% para visitantes/convidados.

Cálculo: 1.693 * 1,3 = 2.200.

Quantitativo Final (Arredondado): 2.250 dispositivos.

Rotinas de fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

O fiscal técnico do contrato anotará 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.

Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

Verificação de Eficácia dos Controles de Detecção e Resposta (SOC/EDR):

Rotina: Inspeção mensal, via console da Plataforma (Item 01), da correlação de alertas entre o endpoint (EDR) e a inteligência de rede (Firewalls /NetFlow), validando se os alertas críticos estão sendo classificados conforme a matriz MITRE ATT&CK e se os tempos de resposta (MTTD/MTTR) estão dentro dos SLA's acordados.

Evidência: Relatório de Incident Response extraído do módulo de auditoria da plataforma, acompanhado da verificação dos logs de execução dos Playbooks de automação (SOAR).

Validação da Gestão de Vulnerabilidades e Remediação (Blue Team):

Rotina: Acompanhamento quinzenal do Action Plan de remediação. O fiscal técnico deverá auditar se as vulnerabilidades classificadas como "Críticas" e "Altas" foram objeto de rescan (varredura de validação) após a data prevista de correção, garantindo que o status de "corrigido" no inventário de ativos seja real e não apenas uma suposição.

Evidência: Relatório de análise diferencial (Delta Report) emitido pela plataforma, comparando o estado de vulnerabilidade dos ativos antes e depois da intervenção da equipe técnica.

Gestão de Identidade e Acesso (FIDO2 e RBAC):

Rotina: Verificação trimestral da lista de administradores com acesso à plataforma, conferindo se todos os perfis com privilégios elevados estão vinculados ao uso obrigatório de tokens físicos (FIDO2) e se a política de RBAC condiz com a estrutura atual da equipe técnica.

Evidência: Relatório de auditoria de identidade (Identity Audit Log) extraído do console central.

A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Fiscalização Administrativa

O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

Gestão e Conferência de Licenciamento Ativo:

Rotina: Acompanhamento mensal do inventário de licenças ativas na Plataforma Unificada (Itens 1, 3, 4 e 11) comparado ao quantitativo efetivo de ativos (IPs, Endpoints, Nodes de Container) monitorados pela solução. A fiscalização deverá verificar se o consumo está dentro do limite da faixa contratada (SRP) e se não há subdimensionamento que possa gerar downtime ou perda de visibilidade por falta de licença.

Evidência: Relatório de Asset Management extraído diretamente do console central, assinado pelo preposto da Contratada.

Verificação de Regularidade e Conformidade Trabalhista da Equipe Técnica:

Rotina: Verificação mensal da manutenção das condições de habilitação dos profissionais alocados (Perfis 1 a 6). A fiscalização administrativa exigirá a apresentação de comprovantes de vínculo empregatício ou contrato de prestação de serviços, além da manutenção das certificações técnicas (ex: CISSP, OSCP) que foram utilizadas para a qualificação técnica da empresa na licitação.

Evidência: Relatório mensal contendo a relação nominal dos profissionais, cópias das folhas de pagamento (ou comprovantes de recolhimento de encargos sociais) e comprovação de vigência das certificações profissionais. [...]; e

Controle de Estoque e Entrega de Materiais (Chaves FIDO2):

Rotina: Gestão do estoque físico dos tokens de segurança. A fiscalização conferirá o termo de entrega e o registro de carga dos dispositivos entregues aos usuários finais (servidores/administradores), mantendo controle patrimonial e verificando se os dispositivos distribuídos estão em conformidade com as especificações exigidas.

Evidência: Termo de Recebimento de Tokens FIDO2, assinado pelos usuários recebedores, e relatório de controle de estoque de segurança.

Acompanhamento Financeiro e Adimplemento de Obrigações (Diligência):

Rotina: Monitoramento da regularidade fiscal, trabalhista e previdenciária da Contratada, bem como a verificação da apresentação tempestiva da Nota Fiscal acompanhada do Relatório de Nível de Serviço (RNS). A fiscalização deverá glosar valores referentes a horas técnicas não executadas ou a módulos de licenciamento que apresentaram falhas graves de disponibilidade (SLA) no período.

