



ESTADO DO ACRE
SECRETARIA DE ESTADO DE ADMINISTRAÇÃO

Av. Getúlio Vargas, 232, Palácio das Secretarias - 1º e 2º andares - Bairro Centro, Rio Branco/AC, CEP 69900-060
Telefone: - www.ac.gov.br

EDITAL PREGÃO ELETRÔNICO SRP N.º 020/2026 - COMPRASGOV N.º 90020/2026

O Estado do Acre, por intermédio da Secretaria Adjunta de Compras, Licitações e Contratos - SELIC, infra qualificada, torna público aos interessados que na data, horário, e condições abaixo indicados, fará realizar licitação na modalidade de **PREGÃO na forma ELETRÔNICA**, tudo de conformidade com Decreto Estadual n.º 11.363 de 22/11/2023, Lei Complementar n.º 123/2006, Lei n.º 8.078/90, Código de Defesa do Consumidor, aplicando-se subsidiariamente, a Lei n.º 14.133/2021 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

Esta licitação foi regularmente autorizada pelo **Órgão Contratante** conforme consta no processo administrativo, sendo a Secretaria Adjunta de Compras, Licitações e Contratos - SELIC, órgão da estrutura administrativa da Secretaria de Estado de Administração - SEAD, responsável pelos procedimentos licitatórios, designada como **Órgão Promotor** da licitação.

PROCESSO ADMINISTRATIVO:	0715.007435.00055/2025-41
ÓRGÃO CONTRATANTE:	Secretaria de Estado da Fazenda do Acre (SEFAZ/AC)
UASG:	927996
MODALIDADE:	PREGÃO
FORMA:	ELETRÔNICO
SRP:	<input checked="" type="checkbox"/> SIM <input type="checkbox"/> NÃO
CRITÉRIO DE JULGAMENTO:	<input type="checkbox"/> MENOR PREÇO POR ITEM <input checked="" type="checkbox"/> MENOR PREÇO POR LOTE <input type="checkbox"/> MAIOR PERCENTUAL DE DESCONTO POR ITEM <input type="checkbox"/> MAIOR PERCENTUAL DE DESCONTO POR LOTE
MODO DE DISPUTA:	<input checked="" type="checkbox"/> ABERTO
VALOR DE CARÁTER SIGILOSO:	<input checked="" type="checkbox"/> SIM <input type="checkbox"/> NÃO
VALOR ORÇADO:	<input checked="" type="checkbox"/> Valor Estimado <input type="checkbox"/> Valor Máximo Aceitável <input type="checkbox"/> Valor de Referência
PREFERÊNCIA ME/EPP/EQUIPARADAS (Observado o disposto no art. 4º § 1º da Lei 14.133/2021)	<input type="checkbox"/> SIM <input checked="" type="checkbox"/> NÃO

INTERVALO MÍNIMO DE DIFERENÇA ENTRE OS LANCES (DISPUTA ABERTA):	VALOR [R\$ 0,01]
INVERSÃO DE FASES:	<input type="checkbox"/> SIM <input checked="" type="checkbox"/> NÃO
PROVEDOR:	Sistema de Compras do Governo Federal (COMPRASGOV). http://www.gov.br/compras/pt-br/
DATA DA ABERTURA:	30/01/2026
HORÁRIO DE BRASÍLIA:	09h15min
PERÍODO DE RETIRADA:	14/01/2026 à DATA DE ABERTURA
ENDEREÇO ELETRÔNICO:	http://www.gov.br/compras/pt-br/ e/ou http://www.licitacao.ac.gov.br
PREGOEIRO(A):	Mario Jorge Moraes de Oliveira
NOMEAÇÃO:	Portaria SEAD nº. 262 de 12 de Março de 2025, publicado no Diário Oficial do Estado do Acre, ano LVII, Nº. 13.980 de 13 de Março de 2025.
<p>Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local estabelecidos no preâmbulo deste Edital, desde que não haja comunicação do(a) Pregoeiro(a) em contrário.</p>	

O Pregão será realizado pelo(a) Pregoeiro(a) a ser designado por esta secretaria, bem como os Servidores que irão compor a equipe de apoio. Na ausência ou impedimento do(a) Pregoeiro(a) ou equipe de apoio indicado neste item, poderão atuar outros servidores oficialmente capacitados e designados pela Administração.

1. DO OBJETO

- 1.1. Constitui objeto da presente licitação a **Registro de preços para** Contratação de empresa especializada para **prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS (Software as a Service), com o fornecimento das respectivas soluções de software e serviços técnicos especializados, visando atender às demandas da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC),** nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.
- 1.2. **Em caso de divergência existente entre as especificações deste objeto descritas no COMPRASGOV e as especificações constantes do Anexo I deste Edital prevalecerão às últimas.**
- 1.3. Acompanham este Edital os seguintes Anexos:

Anexo I: Termo de Referência

Anexo II: Minuta da ata de Registro de Preço

Anexo III: Minuta de Contrato

Anexo IV: Modelo de Proposta de Preços

Anexo V: Matriz de Risco

2. DA ATA DE REGISTRO DE PREÇOS

- 2.1. O Registro de Preços será formalizado por intermédio da Ata de Registro de Preços, na forma do **Anexo II** e condições previstas neste Edital.
- 2.2. O prazo de vigência da ata de registro de preços será de (01) um ano contado da data da sua assinatura, e poderá ser prorrogado por igual período, desde que comprovada a vantajosidade do preço.
- 2.2.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida na forma prevista no art. [341 do Decreto Estadual nº. 11.363 de 22/11/2023](#).

3. DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES

3.1. Qualquer pessoa poderá apresentar pedido de esclarecimentos ou impugnação ao edital de licitação, por meio eletrônico, no e-mail: selic.protocolo@gmail.com, ou excepcionalmente ou por escrito e entregue sob protocolo da Secretaria Adjunta de Compras, Licitações e Contratos - SELIC, localizada na Estrada do Aviário, 927 – Bairro Aviário - Rio Branco/Acre - CEP 69900-830, de segunda à sexta feira, no horário de 7h às 14h, **em até 03 (três) dias úteis antes da data fixada para a abertura da sessão pública.**

3.2. O(A) Pregoeiro(a) responderá aos pedidos de esclarecimentos e às impugnações no prazo de até 05 (cinco) dias úteis contados da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, podendo requisitar subsídios formais aos responsáveis pela fase preparatória.

3.3. A impugnação não possuirá efeito suspensivo, exceto em situações excepcionais devidamente motivadas pelo(a) Pregoeiro(a) nos autos do processo de licitação.

3.4. As respostas aos pedidos de esclarecimentos e às impugnações serão divulgadas por meio de notificações no sistema COMPRASGOV <http://www.gov.br/compras/pt-br> e no site <http://www.licitacao.ac.gov.br>, ficando todos os interessados obrigados a acessá-los para obtenção das informações prestadas pelo(a) Pregoeiro(a).

3.5. Acolhida a impugnação, será republicado o edital com as mesmas formalidades de sua publicação original e, conforme o caso, será definida nova data para a realização do certame, observando-se a regra do art. 145 do Decreto Estadual nº. 11.363 de 22/11/2023.

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO

4.1. A participação na licitação importa total, irrestrita e irretratável submissão dos proponentes às condições deste Edital.

4.2. Poderão participar deste PREGÃO ELETRÔNICO os interessados que:

4.2.1. Cujo ramo de atividade seja compatível com o objeto desta licitação.

4.2.2. Estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

4.2.3. 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.

4.2.4. 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.

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

4.3. **Não poderão concorrer direta ou indiretamente nesta licitação:**

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

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

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

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

4.3.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

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

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

4.3.8. tenham agente público integrante do órgão promotor e/ou do órgão solicitante da licitação, que participe da empresa na qualidade de sócio, dirigente ou responsável técnico, vedada também sua participação indireta;

4.3.8.1. A vedação de que trata o **item anterior** 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.

4.3.9. estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores ou insolvência, em processo de dissolução ou liquidação, **EXCETO quando autorizada judicialmente ou quando estiver com plano de recuperação aprovado e homologado.**

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

4.3.11. 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](#).

4.3.12. Conste a inscrição da empresa no [Sistema Integrado de Registro do Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS e Cadastro Nacional de Empresas Punidas – CNEP](#). Sendo a inscrição impeditiva apenas nos casos em que o efeito da sanção apontada no referido cadastro representar óbice à participação em licitações e contratações no Estado do Acre.

4.4. O impedimento de que trata o **item 4.3.4** 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.

4.5. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os **itens 4.3.2 e 4.3.3** 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.

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

4.7. O disposto nos itens **4.3.2 e 4.3.3** 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.

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

5. DO CREDENCIAMENTO E DA REPRESENTAÇÃO

5.1. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao Sistema Eletrônico, no site <http://www.gov.br/compras/pt-br/>.

5.2. O credenciamento do interessado e de seu representante junto ao sistema eletrônico de compras implicará a sua responsabilidade legal pelos atos praticados e presunção de capacidade para a realização das transações inerentes à licitação.

5.3. Caberá ao licitante acompanhar as operações no sistema eletrônico de compras durante a sessão pública da licitação, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.4. Caberá ao licitante interessado em participar do processo licitatório na forma eletrônica observar o disposto no art. [148 do Decreto Estadual 11.363/2023](#).

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

6.2. 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.

6.3. 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.

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

6.4.1. 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, conforme disposto no [art. 63 § 1º da Lei 14.133/2021](#).

6.4.2. 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 7º, XXXIII, da Constituição](#);

6.4.3. 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](#);

6.4.4. 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.

6.5. O licitante organizado em cooperativa, **quando permitido a participação**, deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).

6.6. **O fornecedor enquadrado como microempresa, empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 3º 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.

- 6.6.1. 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;
- 6.6.2. 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.
- 6.7. A falsidade da declaração de que trata os **itens 6.4 ou 6.6** sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e neste Edital.
- 6.8. 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.
- 6.9. 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.
- 6.10. 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.
- 6.11. 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:
- 6.11.1. 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
- 6.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima, conforme estabelece o [artigo 19 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022](#)
- 6.12. 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:
- 6.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e
- 6.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto, conforme estabelece a [Instrução Normativa SEGES nº 73, de 30 de setembro de 2022 \(art. 19, § 1º\)](#).
- 6.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do **item 6.11** 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.
- 6.14. 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.
- 6.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

7. DO PREENCHIMENTO DA PROPOSTA

- 7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
- 7.1.1. **Valor unitário e total ou percentual de desconto conforme critério estabelecido no preâmbulo deste edital**, e demais informações exigidas no próprio campo do sistema.
- 7.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.
- 7.3. 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.
- 7.4. 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.
- 7.5. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Projeto Básico/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.
- 7.6. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações, quando participarem de licitações públicas.
- 7.7. 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 Projeto Básico/Termo de Referência.
- 7.8. A existência de elementos na proposta que permitam a identificação do licitante, antes da fase de lances, ensejarão a desclassificação da proposta inicial, conforme estabelece no [art. 151 § 4º do Decreto Estadual 11.363/2023](#).

8. DA SESSÃO PÚBLICA

- 8.1. A abertura da sessão pública deste Pregão, conduzida pelo(a) Pregoeiro(a), ocorrerá na data e na hora indicadas no preâmbulo deste edital, no sítio <http://www.gov.br/compras/pt-br/>.
- 8.2. Durante a sessão pública, a comunicação entre o(a) Pregoeiro(a) e as licitantes ocorrerá mediante troca de mensagens, em campo próprio do sistema eletrônico (“chat”).
- 8.3. Cabe ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.
- 8.4. O(A) Pregoeiro(a) poderá suspender a sessão pública do certame, justificando, no “chat”, os motivos da suspensão e informando, quando houver, a data e o horário previstos para a reabertura da sessão.
- 8.5. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.
- 8.5.1. Na inversão de fases prevista no item anterior, serão observadas as seguintes disposições:
- I - apresentação simultânea pelos licitantes dos documentos de habilitação e das propostas, exceto os relativos à regularidade fiscal;
 - II - análise dos documentos de habilitação de todos os licitantes;
 - III - divulgação do resultado da habilitação;
 - IV - disputa entre os licitantes habilitados;
 - V - exigência e análise dos documentos relativos à regularidade fiscal apenas do licitante provisoriamente classificado em primeiro lugar;
 - VI - divulgação do resultado do julgamento; e
 - VII - previsão de duas etapas recursais, observando-se o disposto no [art. 241 do Decreto Estadual nº. 11.363 de 22/11/2023](#).
- 8.6. Qualquer interessado poderá acompanhar o seu desenvolvimento em tempo real, por meio da internet.

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

- 9.1. 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.
- 9.2. 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.
- 9.3. O sistema disponibilizará campo próprio para troca de mensagens entre o(a) Pregoeiro(a) e os licitantes.
- 9.4. 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.
- 9.5. O lance deverá ser ofertado pelo valor unitário do lote
- 9.6. O prazo mínimo de validade da proposta será de 60 (sessenta) dias a contar da sessão pública.
- 9.7. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 9.8. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema, observando-se, quando houver, o intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir o melhor lance.
- 9.9. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser conforme intervalo disposto no preâmbulo do edital.
- 9.10. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.
- 9.11. Durante a fase de lances, o(a) Pregoeiro(a) poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.
- 9.12. Neste Pregão o **modo de disputa adotado é o "aberto"**, assim definido no [art. 155 do Decreto Estadual n.º 11.363, de 22 de novembro de 2023](#).
- 9.13. O envio de lances no pregão eletrônico o modo de **disputa “aberto”**, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.
- 9.13.1. A etapa de lances da sessão pública terá duração de 10 (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.

9.13.1.1. 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.

9.13.1.2. 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.

9.13.2. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o(a) pregoeiro(a), auxiliado pela equipe de apoio, poderá admitir, por uma única vez, o reinício da disputa aberta, para a definição das demais colocações.

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

9.13.2.2. Os lances iguais serão classificados conforme a ordem de apresentação.

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

9.14. Não serão registrados lances iguais na etapa de disputa aberta e prevalecerá o que for registrado primeiro.

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

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

9.16.1. Quando a desconexão do sistema eletrônico para o(a) Pregoeiro(a) persistir por tempo superior a 15 (quinze) minutos, a sessão pública será suspensa e reiniciada após comunicação expressa no sistema, sempre que possível, no turno seguinte ou em outra data previamente comunicada aos participantes com antecedência mínima de 24 (vinte e quatro) horas.

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

9.18. Após apresentação da proposta e/ou lances não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo(a) Pregoeiro(a).

9.19. 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 no sistema. 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.

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

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

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

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

9.20. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, e art. 219 do Decreto Estadual nº 11.363/2023 nesta ordem:

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

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

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

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

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

9.21.1. 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;

9.21.2. empresas brasileiras;

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

9.21.4. empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).

9.22. Esgotados todos os demais critérios de desempate previsto em lei, a escolha do licitante vencedor ocorrerá por sorteio, em sessão pública, para o qual todos os licitantes serão convocados.

9.23. O(A) Pregoeiro(a) poderá, durante a disputa, como medida excepcional, excluir a proposta ou o lance que possa comprometer, restringir ou frustrar o caráter competitivo do processo licitatório, mediante comunicação eletrônica no sistema.

9.23.1. Eventual exclusão de proposta do licitante na hipótese de que trata o item anterior implicará a retirada do licitante do certame.

9.24. Definido o resultado da disputa, o(a) Pregoeiro(a) poderá negociar o preço com o licitante provisoriamente classificado em primeiro lugar.

9.24.1. Ao licitante é assegurado o **prazo mínimo de 5 (cinco) minutos** para manifestação e/ou resposta, sob pena de desclassificação se extrapolar este limite de tempo, quando sua proposta estiver acima do estimado.

9.24.1.1. Caso o licitante manifeste o interesse em negociar, o(a) Pregoeiro(a) poderá conceder novo prazo para aceitação da contra proposta.

9.24.2. 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 ou com o percentual abaixo do definido pela Administração.

9.24.3. A negociação será realizada, exclusivamente, por meio do sistema e poderá ser acompanhada pelos demais licitantes.

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

9.25. Antes da convocação para apresentar a proposta adequada ao último lance, o(a) Pregoeiro(a) verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

9.25.1. Sistema de Cadastramento Unificado de Fornecedores - SICAF;

9.25.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria Geral da União (<https://portal.datransparencia.gov.br/sancoes/consulta?ordenarPor=nomeSancionado&direcao=asc>); e

9.25.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria Geral da União (<https://portal.datransparencia.gov.br/sancoes/consulta?ordenarPor=nomeSancionado&direcao=asc>).

9.25.3.1. O registro sanção da empresa no SICAF ou CEIS ou CNEP será impeditiva apenas nos casos em que o efeito da sanção apontada no referido cadastro representar óbice à participação em licitações e contratações no Estado do Acre.

9.26. O(A) Pregoeiro(a) solicitará o envio da proposta de preços conforme condições mínimas previstas no **Modelo de Proposta de Preços constante do Anexo IV deste edital, no prazo mínimo de 2 (duas) horas**, adequada ao valor final ofertado, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados, **sob pena de desclassificação**.

9.27. O prazo de que trata o item anterior poderá ser prorrogado por igual período, antes do término do prazo originalmente previsto, mediante solicitação do licitante através do chat no sistema eletrônico ou através do e-mail: selic.protocolo@gmail.com, a critério do(a) Pregoeiro(a).

9.28. Para o envio dos documentos, o(a) Pregoeiro(a) fará uso da opção “**Convocar Anexo**”, selecionando na tela do Sistema, o fornecedor convocado. O Sistema encaminhará, via chat, mensagem de convocação disponibilizando-a a todos, inclusive para a sociedade. Nesse momento o fornecedor convocado poderá encaminhar arquivo anexo, por meio do link “Anexar”, disponível apenas para o fornecedor selecionado.

9.28.1. Confirmado o envio do anexo, o link “Anexar” do fornecedor passa a ter a função de “Consultar”. Na tela do(a) Pregoeiro(a), após a convocação, o Sistema informa na coluna “Anexo” o link “Convocado”, o qual, após o envio do anexo pelo fornecedor, passa a disponibilizar o link “Consultar”.

9.28.2. Diante da indisponibilidade momentânea do campo próprio do sistema eletrônico, o licitante, excepcionalmente, poderá remeter pelo e-mail selic.protocolo@gmail.com, dentro do prazo estabelecido.

9.29. Incumbirá o Licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema ou de sua desconexão.

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

10. DO JULGAMENTO DAS PROPOSTAS E DA ACEITABILIDADE

10.1. O julgamento das Propostas de Preços dar-se-á **conforme critério de julgamento estabelecido no preâmbulo deste edital**, observadas as especificações técnicas e os parâmetros mínimos de desempenho definidos no Edital e seus anexos.

10.2. O(A) Pregoeiro(a) realizará a verificação da conformidade da proposta provisoriamente classificada em primeiro lugar quanto à adequação ao objeto especificado e à compatibilidade do preço ou percentual de desconto, conforme critério de julgamento estabelecido no preâmbulo, em relação ao estimado pela contratação.

10.3. **O(A) Pregoeiro(a) poderá solicitar parecer do setor técnico do órgão demandante para orientar sua decisão.**

10.4. 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.

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

10.5. Será desclassificada a proposta que:

10.5.1. Não atender às especificações técnicas previstas neste edital e seus anexos;

10.5.2. Permanecer, após a etapa de negociação, com preço acima do orçamento estimado para a contratação ou com o percentual abaixo ao estimado para a contratação;

10.5.3. Apresentar desconformidade insanável com quaisquer outras exigências do edital;

10.5.4. Apresentar preço manifestamente inexequível.

10.5.4.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

10.5.5. Não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

10.6. Considera-se indícios de inexequibilidade da proposta:

10.6.1. em serviços de engenharia, valores inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração Pública; e

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

10.7. O(A) Pregoeiro(a) por meio de diligência, deverá conferir ao licitante a oportunidade de demonstrar a exequibilidade de sua proposta.

10.7.1. A inexequibilidade, só ficará comprovada quando, cumulativamente:

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

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

10.8. Em sede de diligência, somente será possível a aceitação de novos documentos quando:

10.8.1. necessários para complementar informações acerca dos documentos já apresentados pelo licitante e que se refiram a fato já existente à época da abertura do certame;

10.8.2. destinados à atualização de documentos vencidos após a data de recebimento das propostas.

10.9. O(A) Pregoeiro(a), por meio de diligência, poderá encaminhar o processo para o órgão ou entidade demandante para que se manifeste a respeito da exequibilidade da proposta.

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

10.11. Quando o licitante provisoriamente classificado em primeiro lugar for desclassificado, o(a) Pregoeiro(a) convocará os demais licitantes, na ordem de classificação, para negociação.

10.12. Nos itens não exclusivos para a participação de microempresas, empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o(a) Pregoeiro(a) passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da Lei Complementar Federal n.º 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

10.13. Encerrada a análise quanto à aceitação da proposta, o(a) Pregoeiro(a) verificará a habilitação do licitante, observado o disposto neste Edital.

11. DA HABILITAÇÃO

11.1. A habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e qualificação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 26 de abril de 2018.

11.2. A verificação no SICAF ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante classificado em primeiro lugar.

11.3. As empresas licitantes deverão apresentar a seguinte documentação relativa à Habilitação Jurídica, à Regularidade Fiscal e Trabalhista, Qualificação Econômico-Financeira, Qualificação Técnica:

11.3.1. Habilitação Jurídica

a) Contrato social ou instrumento equivalente.

11.3.2. Regularidade Fiscal e Trabalhista

a) Prova de regularidade com a Fazenda Federal e Seguridade Social (Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União);

b) Prova de regularidade com a Fazenda Estadual e Municipal, do domicílio ou sede do licitante, na forma da lei

c) Certidão Negativa ou Certidão Positiva com efeitos Negativa da Dívida Ativa do Estado.

d) Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço (FGTS) demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei; e

e) Certidão Negativa de Débitos Trabalhistas - CNDT, ou Certidão Positiva com efeitos de Negativa, relativos a débitos inadimplidos perante a Justiça do Trabalho.

11.3.3.

Qualificação Econômico-Financeira

a) Certidão negativa de falência, concordata, recuperação judicial ou Certidão Negativa de Ação Cível em que não conste ação de falência/recuperação judicial/concordata/extrajudicial expedida pelo cartório distribuidor da sede da pessoa jurídica, **EXCETO quando autorizada judicialmente ou quando estiver com plano de recuperação aprovado e homologado**

b) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações **contábeis dos 2 (dois) últimos exercícios sociais**, conforme estabelece o [Art. 69 da Lei 14.133/2021](#).

b.1) O último exercício social para o registro dos balanços nos órgãos competentes será aquele estabelecido no art. 1.078 do Código Civil Brasileiro, qual seja, **30 de abril do ano seguinte**. Tal prazo, não se aplica as empresas que utilizam o Sistema Público de Escrituração Digital – SPED, que será até o último dia útil do mês de maio do ano seguinte.

c) O licitante deverá comprovar através seu balanço do último exercício social, que possui patrimônio líquido igual ou superior a XX% (XXXXXX) do valor estimado da contratação, na forma da lei, de acordo com o [§4º do art. 69 da Lei nº 14.133/2021](#).

11.3.4.

Qualificação Técnica

a) **Atestado de capacidade técnica**, expedido por pessoas jurídicas de direito público ou privado, que comprovem ter o licitante fornecido satisfatoriamente os bens ou serviços pertinentes e compatíveis com o objeto desta licitação. Podendo ser exigido da proposta melhor classificada, em diligência, que apresente cópia autenticada do contrato da prestação do serviço ou da nota fiscal, que deram origem ao Atestado.

b) **E demais exigências solicitadas no Termo de Referência - Anexo I, do edital. ITEM 15.**

11.4.

A verificação pelo(a) Pregoeiro(a), em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

11.5.

Os documentos exigidos para habilitação que não estejam contemplados no Sicaf e documentos complementares (quando for o acaso) serão enviados por meio do sistema, em formato digital, no prazo mínimo de **2 (duas) horas**, contado da solicitação do(a) Pregoeiro(a), **sob pena de inabilitação**.

11.5.1.

O prazo de que trata o item anterior poderá ser prorrogado por igual período, antes do término do prazo originalmente previsto, mediante solicitação do licitante através do chat no sistema eletrônico ou através do e-mail: selic.protocolo@gmail.com, a critério do(a) Pregoeiro(a).

11.5.2.

Para tanto, o(a) Pregoeiro(a) fará uso da opção “**Convocar Anexo**”, selecionando na tela do Sistema, o fornecedor convocado. O Sistema encaminhará, via chat, mensagem de convocação disponibilizando-a a todos, inclusive para a sociedade. Nesse momento o fornecedor convocado poderá encaminhar arquivo anexo, por meio do link “Anexar”, disponível apenas para o fornecedor selecionado.

11.5.3.

Confirmado o envio do anexo, o link “Anexar” do fornecedor passa a ter a função de “Consultar”. Na tela do(a) Pregoeiro(a), após a convocação, o Sistema informa na coluna “Anexo” o link “Convocado”, o qual, após o envio do anexo pelo fornecedor, passa a disponibilizar o link “Consultar”.

11.5.4.

Diante da indisponibilidade momentânea do campo próprio do sistema eletrônico, o licitante, excepcionalmente, poderá remeter pelo e-mail selic.protocolo@gmail.com, dentro do prazo estabelecido.

11.6.

Incumbirá ao licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema ou de sua desconexão.

11.7.

Se o prazo de validade das certidões não estiver expresso, será considerado o prazo de 90 (noventa) dias consecutivos, excluindo-se nesta contagem o dia da emissão/expedição (o primeiro dia na contagem do prazo é o seguinte à sua emissão).

11.8.

A comprovação de regularidade fiscal e trabalhista das MEs e das EPPs será exigida nos termos do disposto no Decreto Federal nº 8.538, de 6 de outubro de 2015, ou de outro que vier a substituí-lo.

11.9.

Na hipótese de haver alguma restrição relativa à regularidade fiscal e trabalhista, será assegurado **prazo de cinco dias úteis, prorrogável por igual período**, para a regularização da documentação, sob pena de inabilitação.

11.10.

Quando permitida a participação de empresas estrangeiras na licitação, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados com tradução livre.

11.10.1.

Na hipótese de o licitante vencedor ser estrangeiro, para fins de assinatura do contrato ou da ata de registro de preços ou de aceitação ou retirada de instrumento equivalente, os documentos de que trata o item acima serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto Federal nº 8.660, de 29 de janeiro de 2016, ou de outro que vier a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

11.11.

O(A) Pregoeiro(a) poderá solicitar parecer do setor técnico do órgão demandante para orientar sua decisão.

11.12. A documentação de habilitação poderá ser apresentada em versão original ou por cópia simples, por meio do sistema eletrônico.

11.13. 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.

11.14. Na hipótese de o licitante não atender às exigências de habilitação, o(a) Pregoeiro(a) examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital de licitação.

11.15. Constatado o atendimento às exigências estabelecidas no edital, o(a) Pregoeiro(a) declarará o(s) licitantes(s) habilitado(s) e vencedor(es) do(s) respectivo(s) item(ns) ou lote(s) do certame.

11.16. A indicação do vencedor, e demais informações relativas à sessão pública do Pregão constarão de ata divulgada no Sistema eletrônico, sem prejuízo das demais formas de publicidade prevista na legislação pertinente.

12. DO SANEAMENTO DA PROPOSTA E DA HABILITAÇÃO

12.1. Durante as fases de julgamento e de habilitação, o(a) Pregoeiro(a), mediante decisão fundamentada, poderá realizar diligências para sanear erros ou falhas que não alterem a substância das propostas e a validade jurídica dos documentos de habilitação.

12.1.1. A diligência deverá ser registrada em ata acessível aos licitantes.

12.2. Será vedada a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

I - complementação de informações ou esclarecimentos adicionais acerca dos documentos já apresentados pelos licitantes;

II - atualização de documentos cuja validade tenha expirado; e

III - comprovação de situação fática preexistente à época da abertura do certame.

12.3. Para os fins do disposto no inciso III do item acima, será admitida a juntada de certidão ou atestado não anexados à documentação originalmente apresentada, desde que tenham data anterior à abertura do certame ou se refiram inequivocamente à condição adquirida pelo licitante antes da abertura do certame.

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

12.5. A realização de diligências não conferirá ao licitante novo prazo ou oportunidade de obter condição ou requisito que antes não detinha, nem autorizará o(a) Pregoeiro(a) a fazer exigências novas não previstas no edital.

12.6. Na hipótese de necessidade de envio de documentos complementares à proposta e à habilitação, os documentos deverão ser apresentados em formato digital, no prazo mínimo de **02 (duas) horas**, a contar da solicitação do(a) Pregoeiro(a).

12.6.1. O prazo de que trata o item anterior poderá ser prorrogado por igual período, antes do término do prazo originalmente previsto, mediante solicitação do licitante através do chat no sistema eletrônico ou através do e-mail: selic.protocolo@gmail.com, a critério do(a) Pregoeiro(a).

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

12.8. Quando todos os licitantes forem desclassificados ou inabilitados, a Administração Pública poderá fixar o prazo de até 08 (oito) dias úteis para a apresentação de novas propostas escoimadas das causas de desclassificação ou inabilitação.

13. DOS RECURSOS

13.1. Do julgamento das propostas e da decisão de habilitação ou inabilitação, qualquer licitante poderá, de forma imediata e motivada, explicitando sucintamente suas razões, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, **em campo próprio do sistema eletrônico, no prazo não inferior a 20 (vinte) minutos**, manifestar sua intenção de recorrer, **sob pena de preclusão**.

13.1.1. O prazo para manifestação concedida no subitem anterior será de no mínimo 10 (dez) minutos por fase (proposta e habilitação).

13.2. A apresentação das razões recursais deverá ser feita no prazo de **03 (três) dias úteis contados do dia útil subsequente, inclusive, à data de manifestação da intenção de recorrer**, ficando os demais licitantes, desde logo, intimados para apresentar contrarrazões em igual prazo, que começará a contar do dia útil subsequente, inclusive, ao término do prazo do recorrente, sendo-lhes assegurada vista imediata das razões.

13.3. A apreciação se dará em fase única; e

13.4. Os efeitos do ato ou da decisão recorrida ficarão suspensos até a decisão final da autoridade competente.

13.5. Quando houver a inversão de fases de que trata o art. 141 do Decreto Estadual nº. 11.363 de 22/11/2023, a fase recursal ocorrerá em duas etapas, observando-se as seguintes disposições específicas, sem prejuízo das regras gerais previstas no caput:

13.5.1. intenção de recorrer deverá ser manifestada imediatamente após a fase de habilitação e após a fase de julgamento, conforme o caso; e

13.5.2. a apreciação dar-se-á em duas fases, após a fase de habilitação e após a fase de julgamento, a partir da declaração do licitante vencedor, conforme o caso.

13.6. O recurso será dirigido ao(a) Pregoeiro(a), que, se não reconsiderar o ato ou a decisão no prazo de 03 (três) dias úteis, encaminhará o recurso, com a sua motivação, à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis contados do recebimento do processo.

13.7. A decisão do recurso deverá ser divulgada no sistema eletrônico.

13.8. O acolhimento do recurso implicará invalidação apenas de ato insuscetível de aproveitamento.

13.9. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

14. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

14.1. Encerradas as fases de julgamento e habilitação, e esgotados os recursos administrativos, o processo licitatório será encaminhado à autoridade superior do órgão ou entidade demandante, que poderá:

14.1.1. determinar o retorno do processo para saneamento de eventuais irregularidades;

14.1.2. revogar a licitação por motivo superveniente de conveniência e oportunidade;

14.1.3. anular a licitação, de ofício ou mediante provocação de terceiros, sempre que verificada ilegalidade insanável; e

14.1.4. adjudicar o objeto, no caso de recurso sem o juízo de retratação, e homologar a licitação.

15. DA FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇO E DO CADASTRO DE RESERVA

15.1. Após a homologação da licitação, deverão ser observadas as seguintes condições para a formalização da ata de registro de preços:

15.1.1. Serão registrados na ata de registro de preços os preços e os quantitativos do adjudicatário, observando-se o disposto no inciso V do caput do art. 319 do Decreto Estadual nº. 11.363 de 22/11/2023.

15.1.2. Será incluído na ata de registro de preços, na forma de anexo, o registro:

a) dos licitantes ou dos fornecedores que aceitarem cotar os bens, obras ou serviços com preços iguais aos do adjudicatário, observando-se a classificação na licitação; e

b) dos licitantes ou fornecedores que mantiverem sua proposta original.

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

15.2. O registro de que trata o item 15.1.2 tem por objetivo a formação de cadastro de reserva, para o caso de impossibilidade de atendimento pelo signatário da ata de registro de preços.

15.3. Para fins da ordem de classificação, os licitantes ou fornecedores de que trata a alínea “a” do item 15.1.2, antecederão aqueles de que trata a alínea “b” do referido item.

15.4. A habilitação dos licitantes que comporão o cadastro de reserva de que tratam o item 15.1.2 e o item 15.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

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

15.4.2. Quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 331 e art. 332 do Decreto Estadual nº. 11.363 de 22/11/2023.

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

15.6. 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:

15.6.1. 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

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

16. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃOS OU ENTIDADES NÃO PARTICIPANTES

16.1. Poderá utilizar-se da Ata de Registro de Preços, durante sua vigência, por qualquer órgão ou entidade da Administração Pública, inclusive empresas estatais que não figurem no rol de órgãos e entidades participantes, mediante anuência expressa do órgão ou entidade gerenciadora e da detentora, atendidos os limites do art. 336 e as demais condições previstas no Decreto Estadual nº. 11.363 de 22/11/2023.

DA PARTICIPAÇÃO DE CONSÓRCIO

17.1. **Não** será permitido participação de empresas sob a forma de consórcio, conforme está disposto no Termo de Referência - Anexo I do Edital.

18. DA PARTICIPAÇÃO DE COOPERATIVAS

18.1. Não se aplica.

19. DA SUBCONTRATAÇÃO

19.1. **Não** será permitido a subcontratação, conforme está disposto no Termo de Referência - Anexo I do Edital

20. DOS PRAZOS E CONDIÇÕES PARA A ENTREGA DO OBJETO

20.1. Será conforme disposto no Anexo I deste Edital.

21. DAS FORMAS, CONDIÇÕES, PRAZOS DE PAGAMENTO, E CRITÉRIO DE REAJUSTAMENTO DO PREÇO

21.1. Será conforme disposto no Anexo I deste Edital.

22. DA GARANTIA DE EXECUÇÃO CONTRATUAL

22.1. **Haverá** garantia de execução contratual, conforme disposto no Anexo I deste Edital

23. DO TERMO DE CONTRATO

23.1. Será conforme disposto no Anexo I deste Edital.

24. DA FISCALIZAÇÃO E GESTÃO DO CONTRATO

24.1. Será conforme disposto no Anexo I e/ou Anexo III deste Edital.

25. DA DOTAÇÃO ORÇAMENTÁRIA

25.1. Será conforme os termos constantes do Anexo I deste Edital.

26. DAS SANÇÕES ADMINISTRATIVAS

26.1. As licitantes estarão sujeitas às sanções administrativas previstas nos [arts. 155 à 163 da Lei n.º 14.133/2021](#), e às demais cominações legais, resguardado o direito ao contraditório e à ampla defesa.

26.2. Na hipótese de abertura de processo administrativo destinado à apuração de fatos e, se for o caso, aplicação de sanções à licitante, em decorrência de conduta vedada neste Pregão, as comunicações à licitante serão efetuadas através do endereço eletrônico (e-mail) indicado em sua proposta.

26.3. Sem prejuízo das sanções previstas neste edital e seus anexos, os atos lesivos à Administração Pública previstos no inciso IV, do art. 5º, da Lei nº 12.846/2013, sujeitarão os infratores às penalidades previstas na referida lei.