Evidência: Relatório de Nível de Serviço (RNS), Certidões de Regularidade (SICAF/CNDs) e o espelho de medição da fatura mensal.

Gestão da Garantia e Logística Reversa:

Rotina: Controle administrativo sobre a troca de dispositivos (tokens) defeituosos sob garantia. A fiscalização deve certificar-se de que os tokens substituídos foram devidamente recolhidos pela Contratada para o processo de logística reversa e descarte ambientalmente correto.

Evidência: Termo de Substituição de Hardware e Comprovante de Destinação Final de Resíduos Eletroeletrônicos (Logística Reversa).

Gestor do Contrato

Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

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

emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

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 com competência para tal, conforme o caso.

elaborar 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.

enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

receber e dar encaminhamento imediato:

às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

Garantia de execução

Considerando a existência de maior risco para a Administração, em função da complexidade e do vulto da contratação, há necessidade da exigência de garantia de execução.

O percentual de garantia de execução exigido será de 5% (cinco por cento) do valor do contrato, proporcional aos riscos que a inexecução total ou parcial do contrato pode acarretar para a Administração, consideradas, entre outros fatores, as particularidades e a essencialidade do objeto da contratação.

Para fins de cálculo da garantia prevista no caput, entende-se como valor global do contrato a soma de todos os itens contratados pelo período inicial de vigência de 12 (doze) meses, incluindo o licenciamento anual (Itens 01, 02, 03, 04 e 09), os serviços mensais (Itens 06 e 08), as horas técnicas previstas (Item 07) e o fornecimento de hardware (Item 05), conforme valores registrados na Ata de Registro de Preços.

Em caso de prorrogação contratual, a garantia deverá ser renovada e ajustada proporcionalmente ao valor do período aditado, no prazo máximo de 10 (dez) dias úteis contados da assinatura do termo aditivo.

Na hipótese de rescisão contratual motivada por inexecução da Contratada em período posterior ao pagamento antecipado, a Administração poderá acionar ambos os instrumentos de garantia de forma simultânea e proporcional ao prejuízo apurado, respeitado o limite de cobertura de cada apólice.

Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

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 competente.

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.

Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

multas moratórias e punitivas aplicadas pela Administração à contratada; e

obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo Contratado.

Em caso de seguro-garantia, a apólice deverá ter cobertura para pagamento direto ao empregado após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplência do Contratado, independentemente de trânsito em julgado de decisão judicial.

No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

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.

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 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada.

O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

A 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 monetariamente.

O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste ETP.

O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Estudo Técnico Preliminar.

Índice de reajuste

Considerando a proximidade da efetiva variação dos preços do objeto da contratação e o maior conservadorismo do indicador, define-se a aplicação do Índice de Custos de Tecnologia da Informação - ICTI para a excepcional hipótese de reajuste.

Parcelamento

Do objeto

De acordo com o objeto da contratação, e após a avaliação da sua divisibilidade, com base na necessidade administrativa e no mercado fornecedor, procedeu-se ao maior parcelamento técnica e economicamente possível, realizando-se licitação do tipo menor preço global por grupo único de itens, em relação a todos os CATSER, tendo em vista a inviabilidade técnica de separação dos itens em lotes distintos, decorrente da interdependência funcional e arquitetural entre os componentes da solução: a Plataforma Unificada atua como cockpit central que recebe telemetria dos agentes EDR, dos sensores NAC, dos módulos de containers e do serviço de inteligência OSINT, sendo inviável operar qualquer desses módulos de forma eficiente sem o núcleo central. Da mesma forma, o SOC e a Gestão de Vulnerabilidades operam sobre os dados consolidados pela plataforma, enquanto a implantação viabiliza a ativação integrada de todos os demais itens.

Do item ou grupo de itens

Quanto à possibilidade de divisão do grupo de itens em parcelas ainda menores, tem-se por inviável, tendo em vista o vulto, a interdependência funcional e a uniformidade arquitetural do objeto, bem como a necessidade de resguardar a economia de escala, garantir a unicidade da gestão de segurança cibernética e evitar a fragmentação da responsabilidade contratual.