27. DAS DISPOSIÇÕES GERAIS

27.1. As normas que disciplinam este procedimento 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.

27.2. Aos casos omissos aplicar-se-ão as demais disposições constantes da Lei nº 14.133/21, com suas posteriores alterações e legislação correlata.

27.3. A realização da licitação não implica necessariamente a contratação total ou parcial do montante previsto, porquanto estimado, podendo o órgão demandante, inclusive, revogá-la, total ou parcialmente, por fatos supervenientes, de interesse público, ou anulá-la por ilegalidade, de ofício ou por provocação de terceiros, mediante manifestação escrita e fundamentada, assegurado o contraditório e a ampla defesa, conforme dispõe o [art. 71 da Lei Federal n.º 14.133, de 2021](#).

27.4. A autoridade superior do órgão ou entidade demandante poderá revogar o processo licitatório por motivo de conveniência e oportunidade, e deverá anular o processo licitatório por ilegalidade insanável, por meio de ato escrito e fundamentado, conforme estabelece no [Art. 250 do Decreto Estadual nº. 11.363 de 22/11/2023](#).

27.5. Os licitantes não terão direito à indenização em decorrência da revogação ou da anulação do processo licitatório, conforme dispõe o [Art. 250 do Decreto Estadual nº. 11.363 de 22/11/2023](#).

27.6. A homologação do resultado desta licitação não implicará direito à contratação do objeto pelo órgão demandante.

27.7. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local estabelecidos no preâmbulo deste Edital, desde que não haja comunicação do(a) Pregoeiro(a) em contrário.

27.8. Todas as referências de tempo estabelecidas no edital, nos avisos e durante a sessão pública observarão, para todos os efeitos, o horário de Brasília - Distrito Federal, inclusive para contagem de tempo e registro no sistema de compras adotado pelo Poder Executivo do Estado do Acre e na documentação relativa ao certame.

27.9. Eventuais modificações no edital de licitação implicarão nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto se, inquestionavelmente, a alteração não comprometer a formulação das propostas, resguardado o tratamento isonômico aos licitantes.

27.10. 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

27.11. Será facultado ao(a) Pregoeiro(a), em qualquer fase da licitação, desde que não seja alterada a substância da proposta, adotar medidas de saneamento destinadas a esclarecer informações, corrigir impropriedades na documentação de habilitação, da proposta, ou complementar a instrução do processo.

27.12. As Licitantes são responsáveis pela fidelidade e legitimidade das informações, declarações e dos documentos apresentados em qualquer fase da licitação.

27.13. O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que sejam possíveis a aferição da sua qualificação, conforme dispõe o [art. 12 da Lei Federal nº 14.133/2021](#).

27.14. Os prazos previstos nesta Lei serão contados com exclusão do dia do começo e inclusão do dia do vencimento e observarão as disposições previstas no [art. 183 da Lei Federal nº 14.133/2021](#).

27.15. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e nos sítios <http://www.gov.br/compras/pt-br/>, <http://www.licitacao.ac.gov.br>, e ainda no Portal de Licitações do Tribunal de Contas do Estado do Acre - LICON.

27.16. O resultado desta licitação poderá ser consultado nos sítios <http://www.gov.br/compras/pt-br/> e/ou <http://www.licitacao.ac.gov.br>.

27.17. Quaisquer informações complementares sobre o presente Edital e seus Anexos poderão ser obtidas pelo telefone (68) 3215-4600 ou através de e-mail selic.protocolo@gmail.com.

27.18. O Foro para dirimir os possíveis litígios que decorrerem do presente procedimento licitatório será o do foro da comarca, de Rio Branco - AC.

Rio Branco - AC, 13 Janeiro de 2026.

Elaborado por:

Antonia Jucilene Oliveira de Moraes
Divisão de Conformidade e Elaboração de Editais- DIVCON



Documento assinado eletronicamente por **ANTONIA JUCILENE OLIVEIRA DE MORAIS, Chefe(a) de Divisão**, em 13/01/2026, às 10:07, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0019007720** e o código CRC **1D36A901**.

TERMO DE REFERÊNCIA Nº 65/2025/SEFAZ - DIPROJ

Processo nº 0715.007435.00055/2025-41

SUMÁRIO

1. OBJETO E CONDIÇÕES GERAIS DA

CONTRATAÇÃO1.1. Objeto1.2. Características Gerais1.3. Classificação do Objeto

quanto à Heterogeneidade ou Complexidade1.4 Classificação do Objeto quanto ao

Modelo de Execução1.5. Do Prazo de Vigência2. ÓRGÃO RESPONSÁVEL E

PARCIPANTE DO REGISTRO DE PREÇOS3. FUNDAMENTAÇÃO DA

CONTRATAÇÃO3.1. Contexto Local3.2. Contexto Global dos Ataques

Cibernéticos3.3. Panorama no Brasil - Evolução dos Ataques de 2019 a

20253.4. Ataques Cibernéticos no Setor Governamental Brasileiro3.5. O uso de

Inteligência Artificial nos Ataques Cibernéticos3.6. Impactos Econômicos no Setor

Público e Privado3.7. Da Fragilidade à Resiliência: Um Projeto para a Segurança

Cibernética da SEFAZ/AC3.8. Objetivos da Contratação3.9. Resultados

Esperados4. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO4.1. Do

Plano de Contratações Anual4.2. Alinhamento Estratégico4.3. Normativos que

Fundamentam a Contratação5. DOS CRITÉRIOS DE AGRUPAMENTO DE ITENS

Em LOTE ÚNICO5.1. Fundamento Legal5.2. Justificativa Técnica6. JUSTIFICATIVA

DO REGISTRO DE PREÇOS7. DESCRIÇÃO DA SOLUÇÃO COMO UM

TODO7.1. Descrição da Solução7.2. Da opção por FORTISIEM como Solução para

Gerenciamento e Correção de Eventos8. REQUISITOS DA

CONTRATAÇÃO8.1. Requisitos de Negócio8.2. Requisitos de

Manutenção8.3. Requisitos Tecnológicos8.4. Requisitos Técnicos

Específicos8.5. Requisitos de Formação da Equipe e Experiência

Profissional8.6. Requisitos Temporais9. OUTROS REQUISITOS DA

CONTRATAÇÃO9.1. Subcontratação9.2. Requisitos Legais9.3. Vistoria9.4. Garantia

de Execução Contratual9.5. Requisitos de Segurança da Informação e

Privacidade9.6. Indicação de Marca ou Modelo9.7. Requisitos de Segurança

Institucional e Procedimental9.8. Requisitos Ambientais10. DAS

RESPONSABILIDADES10.1. Deveres e Responsabilidade do

CONTRATANTE10.2. Deveres e Responsabilidades da CONTRATADA11. MODELO

DE EXECUÇÃO DO OBJETO11.1. Reunião Inicial11.2. Mecanismos Formais de

Comunicação11.3. Procedimentos de Encaminhamento e Controle de

Solicitações11.4. Prazos, Horários da Prestação dos Serviços11.5. Locais de

Entrega11.6. Manutenção de Sigilo e Segurança11.7. Auditoria, Relatórios e

Revisões11.8. Continuidade contratual12. MODELO DE GESTÃO DO

CONTRATO12.1 Princípios Gerais e Execução12.2. Fiscal do Contrato12.3 Gestor do

Contrato12.4. Avaliação de Resultados e Níveis de Serviço12.5 Encerramento

Contratual13. CRITÉRIOS DE PAGAMENTO13.1. Do Pagamento13.2. Do

Preço13.3. Do Equilíbrio Econômico-Financeiro14. FORMA DE SELEÇÃO DO

FORNECEDOR14.1. Da Modalidade e Critério de Julgamento14.2. Da Escolha do

Pregão Eletrônico14.3. Do Prazo de Validade da Proposta14.4. Do Prazo para

Assinatura do Contrato15. QUALIFICAÇÃO TÉCNICA DO

LICITANTE15.1. Atestado de Capacidade Técnica15.2 Certificações de

Mercado16. QUALIFICAÇÃO TÉCNICA PARA EXECUÇÃO DO

CONTRATO17. DA PARTICIPAÇÃO DE CONSÓRCIOS18. ATA DE REGISTRO DE

PREÇOS18.1. Assinatura18.2. Vigência18.3. Alteração ou atualização dos preços

registrados18.4. Da Adesão e Obrigações do Órgão Gerenciador/Detentor da Ata19. DA

ADEQUAÇÃO

ORÇAMENTÁRIA20. RESPONSABILIDADES21. ANEXOS21.1. Anexo I -

Especificações Técnicas Mínimas dos Componentes21.2. Anexo II - Modelo de Termo

de Confidencialidade21.3. Anexo III - Modelo de Declaração de Vistoria

APRESENTAÇÃO

O objeto desta contratação possui características comuns e padronizadas pelo mercado, sendo a descrição e os padrões de desempenho e qualidade possíveis de definir no Edital e no Termo de Referência, de maneira objetiva e suficientemente exaustiva e clara, a ponto de não suscitar dúvidas acerca das especificações do objeto pretendido, sendo caracterizado como serviços comuns e de natureza contínua, conforme previsto no *art. 6º, incisos XIII e XV da Lei nº 14.133/2021*.

O Termo de Referência atende o previsto no *art. 6º, inciso XXIII da Lei 14.133/21* e *art. 96 do Decreto Estadual nº 11.363/2023*.

O Departamento de Tecnologia da Informação - DETI é a unidade administrativa responsável pelas informações e elaboração deste Termo de Referência.

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Objeto

1.1.1. Contratação de empresa especializada para **prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS (Software as a Service), com o fornecimento das respectivas soluções de software e serviços técnicos especializados, visando atender às demandas da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC),** nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

1.1.2. **Tabela 1.** A solução de serviços deverá contemplar os seguintes componentes e quantidades:

LOTE ÚNICO					
ITEM (a)	DESCRIÇÃO DO SERVIÇO (b)	UNIDADE (c)	QUANT (d)	VALOR UNITÁRIO (e)	VALOR TOTAL (f) = (d)x(e)
1	SOC – <i>Security Operations Center</i>	Mês	60		
2	Solução para Gestão de Vulnerabilidades	Mês	60		
3	Solução para Gerenciamento e Correção de Eventos de Segurança – FortiSIEM	Mês	60		
4	Solução de <i>Inteligência contra Ameaças (Threat Intelligence)</i>	Mês	60		
5	Solução para Validade de Segurança Contínua – BAS	Mês	24		
6	Solução para Gestão de Acessos Privilegiados – PAM	Mês	60		
7	Consultoria em Serviços Especializados (<i>on demand</i>)	HST	2000		
Valor Total					

Características Gerais

1.2.1. São os requisitos para a prestação de Serviços de Segurança Cibernética no ambiente da SEFAZ/AC, incluindo Serviços de Security Operations Center (SOC) e fornecimento das respectivas ferramentas:

- Serviços destinados a garantir a segurança das comunicações entre os sistemas da SEFAZ/AC;
- O monitoramento contínuo de todos os ativos de TI e sistemas, além da identificação de vulnerabilidades e a prevenção contra-ataques cibernéticos;
- Verificação de potenciais vulnerabilidades de forma a mitigar ataques e consequentemente danos;

1.2.1.1. Estes serviços possibilitarão identificar imediatamente de forma Preventiva e corretiva:

- a) Potenciais e futuros problemas e gargalos – Preventiva;
- b) Falhas que provocam degradação de desempenho e suas respectivas causas;
- c) Detecção de ameaças cibernéticas à sistemas, tais como como tentativas de invasão e/ou paralisação: páginas web, aplicativos, bases de dados etc;
- d) Solução de problemas de segurança encontrados com agilidade e eficiência;
- e) Riscos de segurança na infraestrutura de TI, através do monitoramento e análise continua dos processos.

1.2.2. Além disso, os serviços prestados atuarão em tempo real sobre todos os sistemas monitorados, com o objetivo de:

- a) Registrar e documentar todas as ocorrências, incluindo as que ameacem a segurança do ambiente de TI;
- b) Acionar os respectivos responsáveis, seja no âmbito da SEFAZ/AC, seja entre os fornecedores da contratante, para a prestação dos serviços eventualmente afetados ou para a correção das falhas identificadas;
- c) Acompanhar a resolução dos problemas e apontar as soluções e providências tomadas;
- d) Gerar documentação, por meio de relatórios, de forma a possibilitar o acompanhamento dos chamados, a verificação dos tempos de resposta em relação aos prazos contratados e a adequada gestão, pela SEFAZ/AC, da prestação dos serviços a seus públicos interno e externo.

1.2.3. Fornecedor de serviços que proporcione segurança nos sistemas da SEFAZ/AC, identificando e mitigando potenciais vulnerabilidades e ataques, pelo prazo de 60 meses, exceto item 5 (cinco) que é pelo prazo de 24 meses.

1.2.4. Para Hora de Serviço Técnico (HST) consideramos a definição constante no subitem 2.2.1, letra “h” da Portaria SGD/MGI nº 750, de 20 de março de 2023:

“2.2.1. Para os efeitos deste documento, aplicam-se os seguintes termos e definições:

(...)

*h) **Horas de Serviço Técnico (HST):** métrica baseada na quantidade de horas necessárias para se alcançar um resultado ou entregar um produto, por meio de atividades executadas por um ou mais perfis profissionais, e aferidas por meio de indicadores de níveis mínimos de serviço e critérios de aceitação previamente estabelecidos.” (Grifamos)*

1.3. Classificação do Objeto quanto à Heterogeneidade ou Complexidade

1.3.1. Os serviços objeto desta contratação possui características comuns e padronizadas pelo mercado, sendo a descrição e os padrões de desempenho e qualidade possíveis de definir no Edital e no Termo de Referência, de maneira objetiva e suficientemente exaustiva e clara, a ponto de não suscitar dúvidas acerca das especificações do objeto pretendido, sendo *caracterizado como serviços comuns*, conforme previsto no **art. 6º, inciso XIII, da Lei nº 14.133/2021**, vejamos:

“Art. 6º Para os fins desta Lei, consideram-se:

(...)

XIII – bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.” (Grifamos)

1.4. Classificação do Objeto quanto ao Modelo de Execução

1.4.1. A contratação de serviços gerenciados de segurança cibernética, abrangendo soluções especializadas de software e serviços técnicos, atende a uma necessidade administrativa de caráter permanente e estratégico. Tal demanda decorre da obrigação institucional de mitigar riscos, proteger ativos informacionais e garantir a disponibilidade contínua das funções públicas, sendo inafastável à luz dos requisitos legais e das boas práticas de governança.

1.4.2. A salvaguarda das operações e sistemas da Administração Pública transcende a mera conveniência, configurando-se como elemento essencial para a manutenção da integridade, da confiabilidade e da continuidade dos serviços prestados à sociedade, em conformidade com os princípios constitucionais da eficiência, segurança e continuidade do serviço público.

1.4.3. Assim sendo, são classificados como **serviços de natureza contínua**, uma vez que sua execução visa atender a necessidades permanentes ou prolongadas da Administração Pública, conforme disposto no **art. 6º, inciso XV, da Lei nº 14.133/2021**, *in verbis*:

“Art. 6º Para os fins desta Lei, consideram-se:

(...)

XV - serviços e fornecimentos contínuos: serviços contratados e compras realizadas pela Administração Pública para a manutenção da atividade administrativa, decorrentes de necessidades permanentes ou prolongadas;” (Grifamos)

Do Prazo de Vigência

1.5.1. O prazo de vigência da contratação para os **itens 1, 2, 3, 4, 6 e 7** será de **60 (sessenta) meses** e para o **item 5** será de **24 (vinte e quatro) meses**, contados da data da assinatura do contrato, de acordo com o que prescreve o art. 106 da Lei 14.133/21, *verbis*:

"Art. 106. A Administração poderá celebrar contratos com prazo de até 5 (cinco) anos nas hipóteses de serviços e fornecimentos contínuos, observadas as seguintes diretrizes:

I - a autoridade competente do órgão ou entidade contratante deverá atestar a maior vantagem econômica vislumbrada em razão da contratação plurianual;

II - a Administração deverá atestar, no início da contratação e de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção;

III - a Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

§ 1º A extinção mencionada no inciso III do caput deste artigo ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

§ 2º Aplica-se o disposto neste artigo ao aluguel de equipamentos e à utilização de programas de informática.

1.5.2. O contrato poderá ser prorrogável na forma do artigo 107 da Lei nº 14.133, de 2021, vejamos:

Art. 107. Os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes."

1.5.3. No período de vigência do Contrato estão incluídos todos os prazos necessários à perfeita execução do objeto nos termos pactuados entre as partes, ressalvados os casos referentes às garantias do objeto, que extrapolam o referido prazo de vigência.

2. ÓRGÃO RESPONSÁVEL E PARTICIPANTE DO REGISTRO DE PREÇOS

2.1. O órgão gerenciador será a **Secretaria de Estado da Fazenda do Acre - SEFAZ/AC**.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Contexto Local

3.1.1. A Secretaria de Estado da Fazenda do Acre enfrenta desafios críticos em segurança da informação, devido ao aumento da sofisticação e frequência das ameaças cibernéticas, que colocam em risco a integridade, confidencialidade e disponibilidade dos dados públicos e sistemas críticos, especialmente os vinculados às operações tributárias e financeiras do Estado. A infraestrutura atual é insuficiente para responder com agilidade e eficácia a esses ataques, o que pode comprometer a continuidade dos serviços públicos essenciais e a confiança da população.

3.2. Contexto Global dos Ataques Cibernéticos

3.2.1. O cenário global de ataques cibernéticos tem se tornado cada vez mais complexo e perigoso, impulsionado pela rápida digitalização da sociedade e das atividades econômicas, sociais e governamentais. A migração massiva dessas atividades para o ambiente digital cria novas oportunidades para a atuação de cibercriminosos.

3.2.2. O custo global dos crimes cibernéticos era estimado em mais de US\$ 1 trilhão em 2020 e deve alcançar US\$ 10,5 trilhões anuais até 2025, tornando o cibercrime mais lucrativo até que o tráfico internacional de drogas. A pandemia de COVID-19 e a transformação digital acelerada ampliaram a superfície de ataque, com a proliferação de dispositivos IoT, migração para a nuvem e aumento do trabalho remoto, expondo vulnerabilidades rapidamente exploradas.

3.2.3. Os ataques mais prevalentes são os de *ransomware*, *phishing* e *negação de serviço distribuído (DDoS)*, que crescem em frequência, sofisticação e impacto. Exemplos notórios incluem grupos organizados como *DarkSide* e *REvil*, sendo que incidentes como o ataque ao Colonial Pipeline, em 2021, evidenciam a ameaça à infraestrutura crítica global. Esses fatores tornam a segurança cibernética um desafio urgente, que exige respostas rápidas, integradas e tecnologia avançada para proteção eficaz das organizações públicas e privadas em todo o mundo.

3.3. Panorama no Brasil - Evolução dos Ataques de 2019 a 2025

3.3.1. Entre 2019 e 2025, o Brasil viveu um crescimento explosivo e contínuo dos ataques cibernéticos, tanto em volume quanto em sofisticação. Em 2019, foram registradas mais de 24 bilhões de tentativas de ataque, majoritariamente focadas no setor financeiro, refletindo o interesse dos cibercriminosos em redes bancárias e dados financeiros. Houve também um aumento expressivo de ataques de negação de serviço (DDoS), com crescimento de 90% em relação ao ano anterior.

3.3.2. Durante a pandemia de COVID-19, o número de tentativas de invasão cresceu ainda mais, atingindo 16,2 bilhões somente no primeiro semestre de 2021, impulsionado pela adoção em massa do trabalho remoto e maior uso de dispositivos IoT, ampliando a superfície de ataque.

3.3.3. Em 2023, o Brasil registrou cerca de 60 bilhões de tentativas de ataque, indicando uma redução quantitativa em relação a 2022, mas com um perfil qualitativamente mais sofisticado, com ameaças direcionadas e personalizadas, como variantes avançadas de ransomware e malwares propagados por arquivos do Microsoft Office.

3.3.4. No segundo e terceiro trimestres de 2024, o país enfrentou um aumento expressivo nos ataques, com picos históricos de notificações ao CERT.br, além de um crescimento de 1.801% nos ataques DDoS, prejudicando fortemente a disponibilidade dos

serviços digitais.

3.3.5. Esse cenário coloca o Brasil como um dos países mais visados da América Latina, consequência da sua importância econômica e da maturidade ainda incipiente em segurança digital em muitas organizações públicas e privadas. A combinação das vulnerabilidades estruturais com o uso crescente de inteligência artificial por cibercriminosos reforça a necessidade urgente de políticas integradas, automação e capacitação para aumentar a resiliência digital do país.

3.3.6. Hospitais, órgãos públicos, setor financeiro, PME's e outros setores enfrentam riscos significativos, tornando a segurança cibernética uma prioridade estratégica para garantir a continuidade das operações e proteger dados sensíveis.

3.4. Ataques Cibernéticos no Setor Governamental Brasileiro

3.4.1. Em 2025, o setor governamental brasileiro sofreu um aumento significativo de ataques cibernéticos, com cerca de 5 mil incidentes registrados nos primeiros seis meses, principalmente envolvendo vazamento de dados e interrupção de serviços digitais essenciais.

3.4.2. Sistemas críticos como e-CAC, Meu INSS, Conecte SUS e Carteira de Trabalho Digital foram alvos de ataques de negação de serviço distribuído (DDoS), causando instabilidades e dificultando o acesso dos cidadãos a serviços públicos fundamentais. Além disso, órgãos de inteligência e fiscalização, como Polícia Federal, Anatel e ABIN, sofreram invasões sofisticadas, muitas vezes ligadas a grupos de hacktivismo com motivações políticas e sociais.

3.4.3. O setor governamental representou 12,47% dos incidentes cibernéticos no país, sendo o segundo mais atacado após o financeiro. Este cenário reforça a necessidade urgente de investimentos estratégicos e contínuos em segurança cibernética para proteger informações estratégicas, garantir a continuidade dos serviços públicos digitais e preservar a confiança da sociedade na administração pública.

3.5. O uso de Inteligência Artificial nos Ataques Cibernéticos

3.5.1. A Inteligência Artificial (IA) tem revolucionado o cenário da segurança digital, sendo utilizada tanto para defesa quanto para a intensificação dos ataques cibernéticos. Cibercriminosos fazem uso da IA para aumentar a eficiência, rapidez e escala das suas ações maliciosas, tornando esses ataques mais sofisticados e difíceis de combater.

3.5.2. Em 2024, ataques baseados em IA deixaram de ser exceção e passaram a integrar grandes campanhas maliciosas, incluindo manipulação de informações por meio de deepfakes e campanhas de desinformação que ameaçam processos democráticos e a confiança social. A IA também aprimora ataques que roubam informações sensíveis, como *infostealers*, e torna o *ransomware* mais perigoso ao combinar criptografia com exfiltração de dados para extorsão.

3.5.3. Além disso, a IA automatiza a exploração de vulnerabilidades em dispositivos de borda (IoT, câmeras, roteadores) e em cadeias de suprimento completas, aumentando a velocidade e o alcance dos ataques. No entanto, a IA também é uma ferramenta valiosa para a defesa, sendo aplicada em monitoramento comportamental e automação de respostas para identificar e mitigar ameaças emergentes.

3.5.4. No contexto brasileiro e da América Latina, a preocupação com ataques impulsionados por IA cresce rapidamente, dada a vulnerabilidade causada pela digitalização acelerada e falta de maturidade em segurança. Apesar dos desafios, a maioria dos líderes do setor acredita que a IA será fundamental para fortalecer a defesa cibernética contra essas novas ameaças.

3.5.5. Em suma, a IA representa um ponto de inflexão na segurança digital, exigindo esforços proativos e integrados para enfrentar ataques cada vez mais evoluídos.

3.6. Impactos Econômicos no Setor Público e Privado

3.6.1. Os ataques cibernéticos geram perdas econômicas significativas tanto para o setor privado quanto para o setor público no Brasil. Estima-se que até 2028 as empresas brasileiras possam acumular prejuízos em torno de R\$ 2,2 trilhões, afetando especialmente médias e grandes organizações nos setores financeiro, varejo e indústria. Cerca de 48% das empresas serão vítimas de invasões de alto impacto que podem causar interrupções operacionais e vazamentos de dados críticos, comprometendo a sustentabilidade e competitividade dos negócios.

3.6.2. As perdas econômicas envolvem danos diretos, como roubos financeiros e extorsão via *ransomware*, além de perdas indiretas, como redução da produtividade, custos para recuperação e multas por não conformidade com regulamentos, além de prejuízos à reputação institucional. O setor público também enfrenta vulnerabilidades, evidenciadas por incidentes recentes, como o ataque de *ransomware* à prefeitura de Anitápolis (SC), com prejuízo direto de R\$ 1,6 milhão, e ataques ao setor financeiro, que causaram prejuízos estimados em cerca de R\$ 800 milhões.

3.6.3. Pequenas e médias empresas (PMEs) são particularmente afetadas, acumulando perdas superiores a R\$ 1 trilhão em 2024, impactando mais de um milhão de empregos. O investimento em cibersegurança, por sua vez, pode gerar impactos positivos na economia, criando empregos e aumentando renda. Contudo, a ausência de políticas públicas robustas e a baixa maturidade em segurança aumentam a exposição a riscos. Portanto, a integração entre governo e iniciativa privada e o investimento em estratégias avançadas de segurança são fundamentais para mitigar perdas econômicas e garantir a continuidade dos serviços essenciais no país.

3.7. Da Fragilidade à Resiliência: Um Projeto para a Segurança Cibernética da SEFAZ/AC

"Essa abordagem robusta e preventiva não deve ser vista como custo, mas como um investimento indispensável para a sustentabilidade operacional e a segurança institucional da SEFAZ/AC na era digital."

3.7.1. A presente iniciativa tem como finalidade prover a Secretaria de Estado da Fazenda do Acre (SEFAZ/AC) de serviços técnicos especializados em segurança da informação, indispensáveis para assegurar a continuidade operacional e a confiabilidade dos sistemas de Tecnologia da Informação e Comunicação (TIC). O objetivo é fortalecer a capacidade de prevenção, detecção e contenção

de incidentes, garantindo a integridade, a confidencialidade e a disponibilidade dos dados que sustentam as atividades estratégicas da instituição.

3.7.2. A infraestrutura tecnológica da SEFAZ/AC é composta por diversos ativos críticos, que incluem soluções de segurança, redes de comunicação, sistemas de telefonia, servidores, bancos de dados, plataformas de backup e mecanismos de armazenamento de informações. Dada a relevância dos sistemas hospedados, esses componentes precisam operar em condições de alta disponibilidade e apresentar resiliência frente a falhas ou tentativas de ataque. A intensificação do uso de recursos digitais e o crescimento do volume de informações tornam a proteção dos dados um elemento central da governança institucional e da continuidade dos serviços públicos.

3.7.3. O cenário nacional de segurança cibernética em 2025 reforça a urgência dessa iniciativa. O setor público brasileiro experimenta uma escalada de ataques e incidentes digitais, com centenas de milhares de alertas registrados apenas no primeiro semestre do ano, abrangendo desde tentativas de força bruta e disseminação de malwares até ataques de negação de serviço e invasões persistentes direcionadas. O próprio Supremo Tribunal Federal contabilizou mais de 750 milhões de tentativas de ataque até julho de 2025, evidenciando que órgãos governamentais se tornaram alvos prioritários pela criticidade e sensibilidade das informações sob sua guarda.

3.7.4. Nesse contexto, a SEFAZ enfrenta riscos estratégicos que transcendem a dimensão tecnológica, e podem afetar diretamente a arrecadação fiscal, a prestação de serviços públicos essenciais e a confiança da sociedade na gestão financeira do Estado. Tais riscos demandam ações coordenadas de prevenção, detecção e resposta a incidentes de segurança, em alinhamento às determinações do Tribunal de Contas da União, que, por meio do Acórdão nº 4.035/2020-Plenário, destacou a necessidade de aprimorar a governança da segurança da informação na Administração Pública, com clara definição de responsabilidades e implementação de controles preventivos e corretivos.

3.7.5. A complexidade crescente das infraestruturas digitais, conjugada ao surgimento contínuo de novas ameaças, impõe à Secretaria a adoção de soluções tecnológicas avançadas e a formação de equipes especializadas capazes de operar em regime ininterrupto. O uso combinado de monitoramento contínuo, análise de comportamento e automação de respostas possibilita maior agilidade na identificação de anomalias e na contenção de incidentes, reduzindo impactos sobre os serviços públicos e fortalecendo a postura institucional diante de ameaças.

3.7.6. Considerando a escassez de profissionais com formação específica na Administração Pública e a necessidade de atuação permanente frente ao ambiente cibernético atual, a contratação de serviços gerenciados de segurança da informação surge como alternativa estratégica. Tais serviços combinam tecnologias avançadas com operação 24 horas por dia, oferecendo capacidade ampliada de monitoramento, correlação de eventos e resposta rápida a incidentes, fatores que contribuem para a elevação do nível geral de segurança da Secretaria.

3.7.7. Dessa forma, o investimento em segurança cibernética deve ser compreendido não como um custo adicional, mas como um componente essencial para a sustentabilidade institucional, a continuidade dos serviços digitais e a proteção dos ativos informacionais do Estado. A consolidação de uma postura resiliente representa passo decisivo para transformar vulnerabilidades em capacidade estratégica de defesa e garantir maior confiança dos cidadãos e parceiros na atuação da SEFAZ/AC na era digital.

3.8. Objetivos da Contratação

3.8.1. A contratação de empresa especializada para prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS, com fornecimento das soluções de software e serviços técnicos especializados, é uma medida imprescindível e estratégica e tem como objetivo principal fortalecer a segurança cibernética da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC).

3.8.2. Diante do cenário crítico e dinâmico das ameaças digitais, esse investimento é vital para:

- a) Garantir a proteção robusta dos ativos digitais e dados sensíveis da SEFAZ/AC;
- b) Assegurar a continuidade e a integridade dos serviços públicos essenciais oferecidos à sociedade;
- c) Mitigar riscos operacionais, financeiros, legais e reputacionais decorrentes de incidentes cibernéticos;
- d) Alinhar a segurança digital com as melhores práticas internacionais e regulamentos específicos, como a LGPD;
- e) Otimizar recursos e capacidades técnicas, através da mão de obra especializada e da adoção de tecnologia avançada;
- f) Fortalecer a resiliência institucional frente à evolução constante das técnicas de ataque e vulnerabilidades.

3.9. Resultados Esperados

3.9.1. A implantação de serviços gerenciados de segurança cibernética proporcionará à SEFAZ/AC uma série de benefícios estratégicos, operacionais e tecnológicos, fundamentais para a proteção dos ativos digitais e a continuidade dos serviços públicos. Os principais benefícios incluem:

- a) **Monitoramento Contínuo e Resposta Imediata:** Atuação em tempo real para identificar e responder a ameaças cibernéticas, reduzindo o tempo de resposta e os impactos de incidentes, por meio de um SOC ativo e integrado.
- b) **Redução da Superfície de Ataque:** Proteção abrangente de ambientes híbridos, dispositivos IoT, sistemas em nuvem e recursos utilizados em trabalho remoto, reduzindo significativamente os pontos vulneráveis à exploração por agentes maliciosos.
- c) **Conformidade Regulatória e Governança:** Atendimento às exigências legais, como a LGPD, com políticas robustas de controle de acesso, gestão de identidade e rastreabilidade, fortalecendo a governança digital e mitigando riscos legais.

d) **Eficiência Operacional e Otimização de Recursos:** Liberação da equipe interna de TI para atividades estratégicas, enquanto especialistas externos assumem o monitoramento e resposta a incidentes. O modelo SaaS garante escalabilidade, atualização tecnológica contínua e previsibilidade de custos.

e) **Fortalecimento da Resiliência Institucional:** Capacidade de manter operações críticas mesmo diante de ataques sofisticados, como ransomware com exfiltração de dados, protegendo os sistemas, a arrecadação estadual e os serviços à população.

f) **Inteligência Cibernética e Prevenção:** Uso de inteligência artificial e análise comportamental para antecipar ameaças e automatizar respostas, elevando o nível de maturidade em segurança cibernética da instituição.

g) **Impacto Econômico Positivo:** Prevenção de perdas financeiras diretas e indiretas, como interrupções de serviços, multas por não conformidade e danos à imagem institucional, contribuindo para a sustentabilidade da SEFAZ/AC.

3.9.2. Portanto, esta contratação não apenas responde às demandas atuais de segurança da Secretaria, mas também projeta sua capacidade de adaptação e proteção contínua num ambiente tecnológico em rápida transformação, promovendo eficiência, transparência e segurança jurídica na gestão pública do Estado do Acre.

4. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO INSTITUCIONAIS

4.1. Do Plano de Contratações Anual

4.1.1. A contratação encontra-se contemplada no Plano de Contratação Anual da Secretaria de Estado da Fazenda (0715.012462.00176/2024-88) para o ano corrente, conforme previsto item **3.6 – Serviços de TI - Segurança Cibernética (SOC E Ferramentas)**.

4.1.2. A inclusão da demanda no Plano Anual de Contratações evidencia a aderência da contratação à programação orçamentária e ao planejamento administrativo da Secretaria, em conformidade com o disposto no inciso II do § 1º do art. 18 e no art. 12, inciso VII, da Lei 14.133/2021.

4.2. Alinhamento Estratégico

4.2.1. A presente contratação está alinhada com os objetivos estratégicos da instituição, que incluem a busca contínua pela excelência na gestão pública, a transparência nas contratações e a promoção da inovação e, tem como base o alinhamento à missão, o Planejamento Estratégico e o Plano Diretor de Tecnologia da Informação (PDTI), atendendo aos seguintes objetivos estratégicos

- OE2: Promover a excelência no atendimento aos usuários da TI;
- OE3: Acelerar a transformação digital de forma sistêmica, aprimorando a gestão de Tecnologia da Informação;
- OE6: Otimizar as infraestruturas de TI;
- OE9: Garantir a gestão eficiente dos recursos orçamentários e financeiros de TI.

4.3. Normativos que Fundamentam a Contratação

- Lei nº 14.133, de 1º de abril de 2021 - Regulamento Lei de Licitações e Contratos Administrativos.
- Decreto Estadual nº 11.363, de 22 de novembro de 2023 – que regulamenta a Lei nº 14.133/2021, no âmbito do Estado do Acre.
- E demais legislações pertinentes.

5. DOS CRITÉRIOS DE AGRUPAMENTO DE ITENS EM LOTE ÚNICO

5.1. Fundamento Legal

5.1.1. A Lei 14.133/2021, em seus **art. 40, inciso V, alínea ‘b’, §§ 2º, inciso I, e 3º, inciso II**, bem como o **art. 47, inciso II**, determina que o parcelamento do objeto deve ser adotado quando tecnicamente viável e economicamente vantajoso. Entretanto, a mesma legislação prevê exceções, admitindo a **contratação em LOTE ÚNICO quando o objeto for tecnicamente integrado, a divisão comprometer a economia de escala, aumentar custos de gestão, ou houver risco à funcionalidade do sistema como um todo**. Senão vejamos:

"Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

(...)

V - atendimento aos princípios:

(...)

b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso;

(...)

§ 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

I - a viabilidade da divisão do objeto em lotes;

(...)

§ 3º O parcelamento não será adotado quando:

(...)

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

(...)

“Art. 47. As licitações de serviços atenderão aos princípios:

(...)