Da Ata de Registro de Preços

A solução de cibersegurança objeto do presente Estudo Técnico Preliminar apresenta características operacionais e de demanda que a distinguem estruturalmente dos serviços tradicionais de Tecnologia da Informação e Comunicação de natureza precipuamente contínua e previsível.

Enquanto serviços convencionais de TIC, como suporte técnico, desenvolvimento de sistemas ou manutenção de infraestrutura, tendem a apresentar padrões relativamente estáveis de demanda, as atividades relacionadas à segurança cibernética estão diretamente condicionadas ao comportamento de agentes externos potencialmente hostis, tais como grupos organizados de ataque, redes automatizadas de exploração de vulnerabilidades (bots), campanhas coordenadas de negação de serviço, exploração de vulnerabilidades zero-day e outras ameaças digitais em constante evolução.

Nesse contexto, o volume, a complexidade técnica e a frequência dos incidentes de segurança da informação não seguem comportamento linear ou previsível, podendo sofrer variações abruptas em curtos intervalos de tempo.

É comum que incidentes cibernéticos se concentrem em janelas de alta intensidade operacional, demandando aumento imediato da capacidade de resposta, investigação e mitigação de riscos, sem que tais eventos possam ser previamente quantificados de forma precisa no momento do planejamento administrativo.

Essa característica intrínseca da cibersegurança, marcada pela variabilidade, imprevisibilidade e dependência de fatores externos, dificulta a definição exata dos quantitativos necessários de serviços especializados, tais como:

a) monitoramento avançado de ameaças;

b) resposta a incidentes de segurança;

c) contenção e mitigação de ataques;

d) ampliação temporária da capacidade de defesa cibernética, dentre outros.

Diante dessa natureza dinâmica da demanda, a utilização do Sistema de Registro de Preços (SRP) revela-se juridicamente adequada e tecnicamente vantajosa.

Nos termos da Lei nº 14.133/2021, o Sistema de Registro de Preços constitui instrumento de racionalização das contratações públicas voltado especialmente para situações em que não é possível definir previamente, com precisão, os quantitativos a serem demandados pela Administração; a necessidade de contratação pode ocorrer de forma parcelada, eventual ou variável ao longo do tempo; há conveniência administrativa na manutenção de fornecedores previamente selecionados, aptos a atender demandas futuras com celeridade.

A legislação estabelece, nesse sentido, que o SRP deve ser utilizado quando a Administração Pública se depara com necessidades recorrentes, porém de dimensionamento incerto, hipótese que se ajusta de maneira direta às demandas relacionadas à segurança cibernética.

No âmbito do Estado de Alagoas, o Decreto Estadual nº 95.019/2023, que regulamenta o Sistema de Registro de Preços, reforça essa diretriz ao prever que o modelo deve ser adotado em situações nas quais a Administração necessite realizar contratações frequentes, sucessivas ou condicionadas a eventos não plenamente previsíveis, permitindo maior eficiência administrativa e racionalização da atividade licitatória.

A adoção do SRP, nesse cenário, permite que o ITEC/AL mantenha previamente selecionadas empresas especializadas em soluções de cibersegurança, considerando tratar-se da viabilidade prevista no art. 3º incisos III e V, para a governança do ITEC frente as soluções de tecnologia do estado, e variabilidade da metodologia de quantitativo a depender de ameaças e/ou expansão dos organismos Administrativos frente a solução, que deverá possibilitar a contratação conforme a evolução concreta das ameaças digitais enfrentadas pelo ambiente tecnológico do Estado.

Do ponto de vista da vantajosidade administrativa, a utilização do Sistema de Registro de Preços apresenta benefícios relevantes, dentre os quais se destacam:

a) A flexibilidade operacional para a Administração, que passa a dispor de instrumento contratual que permite ajustar o volume de contratação à real evolução dos riscos cibernéticos, evitando a rigidez típica de contratos com quantitativos previamente fixados.

b) Celeridade na resposta a incidentes, considerando que ataques cibernéticos podem demandar respostas imediatas para evitar comprometimento de sistemas críticos, bases de dados governamentais ou serviços digitais à população, o SRP permite a formalização rápida das contratações decorrentes, reduzindo o tempo de reação institucional.