II - do parcelamento, quando for tecnicamente viável e economicamente vantajoso.” (Grifamos)

5.1.2. Além disso, o Tribunal de Contas da União (TCU) reconhece jurisprudencialmente a legitimidade do agrupamento em **lote único** quando a divisão possa prejudicar a funcionalidade do objeto, conforme pode ser observado **Acórdão nº 5.260/2011 - Primeira Câmara**, vejamos:

*“REPRESENTAÇÃO DE LICITANTE. PREGÃO PARA REGISTRO DE PREÇOS. ADJUDICAÇÃO POR LOTE. INEXISTÊNCIA DE IRREGULARIDADES. CONHECIMENTO E ARQUIVAMENTO. **Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si.**” (Grifamos)*

5.1.3. Ainda, na doutrina recorremos ao Professor Jorge Ulisses Jacoby Fernandes, em Parecer de nº 2086/00, elaborado no Processo nº 194/2000 do TCDF, que ensina:

*“Desse modo a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. Não se imagina, quando o objeto é fisicamente único, como um automóvel, que o administrador esteja vinculado a parcelar o objeto. Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidencia que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. **Não é pois a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório.** Observa-se que, na aplicação dessa norma, até pela disposição dos requisitos, fisicamente dispostos no seu conteúdo, a avaliação sob o aspecto técnico precede a avaliação sob o aspecto econômico. É a visão jurídica que se harmoniza com a lógica. Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica, imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico. Por esse motivo, deve o bom administrador, primeiramente, avaliar se o objeto é divisível. Em caso afirmativo, o próximo passo será avaliar a conveniência técnica de que seja licitado inteiro ou dividido.”*

5.2. Justificativa Técnica

5.2.1. No presente caso, a **interdependência técnica e operacional entre os componentes** da solução de segurança cibernética é **profunda e indispensável para garantir a eficácia do sistema como um todo**. O Centro de Operações de Segurança (SOC), por exemplo, atua como o ponto central de monitoramento e resposta a incidentes, mas sua eficiência depende diretamente da integração com a solução SIEM, que agrega e correlaciona dados de eventos e logs de toda a infraestrutura. Sem essa integração, o SOC perde a capacidade de obter uma visão consolidada e contextualizada dos eventos de segurança, prejudicando a detecção precoce e a resposta rápida a ameaças. Além disso, o SIEM necessita receber informações contínuas e atualizadas da gestão de vulnerabilidades para priorizar os riscos mais críticos, assim como da inteligência de ameaças (*Threat Intelligence*), que fornece dados sobre novos vetores e técnicas de ataque, possibilitando a antecipação de incidentes. A solução de validação contínua de segurança (BAS) complementa esse ciclo ao simular ataques reais, testando a eficácia dos controles implementados e fornecendo feedback essencial para ajustes nas regras de detecção e resposta do SOC e SIEM.

5.2.2. Essa cadeia de dependências cria um ambiente em que a fragmentação das soluções entre fornecedores distintos pode gerar sérios problemas de interoperabilidade, dificultando a integração dos sistemas e a gestão centralizada dos incidentes. A multiplicidade de contratos e fornecedores aumenta a complexidade operacional, eleva os custos de coordenação e fiscalização, e, principalmente, cria pontos de falha e lacunas de segurança exploráveis por agentes maliciosos. Essa fragmentação também compromete a agilidade na resposta a incidentes, pois a comunicação entre sistemas e equipes pode ser prejudicada, atrasando ações corretivas e ampliando o impacto dos ataques.

5.2.3. Assim, a interdependência técnica e operacional entre as soluções torna imprescindível à contratação em lote único, assegurando que todas as ferramentas e serviços estejam plenamente integrados, sob uma única gestão e responsabilidade, o que maximiza a eficiência, a segurança e a resiliência do ambiente cibernético da Secretaria de Estado da Fazenda do Acre.

5.2.4. O parcelamento, embora possa ampliar a competição, neste contexto específico, traria riscos concretos:

- Perda de responsabilidade técnica centralizada, dificultando a atribuição de responsabilidades em caso de incidentes.
- Aumento de custos administrativos e de fiscalização, exigindo múltiplos contratos, equipes e controles paralelos, o que é ineficiente para a Administração.
- Possibilidade de conflitos contratuais e atrasos, caso fornecedores distintos não consigam garantir a integração plena das soluções.
- Risco à segurança cibernética, pois a ausência de integração pode gerar lacunas exploráveis por agentes maliciosos, prejudicando a efetividade da proteção da informação institucional

5.2.5. A adoção de lote único proporciona:

- Padronização tecnológica e operacional, facilitando a gestão, fiscalização e integração dos serviços e soluções.
- Economia de escala, com potencial redução de custos globais e maior poder de negociação junto ao fornecedor.
- Maior eficiência e agilidade na execução, com cronogramas e entregas alinhados sob uma única coordenação.
- Concentração da responsabilidade, garantindo maior controle e eficiência na resolução de incidentes e no cumprimento dos níveis de serviço acordados.

5.2.6. Portanto, recomenda-se a realização da licitação por LOTE ÚNICO, pois assegura a plena integração das ferramentas e serviços sob uma única gestão, evitando incompatibilidades técnicas, atrasos e possíveis falhas na comunicação entre diferentes

fornecedores. Essa centralização facilita a responsabilização, otimiza a eficiência operacional e eleva o nível de segurança cibernética da Secretaria de Estado da Fazenda do Acre, uma vez que permite uma visão unificada do ambiente tecnológico. Adicionalmente, essa abordagem está em conformidade com a legislação vigente, simplifica a fiscalização e a gestão contratual, além de garantir maior transparência e economia para a administração pública. Dessa forma, a contratação por lote único contribui significativamente para a efetividade, resiliência e sustentabilidade da proteção institucional, assegurando a continuidade das operações e o fortalecimento da infraestrutura tecnológica pública.

6. JUSTIFICATIVA DO REGISTRO DE PREÇOS

6.1. Motivação do Registro de Preço

6.1.1. A escolha do Sistema de Registro de Preços (SRP), conforme disposto nos **arts. 82 e 84 da Lei nº 14.133/2021**, justifica-se pela natureza e características do objeto, que envolve serviços contínuos e soluções tecnológicas passíveis de contratação conforme necessidade e disponibilidade orçamentária ao longo do exercício. O SRP permite maior eficiência administrativa e econômica, ao possibilitar a formação prévia de um registro de preços com fornecedores qualificados, assegurando celeridade nas futuras contratações, sem comprometer os padrões de segurança, confiabilidade e conformidade técnica exigidos pela SEFAZ/AC.

6.1.2. Além disso, o uso do SRP é adequado em razão da possibilidade de variação na demanda dos serviços de segurança cibernética, que está diretamente relacionada à evolução das ameaças, atualizações tecnológicas e necessidades de ampliação de cobertura dos ambientes digitais do órgão. O SRP possibilita a aquisição de serviços e soluções com preços registrados e previamente avaliados, garantindo padronização, economicidade, competitividade e transparência nos processos subsequentes, atendendo aos princípios previstos no **art. 5º da Lei nº 14.133/2021**.

6.1.3. Dessa forma, a adoção do Sistema de Registro de Preços proporciona melhor planejamento das contratações públicas, permitindo ao órgão a realização de contratações futuras conforme o surgimento de novas demandas, sem necessidade de realizar novo processo licitatório integral, o que contribui para a racionalização de procedimentos e a otimização dos recursos públicos. Portanto, diante da natureza tecnológica e da variabilidade de demanda dos serviços de segurança cibernética, bem como da necessidade de manutenção contínua da integridade dos sistemas da SEFAZ/AC, justifica-se a adoção do Sistema de Registro de Preços como o instrumento mais adequado para a licitação do objeto, em observância aos princípios da eficiência, economicidade, continuidade e planejamento da administração pública.

6.1.4. Também, o *TCU tem se manifestado favoravelmente ao emprego do Sistema de Registro de Preços para a contratação de soluções tecnológicas*, desde que observados os critérios de padronização, recorrência da demanda e planejamento adequado, conforme dispõe a Lei nº 14.133/2021. Na decisão (Acórdão nº 969/2022 – Plenário), o TCU avaliou registro de preços para contratação de serviços técnicos de apoio administrativo e tecnológico, ressaltando que o SRP é admitido quando o serviço é de natureza continuada, com características de padronização e possibilidade de contratação futura conforme necessidade do órgão. Ainda, no Acórdão nº 2736/2023 – Plenário, o Tribunal analisou certame voltado à contratação de solução tecnológica do tipo BPMS (*Business Process Management System*) para automação de serviços públicos, em que destacou ser possível a utilização do SRP para demandas replicáveis e passíveis de padronização.

6.1.5. Adicionalmente, o tribunal orienta que os órgãos interessados em aderir a atas de registro de preços de serviços de tecnologia da informação e comunicação (TIC) devem evidenciar, no estudo técnico preliminar, os ganhos de eficiência, viabilidade e economicidade da adoção do SRP para tais contratações, conforme determina o §3º do art. 86 da Lei nº 14.133/2021. Portanto, a fundamentação está amparada pelo entendimento do TCU, que recomenda a utilização do SRP em serviços tecnológicos em razão da recorrência, da padronização e da possibilidade de escolha planejada do momento e do quantitativo a serem contratados, sempre visando à eficiência e à economicidade para a Administração Pública.

6.1.6. Por derradeiro, **o procedimento licitatório na MODALIDADE PREGÃO ELETRÔNICO, para REGISTRO DE PREÇOS**, está em **plena consonância com a Lei nº 14.133/2021**, atendendo aos princípios de eficiência, economicidade, transparência e planejamento público, e se adequa perfeitamente à natureza dos serviços demandados, que exigem continuidade, qualidade técnica, inovação constante e flexibilidade de execução para a garantia da segurança institucional da SEFAZ/AC.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1. Descrição da Solução

7.1.1. Consiste na contratação de prestação de serviços gerenciados de segurança cibernética na modalidade SaaS (Software as a Service), abrangendo tanto o fornecimento de soluções de software quanto serviços especializados, conforme especificações técnicas estabelecidas. Essa contratação visa atender integralmente às demandas de segurança da informação da Secretaria, garantindo proteção contínua e eficiente contra ameaças cibernéticas.

7.1.2. A solução contempla um conjunto integrado de serviços e ferramentas essenciais para a gestão e operação da segurança cibernética, distribuídos em oito itens principais, com fornecimento mensal e quantitativos definidos para um período de 60 meses, exceto para o serviço de Gestão de Identidade e Governança (IGA), que será fornecido por 24 meses, e consultoria especializada sob demanda, totalizando 2000 horas técnicas.

7.1.3. Os principais componentes da solução incluem:

- a) *SOC – Security Operations Center*: Serviço de monitoramento contínuo de segurança da informação, com capacidade de detecção, análise e resposta a incidentes em tempo real;
- b) *Solução para Gestão de Vulnerabilidades*: Ferramenta para identificação, classificação, priorização e correção de vulnerabilidades em ativos tecnológicos;

c) *Solução para Gerenciamento e Correção de Eventos de Segurança - FortiSIEM*: Plataforma de correlação de eventos, automação de respostas e geração de alertas de segurança;

d) Solução de Inteligência contra Ameaças (Threat Intelligence): Integração de fontes de inteligência cibernética para antecipação e mitigação de ameaças emergentes;

e) Solução para Validação de Segurança Contínua (BAS - Breach and Attack Simulation): Simulação contínua de ataques para avaliação da eficácia dos controles de segurança implementados;

f) Solução para Gestão de Acessos Privilegiados (PAM - Privileged Access Management): Controle, auditoria e rastreabilidade de acessos privilegiados a sistemas críticos;

g) Consultoria em Serviços Especializados (on demand): Apoio técnico especializado sob demanda, para suporte em ações específicas de segurança da informação.

7.1.4. A solução, ao ser ofertada na modalidade SaaS, traz benefícios como redução de custos com infraestrutura, rápida implementação, escalabilidade conforme a necessidade da Secretaria, manutenção e atualizações contínuas realizadas pelo fornecedor, além de acesso a expertise especializada e monitoramento 24/7, garantindo alta eficiência operacional e mitigação proativa de riscos.

7.1.5. Em síntese, a solução contratada é um pacote completo e integrado de serviços gerenciados de segurança cibernética, que combina tecnologia avançada e suporte especializado para proteger a Instituição contra ameaças digitais, assegurando a continuidade e integridade dos seus sistemas e dados críticos.

7.1.6. As demais descrições da solução como um todo encontram-se pormenorizadas no **Anexo I - Especificações Técnicas Mínimas**.

7.2. **Da opção por FORTISIEM como Solução para Gerenciamento e Correção de Eventos de Segurança**

7.2.1. A Secretaria de Estado da Fazenda do Acre (SEFAZ/AC) utiliza, de forma contínua e satisfatória, há mais de cinco anos, solução de segurança perimetral gerenciada com alta disponibilidade da fabricante Fortinet. Essa solução se integra de maneira eficiente à arquitetura tecnológica da instituição, proporcionando uma camada de proteção que abrange firewall, inspeção de tráfego, filtragem de conteúdo e prevenção contra intrusões, elementos essenciais para um ambiente seguro e resiliente.

7.2.2. Do ponto de vista estratégico, a adoção da solução FORTISIEM representa uma decisão fundamentada na continuidade tecnológica e na maximização dos investimentos já realizados. Manter a uniformização da infraestrutura tecnológica assegura não apenas a compatibilidade, mas também a otimização dos processos operacionais, evitando rupturas ou incompatibilidades que poderiam comprometer a estabilidade dos sistemas da SEFAZ/AC. Além disso, a arquitetura Fortinet é reconhecida mundialmente pela sua robustez, escalabilidade e capacidade de integração com múltiplas fontes e ambientes híbridos, garantindo uma visão unificada e aprofundada dos eventos de segurança em tempo real.

7.2.3. Importante ressaltar que o FORTISIEM atuará como um componente central e integrador da arquitetura de segurança da SEFAZ/AC, recebendo dados e informações provenientes de diversas soluções especializadas, como o *Security Operations Center (SOC)*, Solução de Gestão de Vulnerabilidades, *Threat Intelligence*, Gestão de Acessos Privilegiados (PAM) e a plataforma de Validação de Segurança Contínua (BAS). Essa interação sistêmica, permite a correlação automática e contextualizada dos eventos de segurança, favorecendo a análise precisa, a automação de respostas e o fortalecimento da postura proativa de defesa da instituição, ao criar uma malha de proteção dinâmica, integrada e eficiente.

7.2.4. Outro ponto crucial é que a equipe técnica da SEFAZ/AC já possui capacitação e certificações específicas na tecnologia Fortinet, o que representa uma economia significativa em recursos e tempo, ao eliminar a necessidade de treinamentos extensivos e acelerar a curva de aprendizagem. Essa expertise interna permite uma resposta mais ágil e eficaz diante de incidentes, elevando o nível de maturidade da segurança cibernética da instituição, com maior assertividade na detecção, correlação e resposta automática a ameaças complexas.

7.2.5. Adicionalmente, a padronização tecnológica baseada no FORTISIEM contribui diretamente para a economicidade, ao reduzir custos de manutenção, suporte e integração técnica frente a múltiplas soluções heterogêneas. O uso consolidado dessa plataforma facilita a governança, o controle e o *compliance*, atendendo exigências regulatórias como a Lei Geral de Proteção de Dados (LGPD). No médio e longo prazo, a adoção dessa solução fortalece a escalabilidade e a sustentabilidade da infraestrutura de segurança, permitindo a incorporação contínua de novas funcionalidades, atualizações automáticas e adaptação ágil às mudanças no cenário de ameaças cibernéticas.

7.2.6. Portanto, a escolha pelo FORTISIEM se constitui numa decisão que associa racionalidade técnica, eficiência operacional e responsabilidade fiscal, alinhando-se às melhores práticas internacionais e garantindo à SEFAZ/AC uma postura sólida, integrada e proativa em segurança da informação, essencial para a proteção dos ativos públicos e a continuidade dos serviços essenciais à população.

8. **REQUISITOS DA CONTRATAÇÃO**

8.1. **Requisitos de Negócio**

8.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

a) Garantir a proteção integral dos ambientes digitais da SEFAZ/AC, identificando e mitigando ameaças cibernéticas em tempo real para assegurar a disponibilidade, integridade e confidencialidade dos sistemas;

b) Disponibilizar serviços gerenciados eficientes que possibilitem a prevenção, detecção, resposta e remediação de incidentes cibernéticos, alinhados às melhores práticas de segurança e regulamentações aplicáveis, como a LGPD;

- c) Compensar a insuficiência de profissionais especializados internos, com fornecimento de equipe capacitada e soluções tecnológicas avançadas para a gestão contínua da segurança cibernética;
- d) Implementar os serviços gerenciados de segurança cibernética para otimizar custos e escalar recursos conforme necessidade;
- e) Atender demandas de consultoria especializada sob demanda para melhorias, atualizações e adaptações contínuas das soluções de segurança;
- f) Assegurar conformidade legal e regulatória, promovendo a governança e a transparência através de relatórios e indicadores de desempenho.

8.2. Requisitos de Manutenção

8.2.1. Entende-se por requisitos de manutenção a necessidade de continuidade da prestação de serviços de TIC relacionados a segurança cibernética, visando garantir o acesso aos serviços de TIC na SEFAZ/AC, bem como reduzir ou mitigar a ocorrência de falhas, problemas ou incidentes, conforme detalhado neste Termo de Referência e respectivos Anexos.

8.2.2. Abrange SOC, Gestão de Vulnerabilidades, SIEM (FortiSIEM), *Threat Intelligence*, BAS, Gestão de Acessos Privilegiados (PAM) e Consultoria Especializada *on demand*.

8.2.3. Substituição obrigatória, em até 10 dias úteis, de quaisquer *appliances*, softwares ou componentes que apresentem:

- a) Ocorrência de 3 ou mais chamados de manutenção corretiva em 30 dias contínuos.
- b) Tempo de paralisação acumulado superior a 20 horas em 30 dias contínuos.

8.2.4. No caso de inviabilidade da solução definitiva do problema, a contratada poderá substituir o item definitivo, mediante aprovação técnica da contratante.

8.2.5. A contratada deve manter as soluções em versões atualizadas, garantindo o correto funcionamento e atendimento aos requisitos do contrato.

8.2.6. Disponibilização de suporte e atendimento técnico 24x7, com canais dedicados e equipe com certificações exigidas.

8.2.7. Atualizações, patches e correções devem ser aplicados pela contratada conforme melhores práticas, com monitoramento contínuo de vulnerabilidades e riscos.

8.2.8. Documentação técnica completa dos procedimentos de manutenção e correções realizados deve ser entregue à contratante.

8.2.9. Garantir a operação estável e segura das soluções implantadas, realizando manutenção preventiva e corretiva.

8.2.10. O monitoramento deve incluir avaliação e *tunning* das soluções para reduzir falsos positivos e melhorar a eficácia dos controles.

8.2.11. Serviços de consultoria técnica para ajustes e melhorias contínuas, incluindo atualização de versões de software/hardware contratados.

8.2.12. Relatórios periódicos de desempenho, ocorrências, correções aplicadas, incidentes tratados e estado da manutenção devem ser gerados e entregues.

8.2.13. Demais requisitos de manutenção do objeto encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

8.3. Requisitos Tecnológicos

8.3.1. Esta seção contempla os requisitos tecnológicos necessários para a implementação das soluções de segurança cibernética no ambiente da SEFAZ/AC. São detalhadas as especificações técnicas fundamentais para que as ferramentas e plataformas adotadas possam oferecer alto desempenho, integração, escalabilidade e compatibilidade com o ambiente tecnológico atual, assegurando uma infraestrutura segura, confiável e atualizada:

- a) Implementação de um *Security Operations Center* (SOC) com estrutura física e operacional em território nacional;
- b) Soluções fornecidas em modelo SaaS, garantindo atualização contínua e aplicação de melhores práticas automáticas;
- c) Ferramentas integradas para gestão e correlação de eventos de segurança (FortiSIEM), Gestão de Vulnerabilidades, Threat Intelligence, BAS, PAM e suporte técnico;
- d) Integração dos sistemas de monitoramento via API (REST/SOAP), compatibilidade ampla de plataformas e capacidade de processamento (mínimo de 12.500 EPS e 2.500 dispositivos monitorados);
- e) Compatibilidade com ambientes virtuais (VMware, Hyper-V, KVM) e nuvens públicas (Azure, AWS, OCI);
- f) Capacidades avançadas em análise comportamental, automação de *playbooks*, geração de alertas e relatórios customizáveis;
- g) Suporte a autenticação multifator, autenticação federada, *Single Sign-On* (SSO) e integração com diretórios corporativos.

8.3.2. As demais definições técnicas encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

8.4. Requisitos Técnicos Específicos

8.4.1. Os requisitos técnicos específicos mínimos estabelecem os critérios obrigatórios que as soluções e serviços contratados devem atender para garantir uma prestação eficaz e alinhada às melhores práticas do mercado. Incluem certificações, capacidades técnicas, padrões de segurança e metodologias que asseguram a qualidade dos serviços e a capacidade de resposta frente às ameaças cibernéticas:

- a) Certificações obrigatórias ISO/IEC 27001, ISO/IEC 20000, ISO/IEC 27701 e ISO/IEC 9001 para os serviços e o SOC;
- b) Equipe técnica certificada, mínima com certificações como CEH, CYSA+, Fortinet NSE4, CISSP, CISM, e similares, conforme a necessidade de cada solução;
- c) Soluções devem ter capacidade para múltiplos usuários simultâneos, controle de acesso granular via RBAC, armazenamento criptografado e registros invioláveis (FIPS 140-2);
- d) Serviços de detecção e resposta a incidentes devem obedecer frameworks internacionais como MITRE ATT&CK, NIST e SANS;
- e) Ferramentas devem possuir funcionalidades de *discovery*, varredura passiva e ativa, monitoramento remoto, e avaliação e priorização automática de vulnerabilidades utilizando CVSS;
- f) Implementação dos serviços conforme metodologia PMBOK, com apresentação de projeto, planos de instalação e treinamento;
- g) Atualização automática das bases de dados de ameaças, regras de correlação e ferramentas;
- h) Capacidades de orquestração e integração das soluções com sistemas externos de incidentes, compliance e segurança;

8.4.2. As demais definições técnicas encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

8.5. **Requisitos de Formação da Equipe e Experiência Profissional**

8.5.1. Considerando a complexidade do ambiente e a criticidade das informações existentes, não é razoável permitir que os serviços de segurança cibernética sejam realizados por profissionais sem o preparo técnico adequado. Tendo em vista que a SEFAZ possui uma complexa infraestrutura de TI e que produz, diariamente, grande volume de documentos classificados, é necessária excelência técnica para que a identificação e respostas de incidentes de segurança ocorram com a máxima precisão.

8.5.2. Entende-se que os serviços deverão ser executados por especialistas habilitados, considerando que a capacitação deve ter base em programas de formação e certificações oficiais, oferecendo indícios de capacidade técnica mínima para atender as complexidades especificadas neste Termo de Referência, requisito este em consonância com o Tribunal de Contas da União (TCU):

“Em diversas assentadas, este Tribunal reconheceu como válida a exigência de comprovação de ambos os ângulos da capacitação técnica, que deverá abranger tanto o aspecto operacional (demonstração de possuir aptidão para o desempenho de atividade pertinente e compatível com o objeto do certame) como o profissional (deter, no quadro permanente, profissionais aptos a executar serviço de características semelhantes àquele pretendido pela Administração). Nesse sentido, vale destacar as Decisões nº 395/95-Plenário, 432/96- Plenário, 217/97-Plenário, 285/00-Plenário, 2.656/2007-Plenário, bem como o Acórdão nº 32/2003- 1ª Câmara. (Acórdão nº 1.265/2009, Plenário, rel. Min. Benjamin Zymler)”

8.5.3. Portanto, a capacitação e certificação da equipe técnica designada para a prestação dos serviços gerenciados de segurança cibernética são fatores essenciais para garantir a eficácia, qualidade e confiabilidade das operações de segurança da SEFAZ/AC.

8.5.4. A equipe deverá possuir conhecimentos especializados, atualizados, e comprovados por meio de certificações reconhecidas internacionalmente, alinhadas aos padrões das ferramentas e tecnologias adotadas no ambiente contratado. O objetivo central é assegurar que os profissionais sejam aptos a operacionalizar, analisar, responder e mitigar incidentes cibernéticos com agilidade e competência, utilizando metodologias consolidadas e melhores práticas do mercado.

8.5.5. As demais definições de formação das equipes encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

8.6. **Requisitos Temporais**

8.6.1. Requisitos temporais são condições que especificam prazos, duração, horários ou tempos específicos para a execução, resposta ou conclusão de atividades ou serviços:

- a) A entrega do Projeto de Instalação deverá ocorrer em até 5 dias após o recebimento da ordem de serviço;
- b) O prazo para a conclusão da instalação das soluções - itens 1 a 5 - será de até 90 (noventa) dias consecutivos, contados a partir do primeiro dia útil subsequente ao recebimento da respectiva Ordem de Serviço (OS) emitida pela CONTRATANTE para início da implantação;
- c) O prazo para conclusão da instalação da Solução de Gestão de Acessos Privilegiados - PAM (item 6) será de até 06 (seis) meses, contados a partir do primeiro dia útil subsequente ao recebimento da respectiva Ordem de Serviço (OS) emitida pela CONTRATANTE para início da implantação;
- d) SLA para atendimento: resposta inicial em até 2 horas para incidentes críticos, escalando até 24 horas para chamados de menor severidade;
- e) SLA para resposta inicial da equipe CSIRT para incidentes críticos em até 30 minutos, com tempo máximo para resolução inicial de 4 horas;

f) Monitoramento dos ativos em regime 24x7, escalonado entre equipe N1 e N2;

g) SLA para primeira notificação de *takedown* na Solução de *Threat Intelligence*: máximo de 5 minutos após solicitação;

h) Tempo máximo para substituir appliance, software ou componentes após falhas graves: no máximo 10 dias úteis;

i) Prazo máximo para início do atendimento on demand de consultoria: 3 dias úteis;

j) Política para chamadas de manutenção corretiva: substituição obrigatória se ocorrerem 3 ou mais chamados em um período contínuo de 30 dias (diversos pontos);

k) Política de paralisações: substituição obrigatória se somatório de paralisação ultrapassar 20 horas em período contínuo de 30 dias (diversos pontos);

l) Para relatórios na solução de *Threat Intelligence*, devem ser enviados relatórios mensais com síntese dos dados.

8.6.2. A critério da CONTRATANTE, e mediante justificativa da CONTRATADA por fatos supervenientes ou necessidades técnicas específicas, os prazos tratados nas letras "b" e "c" (8.4.1.) poderão ser prorrogados, mediante a aprovação prévia de Cronograma de Execução revisado e acordado entre as partes, sem prejuízo da remuneração e dos prazos de vigência contratual.

8.6.3. Demais requisitos temporais encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

9. OUTROS REQUISITOS DA CONTRATAÇÃO

9.1. Subcontratação

9.1.1. Não será admitida a subcontratação do objeto contratual.

9.2. Requisitos Legais

9.2.1. Constituição Federal;

9.2.2. Lei nº 14.133, de 2021 (Lei de Licitações e Contratos Administrativos);

9.2.3. Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

9.2.4. Decreto Estadual nº 11.363, de 2023 (Regulamenta a Lei nº 14.133/21, no âmbito do Estado do Acre);

9.2.5. Demais legislações aplicáveis.

9.3. Vistoria

9.3.1. Para o correto dimensionamento e elaboração de sua proposta, será facultado à LICITANTE realizar vistoria para conhecer a infraestrutura e as instalações do CONTRATANTE.

9.3.2. O ambiente tecnológico será apresentado e detalhado aos interessados no ato da Vistoria sob a assinatura do TERMO DE CONFIDENCIALIDADE (Anexo II).

9.3.3. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo até 5 (cinco) dias corridos antes da data marcada para o recebimento de propostas.

9.3.3.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado junto ao Departamento de Tecnologia da Informação - DETI, pelo do E-mail: deti@sefaz.ac.gov.br, ou pelo telefone (68) 3212-7958, em dias úteis, das 8h às 14h, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

9.3.3.2. A visita destina-se à vistoria preliminar, avaliação e ciência das empresas interessadas para conhecimento pleno das condições e peculiaridades do objeto a ser contratado, com fins de elaboração da proposta e demais efeitos decorrentes deste Edital.

9.3.3.3. A vistoria deverá ser feita por profissional qualificado da empresa interessada, o qual deverá estar munido de documento de identificação e de instrumento que o habilite à representação legal da empresa.

9.3.3.4. Para todos os efeitos, considerar-se-á que a LICITANTE, optante pela realização de vistoria ou não, tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos serviços e de dificuldades técnicas não previstas.

9.3.4. Efetuada a vistoria será lavrado, por representante da equipe técnica de TI, a respectivo DECLARAÇÃO DE VISTORIA (Anexo III), o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando à sua habilitação.

9.3.5. Os custos da vistoria são de responsabilidade do licitante, incluindo seus deslocamentos em veículo aos locais vistoriados.

9.3.6. Os licitantes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a vistoria. A simples participação na vistoria caracteriza o compromisso irretratável de guarda do sigilo dos dados colhidos.

9.3.7. A opção por não realizar a vistoria facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

9.3.8. Caso a LICITANTE renuncie à vistoria técnica, deverá entregar junto à documentação de habilitação, a DECLARAÇÃO DE RENÚNCIA À VISTORIA TÉCNICA (Anexo VI), o qual deverá ser preenchido e assinado pelo interessado em participar da licitação.

9.3.8.1. A não apresentação da DECLARAÇÃO será motivo de inabilitação.

9.4. **Garantia de Execução Contratual**

9.4.1. No ato da assinatura do Contrato, o fornecedor deve apresentar comprovante de garantia para sua execução, com validade durante todo período de vigência contratual, correspondente a 5% (cinco por cento) de seu valor global, em uma das modalidades de garantia previstas no art. 96 da Lei 14.133/21:

- I - Caução em dinheiro ou em títulos da dívida pública;
- II - Seguro garantia;
- III - Fiança bancária.
- IV - Título de Capitalização.

9.4.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- a) Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- b) Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
- c) Multas moratórias e punitivas aplicadas pela Administração ao contratado; e
- d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pelo contratado.

9.4.3. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

9.4.4. O garantidor não é parte interessada para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao contratado.

9.4.5. A garantia será considerada extinta com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

9.4.6. A garantia prestada deverá vigorar por mais 90 (noventa) dias após o término da vigência contratual e será liberada ou restituída a CONTRATADA findo este prazo, desde que integralmente cumpridas todas as obrigações assumidas, inclusive as trabalhistas. Caso o pagamento das verbas rescisórias trabalhistas não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas diretamente pela Contratante;

9.4.7. A Contratante não executará a garantia nas seguintes hipóteses:

- a) Caso fortuito ou força maior;
- b) Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;
- c) Descumprimento das obrigações pelo contratado decorrente de atos ou fatos da Administração;
- d) Prática de atos ilícitos dolosos por servidores da Administração;

9.4.8. Não serão admitidas outras hipóteses de não execução da garantia, que não as previstas no item anterior;

9.4.9. Cabe à própria administração apurar a isenção da responsabilidade prevista nos incisos III e IV acima, não sendo a entidade garantidora parte no processo instaurado pela CONTRATANTE;

9.4.10. A CONTRATADA se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, inclusive na hipótese de utilização para indenização a terceiros, e, ainda, na alteração do valor contratado, para manter o percentual inicial, no prazo de 48 (quarenta e oito) horas, a partir da data em que for notificada pela Contratante, mediante correspondência entregue contra recibo.

9.5. **Requisitos de Segurança da Informação e Privacidade**

9.5.1. As atividades da CONTRATADA deverão estar em conformidade com as melhores práticas e padrões de segurança da informação, observando frameworks e normas reconhecidas, tais como: ISO/IEC 27001 e 27002 (Gestão da Segurança da Informação), ISO/IEC 27017 e 27018 (Segurança e Privacidade em Serviços de Nuvem), NIST *Cybersecurity Framework* (CSF), CIS *Controls*, ITIL (*Information Technology Infrastructure Library*) e as diretrizes da norma ABNT NBR ISO/IEC 27701 (Gestão de Privacidade da Informação), Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais), bem como demais referenciais técnicos aplicáveis ao contexto de proteção cibernética e governança digital da Administração Pública.

9.5.2. Todas as atividades deverão garantir a integridade, confidencialidade e disponibilidade das informações da CONTRATANTE, obedecendo integralmente às normas internas da SEFAZ/AC.

9.5.3. A CONTRATADA será responsável pela devida proteção de todos os dados, documentos, especificações técnicas e demais ativos informacionais acessados ou produzidos durante a execução dos serviços, vedada sua reprodução, divulgação, utilização ou repasse a terceiros, inclusive após o término do contrato.

9.5.4. Seus representantes e colaboradores deverão firmar Termo de Compromisso e Manutenção de Sigilo e Termo de Ciência, conforme exigido pela SEFAZ/AC, resguardando o sigilo absoluto das informações tratadas.

9.5.5. Eventuais incidentes ou anormalidades que representem riscos ou vulnerabilidades deverão ser comunicados imediatamente, por escrito, à CONTRATANTE.

9.5.6. Outros requisitos de segurança do objeto encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

9.6. **Indicação de Marca ou Modelo**

9.6.1. Na presente contratação será admitida a indicação da marca de acordo com as justificativas a seguir relacionadas:

9.6.2. A Secretaria de Estado da Fazenda do Acre (SEFAZ/AC) utiliza, de forma contínua e satisfatória, há mais de cinco anos, solução de segurança perimetral gerenciada com alta disponibilidade da fabricante FORTINET. Essa solução se integra de maneira eficiente à arquitetura tecnológica da instituição, proporcionando uma camada de proteção que abrange firewall, inspeção de tráfego, filtragem de conteúdo e prevenção contra intrusões, elementos essenciais para um ambiente seguro e resiliente.

9.6.3. Do ponto de vista estratégico, a adoção da solução FORTISIEM representa uma decisão fundamentada na continuidade tecnológica e na maximização dos investimentos já realizados. Manter o padrão da infraestrutura tecnológica assegura não apenas a compatibilidade, mas também a otimização dos processos operacionais, evitando rupturas ou incompatibilidades que poderiam comprometer a estabilidade dos sistemas da SEFAZ/AC. Além disso, a arquitetura Fortinet é reconhecida mundialmente pela sua robustez, escalabilidade e capacidade de integração com múltiplas fontes e ambientes híbridos, garantindo uma visão unificada e aprofundada dos eventos de segurança em tempo real.

9.6.4. Importante ressaltar que o FORTISIEM atuará como um componente central e integrador da arquitetura de segurança da SEFAZ/AC, recebendo dados e informações provenientes de diversas soluções especializadas, como o *Security Operations Center (SOC)*, Solução de Gestão de Vulnerabilidades, *Threat Intelligence*, Gestão de Acessos Privilegiados (PAM) e a plataforma de Validação de Segurança Contínua (BAS). Essa interação sistêmica, permite a correlação automática e contextualizada dos eventos de segurança, favorecendo a análise precisa, a automação de respostas e o fortalecimento da postura proativa de defesa da instituição, ao criar uma malha de proteção dinâmica, integrada e eficiente.

9.6.5. Outro ponto crucial é que a equipe técnica da SEFAZ/AC já possui capacitação, certificações específicas e expertise na tecnologia Fortinet, o que representa uma economia significativa em recursos e tempo, ao eliminar a necessidade de treinamentos extensivos e acelerar a curva de aprendizagem. Essa expertise interna permite uma resposta mais ágil e eficaz diante de incidentes, elevando o nível de maturidade da segurança cibernética da instituição, com maior assertividade na detecção, correlação e resposta automática a ameaças complexas.