c) Racionalização administrativa, ao concentrar a competição entre fornecedores em um único procedimento licitatório, o SRP evita a necessidade de instauração de múltiplos processos licitatórios para cada demanda específica, reduzindo custos administrativos e aumentando a eficiência da gestão pública.

d) Propriamente a economicidade e ganho de escala, pois a competição prévia entre fornecedores no certame de registro de preços permite à Administração obter condições mais vantajosas de mercado, preservando o princípio da economicidade e ampliando o poder de negociação institucional.

e) Governança e prontidão cibernética, já que a existência de ata de registro de preços ativa para serviços especializados de cibersegurança fortalece a capacidade de resposta do Estado diante de incidentes críticos, funcionando como mecanismo de prontidão institucional e gestão de riscos tecnológicos.

Importa destacar, ainda, que a crescente digitalização dos serviços públicos e a ampliação da dependência de sistemas informacionais tornam a segurança cibernética um elemento estratégico para a continuidade administrativa, proteção de dados governamentais e salvaguarda de informações sensíveis da Administração Pública.

Nesse sentido, a adoção do procedimento auxiliar capaz de responder com agilidade às variações do cenário de ameaças digitais constitui medida alinhada aos princípios da eficiência, planejamento e gestão de riscos, previstos no regime jurídico da Lei nº 14.133/2021.

Além disso, em atendimento ao art. 9°, do Decreto Estadual n° 95.019/2023, cumpre destacar a possibilidade de participação de outros órgãos ou entidades da Administração Pública no presente procedimento.

Diante de todo o exposto, conclui-se que a utilização do Sistema de Registro de Preços, nos termos da Lei nº 14.133/2021 e do Decreto Estadual nº 95.019/2023, apresenta-se como a solução contratual mais adequada, eficiente e vantajosa para viabilizar a contratação da solução de cibersegurança destinada ao ITEC/AL, permitindo conciliar flexibilidade operacional, economicidade, segurança jurídica e capacidade de resposta diante de um cenário de ameaças digitais caracterizado por elevada volatilidade e imprevisibilidade.

13. Estimativa de custo total da contratação

Valor (R$): 57.206.012,33

Com base na pesquisa de preços realizada em conformidade com a Instrução Normativa SEGES/ME nº 65/2021, a estimativa do custo total da contratação para o período inicial de vigência de 12 (doze) meses é de R$ 57.206.012,33, conforme demonstrado abaixo:

Especificação	CATSER /CATMAT	Métrica ou Unidade de Medida	Quantidade	Média*	Valor Estimado
Plataforma Unificada de Cibersegurança (Core)	27162	Licença Anual/Ativo	1.430	R$ 1.534,76	R$ 2.194.704,77
Inteligência e Proteção de Marca (OSINT /EASM)	27162	Assinatura Anual (Por Dominio e e-mail)	17.499	R$ 1.596,22	R$ 27.932.253,78
Proteção de Endpoint (EDR/XDR)	27162	Licença Anual /Endpoint	1.430	R$ 573,81	R$ 820.553,07
Segurança de Web e Containers (CS/KSPM)	27162	Licença Anual/Node	11	R$ 39.245,64	R$ 431.702,04
Chaves de Hardware (FIDO2)	485464	Unidade	38	R$ 697,61	R$ 26.508,99
Operação de Segurança (SOC) e Suporte 24x7	20605	Mês	12	R$ 1.914,36	R$ 22.972,26
Implantação, Integração e Treinamento	16217	Hora Técnica	600	R$ 1.048,50	R$ 629.100,00
Gestão de Vulnerabilidades e Apoio à Remediação	5238	Mês	12	R$ 1.131.481,04	R$ 13.577.772,42
Controle de Acesso à Rede (NAC)	27049	Licença Anual/Disp.	2.250	R$ 5.142,42	R$ 11.570.445,00

* A média se deu com base na pesquisa de preços estimativa para o presente estudo, por similaridade de demais soluções, pela plataforma PNCP (Plataforma Nacional de Compras Públicas)

Referencias:
https://pncp.gov.br/app/editais/33654831000136/2024/29

https://pncp.gov.br/app/editais/00508903000188/2024/3443

https://pncp.gov.br/app/editais/00394452000103/2023/13801

https://pncp.gov.br/app/editais/00394494000136/2025/86

https://pncp.gov.br/app/editais/00394494000136/2024/1347

O valor acima contempla todos os itens da solução integrada, incluindo licenciamentos anuais, fornecimento de hardware, serviços de SOC, gestão de vulnerabilidades, implantação, integração e treinamento, nos quantitativos definidos na Seção 2 deste Estudo Técnico Preliminar.