9.6.6. Adicionalmente, a adoção da tecnológica baseada no FORTISIEM contribui diretamente para a economicidade, ao reduzir custos de manutenção, suporte e integração técnica frente a múltiplas soluções heterogêneas. O uso consolidado dessa plataforma facilita a governança, o controle e o *compliance*, atendendo exigências regulatórias como a Lei Geral de Proteção de Dados (LGPD). No médio e longo prazo, a adoção dessa solução fortalece a escalabilidade e a sustentabilidade da infraestrutura de segurança, permitindo a incorporação contínua de novas funcionalidades, atualizações automáticas e adaptação ágil às mudanças no cenário de ameaças cibernéticas.

9.6.7. Portanto, a escolha pelo FORTISIEM se constitui numa decisão que associa racionalidade técnica, eficiência operacional e responsabilidade fiscal, alinhando-se às melhores práticas internacionais e garantindo à SEFAZ/AC uma postura sólida, integrada e proativa em segurança da informação, essencial para a proteção dos ativos públicos e a continuidade dos serviços essenciais à população.

9.7. **Requisitos de Segurança Institucional e Procedimental**

9.7.1. A CONTRATADA deve seguir as orientações de segurança da SEFAZ/AC e legislação pertinente ao assunto, bem como:

- a) Submeter-se aos procedimentos contidos nas normas de segurança corporativa do órgão em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências da CONTRATANTE, inclusive durante o período de prestação dos serviços de garantia.
- b) Exigir dos seus empregados, quando em serviço nas dependências da CONTRATANTE, o uso obrigatório de uniformes e crachás de identificação.
- c) Não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado as informações de propriedade da CONTRATANTE.
- d) Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.
- e) Deverá assinar o Termo de Compromisso e Confidencialidade, e seus funcionários alocados na prestação de serviços, o Termo de Ciência, conforme modelos que estarão anexos ao Termo de Referência.
- f) Deverá comunicar imediatamente a CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

9.7.2. Demais requisitos de segurança do objeto encontram-se no **Anexo I - Especificações Técnicas Mínimas**.

9.8. **Requisitos Ambientais**

9.8.1. A CONTRATADA deverá cumprir, no que couber, as exigências do art. 7º, inciso XI, da Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

“Art. 7º São objetivos da Política Nacional de Resíduos Sólidos:

(...)

XI - prioridade, nas aquisições e contratações governamentais, para:

(...)

b) bens, serviços e obras que considerem critérios compatíveis com padrões de consumo social e ambientalmente sustentáveis;” (Grifamos)

10. DAS RESPONSABILIDADES

10.1. Deveres e Responsabilidade do CONTRATANTE

- 10.1.1. Exigir o cumprimento integral das obrigações assumidas pela CONTRATADA.
- 10.1.2. Conferir e validar os relatórios gerenciais dos serviços executados, apresentados pela CONTRATADA.
- 10.1.3. Orientar e supervisionar a observância, pela CONTRATADA, dos regulamentos administrativos e dos procedimentos de segurança da SEFAZ/AC.
- 10.1.4. Encaminhar formalmente as demandas à CONTRATADA, por meio de Ordem de Serviço, ou por sistema de chamados, de acordo com os critérios dispostos neste Termo de Referência.
- 10.1.5. Exercer o acompanhamento e a fiscalização do contrato, por intermédio de servidores especialmente designados, conforme art. 140 da Lei nº 14.133/2021.
- 10.1.6. Notificar a CONTRATADA por escrito sobre toda e qualquer ocorrência relevante à prestação dos serviços, fixando prazo para correção e certificando-se da adequação das soluções.
- 10.1.7. Realizar avaliações periódicas da qualidade dos serviços após o seu recebimento, promovendo os registros necessários.
- 10.1.8. Aplicar à CONTRATADA as sanções administrativas e contratuais cabíveis, nos termos da legislação.
- 10.1.9. Emitir, por meio do Departamento de Tecnologia da Informação, pareceres sobre atos relativos à execução do contrato, especialmente quanto à exigência de condições estabelecidas no processo licitatório.
- 10.1.10. Liquidar o empenho e efetuar o pagamento à CONTRATADA dentro dos prazos preestabelecidos.
- 10.1.11. Comunicar formalmente à CONTRATADA todas as ocorrências relacionadas à execução dos serviços, inclusive quanto à necessidade de providências corretivas.
- 10.1.12. Prestar informações necessárias à execução do objeto, em tempo hábil, sempre que solicitado pela CONTRATADA.
- 10.1.13. Permitir o acesso do pessoal técnico e dos equipamentos da CONTRATADA necessários à execução dos serviços, obedecidas as normas de segurança e sigilo institucionais.
- 10.1.14. Encaminhar as faturas dos serviços prestados para o ateste dos gestores competentes.
- 10.1.15. Não responder por compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por danos a terceiros decorrentes de atos da CONTRATADA ou de seus prepostos e empregados.

10.2. Deveres e Responsabilidades da CONTRATADA

- 10.2.1. Indicar formalmente, em até 5 dias úteis após a assinatura do contrato, preposto responsável pela execução do objeto e interlocução com a CONTRATANTE.
- 10.2.2. Atender prontamente todas as orientações, exigências e determinações da fiscalização do contrato, inerentes à execução do objeto.
- 10.2.3. Reparar, corrigir, remover, reconstruir ou substituir, integralmente e às suas expensas, quaisquer danos, vícios, defeitos ou incorreções resultantes da execução do contrato, dos serviços ou dos materiais empregados, responsabilizando-se inclusive pelo ressarcimento imediato de prejuízos causados à CONTRATANTE ou a terceiros.
- 10.2.4. Manter, durante toda a execução do contrato, todas as condições referentes à habilitação jurídica, fiscal, trabalhista, previdenciária, técnica e financeira exigidas à época da contratação.
- 10.2.5. Manter sua equipe de profissionais continuamente capacitada, treinada e certificada, conforme requisitos técnicos do Termo de Referência e suas atualizações.
- 10.2.6. Executar todos os serviços contratados em estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), normas correlatas e exigências da CONTRATANTE.
- 10.2.7. Não divulgar, publicar ou utilizar, sem autorização prévia e expressa da CONTRATANTE, qualquer informação ou publicidade relativa à execução dos serviços objeto do contrato.
- 10.2.8. Utilizar as informações e dados da CONTRATANTE exclusivamente para execução do objeto contratual, vedada sua utilização, reprodução ou divulgação para quaisquer outros fins.
- 10.2.9. Garantir que todos profissionais envolvidos possuam perfil técnico adequado e estejam atualizados conforme exigências das soluções contratadas e fabricantes.
- 10.2.10. Responder integralmente por todas as obrigações trabalhistas, fiscais, previdenciárias e tributárias pertinentes, eximindo a Administração de qualquer responsabilidade solidária ou subsidiária em caso de inadimplência.
- 10.2.11. Realizar os serviços conforme especificações técnicas estabelecidas, mantendo a produtividade, qualidade e recursos necessários ao perfeito cumprimento contratual.

- 10.2.12. Realizar a correção, substituição ou reparo de qualquer serviço ou material que apresente inadequação, vício ou defeito, conforme determinação da CONTRATANTE.
- 10.2.13. Aceitar acréscimos e supressões no objeto contratual conforme previsto pela Lei nº 14.133/2021, até o limite de 25% do valor inicial, sem questionar ou impedir a execução do ajuste.
- 10.2.14. Comunicar de imediato à CONTRATANTE qualquer anomalia, acidente, irregularidade ou fato relevante que possa comprometer a boa execução dos serviços.
- 10.2.15. Garantir o acesso irrestrito à fiscalização da CONTRATANTE, disponibilizando documentos, informações e recursos solicitados sempre que necessário.
- 10.2.16. Ressarcir a CONTRATANTE por danos causados por suas ações ou omissões, seja por agentes, prepostos ou empregados, autorizando desconto em garantia ou pagamentos devidos.
- 10.2.17. Arcar com despesas de qualquer infração cometida por empregados/prepostos, inclusive indenizações e penalidades legais.
- 10.2.18. Assegurar que todos profissionais alocados estejam devidamente habilitados e conhecedores dos serviços, cumprindo padrões técnicos e legais em vigor.
- 10.2.19. Manter contato permanente do preposto com a fiscalização da CONTRATANTE, adotando providências e coordenando toda a execução dos serviços contratados.
- 10.2.20. Relatar formalmente à CONTRATANTE qualquer irregularidade constatada durante a prestação dos serviços.
- 10.2.21. Manter sigilo absoluto sobre todas as informações, dados, documentos e procedimentos obtidos em razão da execução do contrato.
- 10.2.22. Notificar ao fiscal do contrato, em até 24 horas, qualquer ocorrência anormal ou acidente verificado nos serviços.
- 10.2.23. Prestar todos os esclarecimentos, apresentar documentos e garantir acesso ao local dos trabalhos aos representantes da CONTRATANTE, sempre que solicitado.
- 10.2.24. Paralisar, imediatamente e por determinação da CONTRATANTE, qualquer atividade que esteja sendo executada em desacordo com a técnica, normas de segurança ou que exponha risco a pessoas, bens ou dados.
- 10.2.25. Planejar, executar, monitorar e manter os serviços contratados conforme níveis de serviço acordados e exigidos pela CONTRATANTE.
- 10.2.26. Submeter previamente à CONTRATANTE, por escrito, qualquer alteração de método, processo ou tecnologia que fuja das especificações do Termo de Referência, aguardando aprovação formal para implementação.
- 10.2.27. Cumprir integralmente todas as normas de segurança institucional determinadas pela CONTRATANTE.
- 10.2.28. Realizar os serviços dentro de rotinas e parâmetros técnicos aceitáveis, observando sempre as boas práticas, normas regulamentares e legislação vigente.
- 10.2.29. Participar das reuniões de alinhamento de expectativas estabelecidas pela CONTRATANTE, bem como das demais convocações necessárias ao acompanhamento contratual.
- 10.2.30. Promover a transferência de conhecimento e técnicas de execução na transição contratual, capacitando técnicos da CONTRATANTE, quando solicitado, sem prejuízo das informações.

11. MODELO DE EXECUÇÃO DO OBJETO

11.1. Reunião Inicial

- 11.1.1. A CONTRATANTE convocará a CONTRATADA imediatamente após assinatura do contrato para reunião de kickoff, visando alinhamento de escopo, definição de responsáveis, cronograma e esclarecimento de dúvidas. Outros assuntos pertinentes poderão ser tratados nessa reunião.
- 11.1.2. Reuniões de monitoramento ou extraordinárias poderão ser convocadas durante a execução, sendo obrigatória a participação da CONTRATADA.
- 11.1.3. Todas as atas e comunicações entre as partes, bem como intercorrências contratuais, serão arquivadas em processo próprio para manutenção do histórico e rastreabilidade da gestão do contrato.
- 11.1.4. Na reunião inicial, a CONTRATADA deverá:
- 11.1.4.1. Apresentar formalmente o preposto responsável.
- 11.1.4.2. Entregar o Termo de Ciência, assinado por todos os funcionários alocados, conforme modelo no Anexo VI.
- 11.1.4.3. Entregar o Termo de Compromisso, assinado pelo representante legal, conforme modelo no Anexo V.
- 11.1.5. Havendo uso de solução complementar para execução dos serviços, a CONTRATADA deverá apresentar declaração do fabricante autorizando comercialização, instalação, configuração e suporte, constando data e número do edital.
- 11.1.6. A CONTRATADA deverá, em até 5 dias úteis da assinatura, apresentar o cronograma de execução dos serviços, que será aprovado formalmente pela CONTRATANTE e servirá como parâmetro para início das atividades.

11.2. Mecanismos Formais de Comunicação

11.2.1. São considerados mecanismos oficiais de comunicação: Ordem de Serviço, correio eletrônico, mensageria instantânea, sistema de chamados, registro de incidente e ofício.

11.3. Procedimentos de Encaminhamento e Controle de Solicitações

11.3.1. A abertura de chamados será realizada por canais definidos (telefone, e-mail, portal web), com categorização por gravidade de 1 a 4 (crítico a baixo), e prioridade atribuída pela CONTRATANTE.

11.3.2. Todo chamado deverá ser registrado com histórico, tempos de resposta e providências, gerando relatório mensal para auditoria.

11.3.3. Providenciar mecanismo de escalonamento para casos de insatisfação com tratamento dos chamados.

11.4. Prazos, Horários da Prestação dos Serviços

11.4.1. A CONTRATADA deverá considerar o horário de 7 horas às 18 horas como de horário normal de expediente da Contratante, para os dias úteis.

11.4.2. Deve ser possível a comunicação com o preposto fora do horário de atendimento.

11.4.3. A CONTRATADA deverá disponibilizar números de celular e escala do(s) profissional(ais) que responderão pelo papel de preposto(s), os supervisores e seu substitutos, mesmo fora do horário de expediente, sem que com isso ocorra qualquer ônus extra para o CONTRATANTE.

11.4.4. As atividades deverão estar disponíveis para o CONTRATANTE, no regime 24/7/365 (todos os dias do ano em horário integral, de forma ininterrupta).

11.4.5. Nos casos de ocorrências de incidentes e problemas graves, poderá ser exigida a presença do supervisor na “Sala de Crise” da CONTRATANTE.

11.4.6. Todos os níveis mínimos de serviço especificados neste documento deverão ser atendidos, independentemente do momento de abertura do chamado.

11.4.7. A CONTRATADA poderá realizar os serviços de forma remota, por meio de acesso seguro em qualquer horário de atendimento, desde que este método de acesso esteja previamente autorizado pela SEFAZ e que sejam atendidas as determinações da Política de Segurança.

11.4.8. Quando necessário os serviços técnicos (que necessitem da presença de técnicos para o atendimento) serão realizados aos finais de semana e feriados, inclusive no período noturno, e em dias úteis durante o período noturno e não deverá acarretar ônus para a CONTRATANTE.

11.4.9. Os custos decorrentes de deslocamento e hospedagem dos profissionais da CONTRATADA correrão por conta exclusiva da CONTRATADA.

11.4.10. Nos serviços prestados no âmbito da presente solução, inclusive nos serviços com execução presencial, não se caracteriza a subordinação direta e nem pessoalidade, uma vez que não se requer a exclusividade dos profissionais e sim, meramente, a disponibilidade do serviço de determinados perfis profissionais. Dessa forma, não há óbice ao compartilhamento de qualquer profissional com outros contratos que porventura a CONTRATADA possua, desde que preservados os níveis mínimos de serviços estipulados no Termo de Referência, e, além disso, não haverá qualquer relação de subordinação jurídica entre os profissionais da CONTRATADA e o CONTRATANTE.

11.5. Locais de Entrega

11.5.1. O fornecimento dos serviços serão executados, quando realizados na modalidade presencial, na sede da SEFAZ, situada na Rua Benjamim Constant, nº 946, Centro, Rio Branco – AC.

11.6. Manutenção de Sigilo e Segurança

11.6.1. A CONTRATADA 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.

11.6.2. Todos os profissionais da CONTRATADA deverão assinar Termo de Compromisso e Ciência, comprometendo-se a guardar sigilo absoluto sobre dados, informações e sistemas acessados no escopo do contrato, inclusive após seu término.

11.7. Auditoria, Relatórios e Revisões

11.7.1. A CONTRATADA deverá manter, durante a vigência contratual e pelo prazo mínimo de 5 anos, toda documentação e logs dos serviços prestados, acessível à auditoria e fiscalização da CONTRATANTE.

11.7.2. Relatórios consolidados de desempenho, históricos de chamados e conformidade deverão ser encaminhados periodicamente.

11.7.3. O modelo de execução poderá ser aprimorado por aditivo diante de novas demandas técnicas, legais ou de evolução tecnológica, mediante justificativa e aprovação formal da CONTRATANTE.

11.8. Continuidade contratual

11.8.1. A CONTRATADA deverá garantir a plena continuidade dos serviços contratados, independentemente de paralisação, greve, falhas internas, falta de pessoal, eventos de força maior ou quaisquer intercorrências, mediante plano de contingência e providências imediatas, previamente aprovado pela CONTRATANTE.

11.8.2. É obrigatória a substituição imediata de profissionais, materiais, equipamentos ou soluções que comprometam a regularidade do serviço, sem interrupção ou prejuízo à CONTRATANTE.

11.8.3. Em caso de transição contratual, a CONTRATADA promoverá transferência ordenada do conhecimento, capacitação de equipe interna, quando solicitada, e apoio técnico à nova empresa, até encerramento regular dos serviços.

12. MODELO DE GESTÃO DO CONTRATO

12.1. Princípios Gerais e Execução

12.1.1. O contrato deverá ser executado fielmente pelas partes, em estrita conformidade com as cláusulas avençadas, observando integralmente as disposições da Lei nº 14.133/2021 e regulamentos aplicáveis.

12.1.2. Em situações de impedimento, ordem de paralisação ou suspensão formal do contrato, o prazo de execução será automaticamente prorrogado pelo período correspondente, devendo tais circunstâncias ser formalizadas por apostila no processo.

12.1.3. Todas as comunicações relevantes para a execução contratual deverão ser realizadas por escrito, admitindo-se o uso de mensagem eletrônica, assegurando-se rastreabilidade e arquivamento nos autos do processo do contrato.

12.1.4. A CONTRATANTE poderá demandar, a qualquer tempo, providências imediatas por parte da CONTRATADA, convocando representantes para reuniões presenciais ou virtuais, sempre que necessário.