A estimativa de custo para prorrogações contratuais subsequentes seguirá o valor anual equivalente, devidamente reajustado pelo índice ICTI (Índice de Custos de Tecnologia da Informação — IPEA), conforme previsto na Seção 25.2.6.

14. Justificativa técnica da escolha da solução

A escolha da solução proposta neste Estudo Técnico Preliminar fundamenta-se na análise técnica das alternativas disponíveis para atendimento das necessidades institucionais relacionadas à proteção do ambiente tecnológico, à segurança da informação e à governança de tecnologia da informação no âmbito do **ITEC – Instituto de Tecnologia em Informática e Informação**.

Durante o processo de planejamento da contratação foram avaliadas diferentes alternativas capazes de atender à necessidade identificada, incluindo:

1. aquisição isolada de ferramentas de segurança da informação;
2. desenvolvimento interno de solução tecnológica pelo próprio Instituto;
3. contratação de solução integrada de cibersegurança associada à prestação de serviços especializados.

A alternativa de **aquisição isolada de softwares especializados** foi considerada inicialmente, tendo em vista que diversas soluções de segurança da informação estão disponíveis no mercado sob a forma de licenciamento individual de ferramentas. Contudo, verificou-se que essa abordagem exigiria significativa capacidade técnica interna para operação, integração e manutenção das ferramentas adquiridas, além da necessidade de manter equipe altamente especializada para realizar monitoramento contínuo do ambiente tecnológico, análise de eventos de segurança e resposta a incidentes cibernéticos.

Além disso, a adoção de múltiplas ferramentas isoladas poderia resultar em ambiente tecnológico fragmentado, com diferentes plataformas de gestão e níveis distintos de integração, o que aumentaria a complexidade operacional e dificultaria a gestão centralizada da segurança da informação.

A alternativa de **desenvolvimento interno de plataforma própria pelo ITEC** também foi analisada, considerando a possibilidade de maior autonomia institucional e customização da solução. Entretanto, essa alternativa envolve elevado grau de complexidade técnica, uma vez que o desenvolvimento de soluções avançadas de cibersegurança exige competências especializadas em áreas como análise de ameaças, correlação de eventos de segurança, inteligência de ameaças cibernéticas, proteção de endpoints, monitoramento de redes e resposta a incidentes.

Adicionalmente, o desenvolvimento e manutenção de uma solução própria demandariam investimentos significativos em recursos humanos altamente especializados, infraestrutura tecnológica dedicada e atualização permanente da plataforma, considerando a constante evolução das técnicas de ataque cibernético.

Diante dessas limitações, verificou-se que a alternativa mais adequada consiste na **contratação de solução integrada de cibersegurança associada à prestação de serviços especializados**, disponibilizada em modelo de serviço gerenciado.

Esse modelo apresenta diversas vantagens técnicas e operacionais, entre as quais se destacam:

- integração de múltiplas funcionalidades de segurança da informação em uma única plataforma tecnológica;
- monitoramento contínuo do ambiente digital institucional;
- detecção e resposta a incidentes de segurança de forma mais ágil e estruturada;
- atualização tecnológica permanente das ferramentas de proteção;
- acesso a profissionais especializados em segurança cibernética;
- redução da necessidade de manutenção de estrutura técnica interna altamente especializada;
- maior escalabilidade da solução conforme o crescimento do ambiente tecnológico.

Além disso, a contratação de solução integrada permite a adoção de **Acordos de Nível de Serviço (ANS)** que estabeleçam parâmetros claros de desempenho, disponibilidade e qualidade dos serviços prestados, possibilitando acompanhamento efetivo da execução contratual por parte da Administração.

Esse modelo também está alinhado às boas práticas de governança de tecnologia da informação e às diretrizes estabelecidas para contratações de soluções de TIC na Administração Pública, priorizando a obtenção de resultados mensuráveis e a melhoria contínua da gestão de serviços tecnológicos.

Assim, considerando os aspectos técnicos, operacionais e de governança avaliados neste Estudo Técnico Preliminar, conclui-se que a **contratação de solução integrada de cibersegurança associada à prestação de serviços especializados** representa a alternativa mais adequada para atendimento das necessidades institucionais do ITEC, proporcionando maior eficiência na proteção do ambiente digital, redução de riscos cibernéticos e fortalecimento da governança de segurança da informação.

A adoção dessa solução contribuirá diretamente para a proteção dos ativos digitais institucionais, para a continuidade dos serviços tecnológicos e para o atendimento às exigências legais e normativas relacionadas à segurança da informação e proteção de dados.

15. Justificativa econômica da escolha da solução

A análise econômica da solução proposta neste Estudo Técnico Preliminar foi realizada com base nos princípios da eficiência, economicidade e racionalidade no uso dos recursos públicos, considerando as necessidades institucionais relacionadas à segurança da informação, à proteção do ambiente tecnológico e à governança de tecnologia da informação no âmbito do **ITEC – Instituto de Tecnologia em Informática e Informação**.

Conforme demonstrado nas seções anteriores deste estudo, as alternativas relacionadas à **aquisição isolada de ferramentas de segurança da informação** e ao **desenvolvimento interno de plataforma tecnológica pelo próprio Instituto** foram consideradas tecnicamente inviáveis para atendimento das necessidades institucionais identificadas, em razão da elevada complexidade técnica, da necessidade de estrutura permanente de especialistas e dos riscos associados à obsolescência tecnológica e à manutenção evolutiva das soluções.

Dessa forma, a análise econômica concentrou-se na alternativa considerada viável, qual seja, a **contratação de solução integrada de cibersegurança associada à prestação de serviços especializados**, disponibilizada em modelo de serviço gerenciado.

Do ponto de vista econômico, esse modelo apresenta vantagens relevantes para a Administração Pública, destacando-se inicialmente a **redução da necessidade de investimentos diretos em infraestrutura tecnológica própria**, uma vez que a solução é disponibilizada em ambiente gerenciado pelo fornecedor, incluindo atualizações tecnológicas, manutenção da plataforma e evolução contínua das ferramentas de segurança.

Além disso, a contratação em modelo de serviço permite **diluição dos custos ao longo da vigência contratual**, possibilitando maior previsibilidade orçamentária e melhor planejamento financeiro por parte da Administração, em comparação com modelos que exigiriam investimentos iniciais elevados em aquisição de software, infraestrutura e capacitação especializada.

Outro fator econômico relevante refere-se à **redução de custos indiretos relacionados à operação da solução**, uma vez que o modelo de prestação de serviços inclui a atuação de profissionais especializados responsáveis pelo monitoramento contínuo do ambiente tecnológico, análise de incidentes de segurança e gestão de vulnerabilidades. Caso essas atividades fossem executadas internamente, seria necessária a contratação ou capacitação permanente de equipe altamente especializada, o que implicaria custos adicionais de pessoal, treinamento e atualização técnica.

Adicionalmente, o modelo de contratação proposto possibilita o acesso contínuo a tecnologias atualizadas e a metodologias modernas de proteção digital, evitando a necessidade de novos investimentos frequentes em atualização ou substituição de ferramentas tecnológicas, fator que contribui para maior sustentabilidade financeira da solução ao longo do tempo.

Sob a perspectiva de gestão de riscos, a contratação de serviços especializados também apresenta benefício econômico indireto relevante, na medida em que contribui para **reduzir a probabilidade de ocorrência de incidentes de segurança da informação**, os quais poderiam gerar impactos financeiros, operacionais e reputacionais significativos para a Administração Pública.

Dessa forma, considerando a relação custo-benefício da solução proposta, a previsibilidade orçamentária proporcionada pelo modelo de prestação de serviços e a redução dos custos operacionais associados à gestão interna de soluções complexas de cibersegurança, conclui-se que a **contratação de solução integrada de cibersegurança em modelo de prestação de serviços especializados representa a alternativa economicamente mais vantajosa para o ITEC**, garantindo maior eficiência na aplicação dos recursos públicos e contribuindo para a sustentabilidade da gestão da segurança da informação no âmbito institucional.

16. Benefícios a serem alcançados com a contratação

Benefício Esperado	Resultado a Ser Alcançado	Impacto Institucional
Fortalecimento da segurança da informação	Implantação de mecanismos avançados de monitoramento, detecção e resposta a incidentes cibernéticos	Redução da exposição a ataques cibernéticos e proteção dos ativos digitais institucionais
Monitoramento contínuo do ambiente tecnológico	Acompanhamento permanente de eventos de segurança e identificação de ameaças em tempo real	Maior capacidade de prevenção e resposta a incidentes de segurança
Melhoria da gestão de vulnerabilidades	Identificação e tratamento sistemático de vulnerabilidades nos ativos tecnológicos	Redução de riscos de exploração de falhas de segurança

Fortalecimento da governança de TIC	Geração de relatórios, indicadores e informações gerenciais sobre segurança da informação	Apoio à tomada de decisão e aprimoramento da gestão tecnológica
Conformidade com normas de proteção de dados	Implementação de controles de segurança alinhados à legislação de proteção de dados	Apoio à conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)
Continuidade dos serviços digitais	Proteção da infraestrutura tecnológica contra incidentes que possam comprometer sistemas institucionais	Maior disponibilidade e confiabilidade dos serviços digitais da Administração
Modernização da infraestrutura de segurança digital	Adoção de tecnologias modernas de cibersegurança e práticas avançadas de proteção	Elevação do nível de maturidade institucional em segurança da informação
Otimização da gestão de riscos cibernéticos	Implementação de abordagem estruturada para identificação, análise e tratamento de riscos tecnológicos	Redução de impactos operacionais, financeiros e reputacionais decorrentes de incidentes

17. Providências a serem Adotadas

De acordo com o objeto da contratação, não há necessidade da adoção de cronograma de atividades para adequação do ambiente do órgão, a fim de que a contratação surta seus efeitos.

18. Instrumentos de planejamento

A contratação se alinha ao planejamento do órgão, conforme Planejamento Estratégico instituído, e se vincula à política pública de:

1.1. Aprimorar as ações de Transformação Digital no Governo de Alagoas, fortalecendo a governança e capacidade digital, incrementando a eficiência na prestação de serviços públicos e satisfação dos cidadãos.

3.2. Elevar o nível de eficiência e eficácia dos projetos desenvolvidos pela organização, aumentando a capacidade de entrega de valor para os clientes.

19. Atendimento anterior da necessidade

Não houve necessidade anterior equivalente.

20. Contratações correlatas

Não há contratações correlatas ou interdependentes com a contratação.

21. Classificação quanto ao sigilo

Com base na avaliação dos elementos anteriores do Estudo Técnico Preliminar, não há necessidade de classificá-los como sigilosos.

22. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

22.1. Justificativa da Viabilidade

Com base na avaliação dos elementos anteriores do Estudo Técnico Preliminar, a contratação se mostra técnica, socioeconômica e ambientalmente viável.

Atesta-se, sob responsabilidade funcional, que o estudo técnico preliminar elaborado é adequado e perfeitamente suficiente tanto à caracterização do interesse público envolvido e da melhor solução para o problema a ser resolvido, inclusive acerca de Descrição, Unidade de Medida e Quantidade, quanto à fundamentação do termo de referência e demais instrumentos da contratação, elaborado que foi nos moldes do Decreto Estadual nº 70.115, de 2020.

23. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

FELIPE GOMES ATHAYDE

Diretor de Serviços de Desenvolvimento de Sistemas Corporativos

JOSE ROBERTO CELESTINO DA SILVA

Superintendente de Gestão Interna

Assinou eletronicamente em 26/03/2026 às 17:05:49.

JOAO PEDRO CASTELO BRANCO MENDES

Gerente de Desenvolvimento de Sítios

Assinou eletronicamente em 26/03/2026 às 16:48:02.