12.2. Fiscal do Contrato

12.2.1. São atribuições do fiscal do contrato, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos, regulamentos e normas internas:

- a) Conferir a execução do serviço e o cumprimento das obrigações contratuais, atestando mediante documento próprio a efetiva prestação dos serviços após conferência do objeto contratado, especificações técnicas e resultados entregues;
- b) Controlar a efetividade, qualidade e conformidade dos serviços executados, exigindo a correção de eventuais vícios, imperfeições, deficiências ou omissões, bem como solicitar medidas corretivas à contratada;
- c) Registrar todas as ocorrências, intercorrências, falhas, não conformidades e eventos relevantes havidos durante a execução do contrato, em sistema próprio ou processo administrativo específico, informando dia, mês, ano e, quando aplicável, os profissionais envolvidos;
- d) Apresentar, periodicamente ou quando solicitado, relatório circunstanciado de acompanhamento da execução do serviço, com avaliação crítica de desempenho, cumprimento dos níveis mínimos de serviço e registro de fatos relevantes;
- e) Encaminhar à autoridade superior, ao gestor do contrato ou à assessoria técnica, quando necessário, questões que ultrapassem sua esfera de atuação ou demandem deliberação específica;
- f) Solicitar, sempre por escrito, esclarecimentos, auxílio, documentações, suporte técnico ou informações adicionais relativas à execução contratual, inclusive em casos em que houver dúvidas sobre providências a adotar;
- g) Emitir atestados, certidões, pareceres técnicos ou registro de avaliação dos serviços prestados, conforme demanda administrativa ou regulatória;
- h) Informar imediatamente o gestor do contrato sobre irregularidades, descumprimentos ou situações que exijam providências administrativas, inclusive para glosa de pagamentos, aplicação de sanções ou revisão contratual;
- i) Participar das reuniões periódicas de acompanhamento e alinhamento contratual, promovendo o registro de questões técnicas, operacionais e administrativas relevantes à boa execução do contrato;
- j) Guardar sigilo sobre informações, processos e documentos acessados no exercício da fiscalização, assegurando a confidencialidade dos dados institucionais e respeitando os termos de sigilo e compromisso exigidos pela Administração;
- k) Zelar pela observância de todas as normas técnicas, legais, de segurança da informação, ambientais e de boas práticas aplicáveis ao serviço fiscalizado, promovendo o atendimento integral às exigências do instrumento contratual.

12.3. Gestor do Contrato

12.3.1. Compete ao Gestor do Contrato, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos, regulamentos e normas internas:

- a) Assegurar que todas as obrigações contratuais assumidas pela contratada estejam sendo cumpridas dentro dos padrões de qualidade, conformidade técnica e observância à legislação vigente;
- b) Solicitar periodicamente ao fiscal do contrato o envio de relatórios circunstanciados, ocorrências relevantes e indicativos de não conformidade para avaliação e eventual adoção de medidas corretivas.
- c) Analisar e homologar as glosas, descontos ou retenções sugeridas pelo fiscal do contrato, deliberando sobre descontos nos pagamentos mensais e notificando a área financeira para os devidos ajustes;
- d) Encaminhar formalmente demandas, ordens de serviço ou de fornecimento ao preposto da contratada, assegurando o registro e rastreabilidade dessas comunicações nos autos do processo;

e) Repassar ao fiscal do contrato todas as informações, documentos e ocorrências relevantes à execução contratual, facilitando o exercício eficiente da fiscalização;

f) Monitorar rigorosamente a vigência contratual, providenciando prorrogações, encerramentos, aditivos ou resoluções, conforme justificativas técnicas, zelo pelo interesse público e observância aos prazos legais e regulatórios;

g) Propor e implementar medidas que visem a melhoria contínua da gestão e da execução do contrato, inclusive revisão de processos, indicadores de desempenho e adoção de melhores práticas administrativas e técnicas;

h) Providenciar, sempre por escrito, a obtenção de esclarecimentos, auxílio ou suporte técnico sobre dúvidas, divergências ou situações complexas relativas à execução do contrato, consultando setores técnicos, jurídicos ou de controle quando necessário;

i) Negociar, dentro dos limites legais e de mercado, condições contratuais previamente estabelecidas com o fornecedor, especialmente durante processos de prorrogação contratual ou em situações que exijam revisão de condições técnicas e comerciais;

j) Informar periodicamente a administração superior sobre o andamento do contrato, eventuais problemas ocorridos, providências adotadas, conclusões de processos de pagamento, sanções e regularidade documental;

k) Notificar a contratada, por ordem da autoridade competente, sobre irregularidades, não conformidades ou descumprimentos identificados no curso da execução contratual;

l) Promover reuniões de acompanhamento da execução contratual, debate de indicadores de desempenho, análise de resultados e alinhamento de expectativas entre todas as partes envolvidas, registrando atas e deliberações nos autos do processo;

m) Participar ativamente de auditorias internas, externas e de órgãos de controle quanto à gestão do contrato, prestando informações, documentação e esclarecimentos sempre que requisitado.

12.4. **Avaliação de Resultados e Níveis de Serviço**

12.4.1. A avaliação da execução contratual será realizada com base nos indicadores de desempenho (KPIs), metas, percentuais e Níveis Mínimos de Serviço (NMS), definidos nas Especificações Técnicas Mínimas e seus anexos, observando-se os seguintes parâmetros:

a) *Tempo de Resposta de Chamados:*

- Para incidentes críticos, resposta inicial em até 2 horas;
- Para incidentes tratados pela equipe CSIRT, resposta inicial em até 30 minutos;
- Para consultoria on demand, início do atendimento em até 3 dias úteis;
- Para chamados de menor severidade, resposta inicial em até 24 horas;
- Primeira notificação de *Takedown (Threat Intelligence)*: máximo de 5 minutos após solicitação formal.

b) *Tempo de Solução Técnica:*

- Para incidentes críticos, solução inicial em até 4 horas após registro;
- Para demais chamados, solução conforme gravidade: até 8 horas (alto), até 24 horas (médio), até 1 dia útil (baixo).

c) *Disponibilidade dos Serviços:*

- Operação e suporte técnico em regime 24x7x365, sem tolerância para interrupções não programadas.

d) *Requisitos de Substituição de Componentes:*

- Obrigatoriedade de substituição de componentes/equipamentos que apresentem 3 ou mais chamados corretivos em 30 dias ininterruptos, ou acumularem tempo de paralisação superior a 20 horas neste período, com prazo máximo de substituição de 10 dias úteis.

e) *Atualização, Monitoramento e Manutenção:*

- Atualização automática das bases de dados, regras de correlação e ferramentas de defesa/monitoramento, conforme ciclo semanal mínimo;
- Avaliação/tuning dos controles para redução de falsos positivos e melhoria contínua da eficácia dos controles.

f) *Relatórios de Desempenho e Conformidade:*

- Entrega de relatório mensal consolidado, contendo: histórico de chamados, ocorrências relevantes, incidentes tratados, tempo de resposta, tempo de solução, status dos indicadores, medidas de contenção e proposta de melhorias.

- Manutenção de registros eletrônicos e logs acessíveis para fiscalização/auditoria pelo prazo legal mínimo de 5 anos.

g) *Avaliação e Sanções:*

- Descumprimento de qualquer indicador ou meta acarretará aplicação imediata de glosa proporcional, desconto em pagamento, comunicação formal à contratada e registro em processo próprio para análise de sanções administrativas e contratuais.
- Ocorrências de indisponibilidade superior a 0,5% ao mês ou descumprimento de prazos críticos ensejam sanções, inclusive rescisão.

h) *Certificações e Perfis Técnicos:*

- Equipe e serviços certificados em normas ISO/IEC 27001, 20000, 9001, 27701 e profissionais com CEH, CYSA, NSE4, CISSP, CISM;
- Adoção de frameworks, metodologias e controles NIST, SANS, MITRE e demais padrões internacionais de segurança e resposta a incidentes.

i) *Reunião de Avaliação:*

- Realização obrigatória de reuniões periódicas entre a CONTRATANTE, gestor, fiscal e representantes técnicos da contratada para análise dos resultados, planos de alinhamento e definição de metas de melhoria contínua.

12.4.2. Todos os indicadores, metas e SLA's contratualmente pactuados estão detalhados no Anexo I deste Termo de Referência, podendo ser revisados e atualizados mediante justificativa técnica e aditamento contratual.

12.5. Encerramento Contratual

12.5.1. Para o encerramento do contrato, será observada a conferência completa de obrigações, entrega definitiva dos serviços, transferência de conhecimento, liquidação das pendências técnicas e emissão do termo de recebimento definitivo, com ciência das partes.

13. CRITÉRIOS DE PAGAMENTO

13.1. Do Pagamento

13.1.1. O pagamento pelos serviços efetivamente prestados dar-se-á em parcelas e será creditado mensalmente à empresa CONTRATADA, ocorrendo no prazo não superior a 5 (cinco) dias úteis, contados do recebimento do documento fiscal e devido ateste da Nota Fiscal/Fatura - que deverá conter o endereço, o CNPJ, os números do Banco, da Agência e da Conta Corrente da Empresa contratada, o número da Nota de Empenho e a descrição clara do objeto - em moeda corrente nacional, de acordo com as condições constantes na proposta da Empresa contratada e aceita pela Administração contratante.

13.1.2. A emissão da ordem bancária será efetivada após o documento fiscal ser conferido, aceito e atestado por servidor responsável, caracterizando o recebimento definitivo, e ter sido verificada a regularidade da Empresa contratada, mediante consulta on-line ao Sistema Unificado de Cadastro de Fornecedores (SICAF), ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do CNJ e à Certidão Negativa (ou Positiva com efeito de Negativa) de Débitos Trabalhistas (CNDT), para comprovação, dentre outras coisas, do devido recolhimento das contribuições sociais (FGTS e Previdência Social) e demais tributos estaduais, federais e municipais, conforme cada caso.

13.1.3. O documento fiscal deverá ser emitido em nome da Secretaria de Estado da Fazenda (SEFAZ) - CNPJ nº 04.034.484/0001-40.

13.1.4. Na ocorrência de rejeição do documento fiscal motivado por erro ou incorreções, ele será devolvido à empresa contratada para retificação e reapresentação, acrescendo-se, no prazo fixado para pagamento, os dias que se passarem entre a data da devolução e a da reapresentação.

13.1.5. Nos casos de eventuais atrasos injustificados de pagamento, desde que a Empresa contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pela Administração contratante, desde a data limite fixada para pagamento até a data do efetivo pagamento, será a seguinte: $EM = (N \times VP \times I / 365)$, onde: EM = Encargos moratórios a serem pagos pelo atraso de pagamento; N = Número de dias de atraso contados entre a data limite prevista para o pagamento e a data do efetivo pagamento; VP = Valor da parcela em atraso; e I = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE) / 100.

13.1.6. Os documentos de cobrança deverão ser entregues pela empresa contratada, na SEFAZ, no horário de expediente da CONTRATANTE, ou por e-mail a ser informado quando da assinatura do contrato.

13.1.7. Em nenhuma hipótese será efetuado pagamento de documento fiscal com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice-versa, ou pertencentes ao mesmo grupo ou conglomerado.

13.1.8. Não será realizado qualquer tipo de pagamento através de boleto bancário ou por outro meio diferente do previsto no Contrato.

13.1.9. A Administração CONTRATANTE, no momento do pagamento, providenciará as devidas retenções tributárias, nos termos da legislação vigente, exceto nos casos em que a empresa contratada comprovar, na forma prevista em lei, não lhe serem aplicáveis tais retenções.

13.1.10. Caso a empresa contratada seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das ME e EPP – SIMPLES, desde que não haja vedação legal para tal opção em razão do objeto executado, deverá apresentar, juntamente com o documento fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

13.2. **Do Preço**

13.2.1. Os preços relativos aos serviços contratados serão fixos e irreajustáveis, durante o período de 12 (doze) meses, contado da data de assinatura do Contrato ou do último reajuste.

13.2.2. Após esse período, os preços poderão ser reajustados, mediante a aplicação do **ICTI (Índice de Custo da Tecnologia da Informação)**, calculado pelo Instituto de Pesquisas Econômicas Aplicadas – IPEA, ocorrido no período, ou por outro índice que o venha a substituí-lo.

13.2.3. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

13.3. **Do Equilíbrio Econômico-Financeiro**

13.3.1. Com vistas à manutenção do equilíbrio econômico financeiro do Contrato, poderá ser promovida revisão contratual, desde que eventuais solicitações nesse sentido estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, configurando álea econômica extraordinária e extracontratual, bem como de demonstração analítica de seu impacto nos custos do Contrato, nos termos da Lei nº 14.133/21.

14. **FORMA DE SELEÇÃO DO FORNECEDOR**

14.1. **Da Modalidade e Critério de Julgamento**

14.1.1. Nos termos da Lei Federal nº 14.133/2021 e do Decreto Estadual nº 11.363/23, será realizado o procedimento licitatório na modalidade **PREGÃO**, na **FORMA ELETRÔNICA**, para **REGISTRO DE PREÇOS**, adotando-se como critério de julgamento o **MENOR PREÇO POR LOTE**, em estrita observância aos princípios da eficiência e da economicidade, bem como em conformidade com as diretrizes estabelecidas.

14.2. **Da Escolha do Pregão Eletrônico**

14.2.1. O Pregão Eletrônico é altamente recomendado para contratação de bens e serviços comuns, entendidos como aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos no edital, o que se aplica às soluções de segurança cibernética pretendidas naquele certame. Referidas soluções, mesmo com complexidade técnica, têm especificações padronizadas e requisitos de desempenho descritos objetivamente, possibilitando avaliação clara das propostas e julgamento objetivo do vencedor, conforme disposto no artigo 6º, XIII da Lei nº 14.133/2021.

14.2.2. Conforme o §2º do art. 17 da lei, as licitações serão realizadas preferencialmente sob a **forma eletrônica**, dada sua capacidade de ampliar o acesso, aumentar a participação de interessados e possibilitar maior igualdade entre os concorrentes, vencendo barreiras geográficas e promovendo competição mais aberta e efetiva.

14.2.3. Assim, uso do Pregão Eletrônico atende aos princípios basilares da administração pública, especialmente os da eficiência, economicidade e transparência, previstos no caput do artigo 37 da Constituição Federal, e expressamente reforçados na Lei nº 14.133/2021 (arts. 5º, 6º e 18).

14.2.4. A modalidade eletrônica amplia a participação de fornecedores interessados, inclusive nacionais e internacionais, favorecendo propostas vantajosas para a administração e o melhor uso dos recursos públicos, além de assegurar maior facilidade de fiscalização e controle pelos órgãos competentes. O uso do Pregão Eletrônico também está alinhado às recomendações do Tribunal de Contas da União e das boas práticas de governança em aquisições públicas de soluções TI, estimulando a disputa entre fornecedores qualificados e assegurando a melhor proposta para a Administração.

14.3. **Do Prazo de Validade da Proposta**

14.3.1. O prazo de validade da proposta deverá ser, no mínimo, de 60 (sessenta) dias corridos, a contar da data de sua apresentação.

14.3.2. Na ausência de indicação expressa do prazo de validade, considerar-se-á tacitamente indicado o prazo de 60 dias.

14.3.3. Decorrido o prazo de validade das propostas, sem convocação para assinatura do Contrato, ficam os proponentes liberados dos compromissos assumidos

14.4. **Do Prazo para Assinatura do Contrato**

14.4.1. A assinatura do contrato deverá ocorrer no prazo máximo de 10 (dez) dias corridos, contado da convocação formal do adjudicatário, podendo ser prorrogado, uma única vez, por igual período, mediante solicitação justificada do interessado e aceitação da Administração.

14.4.2. Decorrido o prazo fixado no item anterior, sem que o adjudicatário compareça ou pratique os atos necessários à assinatura do contrato, sem justificativa aceita pela Administração, poderá ser convocado licitante remanescente, mantidas as condições da proposta, sem prejuízo da aplicação das sanções cabíveis previstas no Decreto Estadual nº 11.363/2023 e na Lei Federal

15. QUALIFICAÇÃO TÉCNICA DO LICITANTE

15.1. Atestado de Capacidade Técnica

15.1.1. Para fins de comprovação da capacidade técnico a licitante deverá apresentar **ATESTADO DE CAPACIDADE TÉCNICA** deverá ser fornecido por pessoa jurídica de direito público ou privado que comprove a aptidão para desempenho de atividade pertinente e compatível de acordo com o ramo atividade, objeto deste documento, podendo ser exigido, em diligência, da proposta mais bem classificada, que apresente cópia autenticada do contrato ou da(s) respectiva(s) nota(s) fiscal(is), que deram origem ao atestado.

15.1.1.1. Devem mencionar o fornecimento integrado de plataformas, na modalidade de serviço, compostas por hardware(s) e software(s), e os respectivos serviços associados a operação das respectivas ferramentas, os quais devem contemplar:

- a) Serviços de coleta, armazenamento e correlação entre analytics (logs), inteligência de ameaças e anomalias no comportamento dos usuários da rede (SIEM) com volumetria mínima de 250GBytes/dia para 4.000 usuários;
- b) Serviço de Gestão, análise e tratamento das vulnerabilidades para no mínimo 4.000 ativos;
- c) Serviço de SOC 24x7 alta disponibilidade com implementação, configuração, administração, treinamento e suporte contendo: Detecção e Resposta a Incidentes (CSIRT e Blue Team); Inteligência Avançada de Segurança;
- d) Serviços de Gerenciamento de Postura de Segurança Estendida e Breach and Attack Simulation – BAS para 4.000 usuários;
- e) Serviços de Threat Intelligence com monitoramento de Deep e Dark Web e Takedown.

15.1.1.2. Será permitida a somatória de ATESTADOS desde que seja na mesma tecnologia/serviço prestado, conforme o Acórdão nº 1.214/2013 – Plenário do Tribunal de Contas da União (TCU), em acordo com o disposto no Art. 67, §2º da Lei nº 14.133/2021

15.1.1.3. O ATESTADO deve conter as seguintes informações: Nome da Empresa atestante, endereço, CNPJ, contatos (nome, cargo e telefone), dados do contrato com a empresa CONTRATADA, local de prestação do serviço, datas de início e término das atividades e total de horas executadas.

15.1.1.4. Deve conter a descrição dos serviços prestados, de forma a possibilitar à CONTRATANTE o entendimento dos trabalhos realizados, bem como a aferição de compatibilidade com o objeto deste documento.

15.1.1.5. Somente serão aceitos atestados de capacidades técnicas expedidos após a conclusão do respectivo contrato ou decorrido no mínimo um ano do início de sua execução.

15.1.1.6. Nos casos de ATESTADOS emitidos por empresas de iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da CONTRATADA.

15.1.1.7. A CONTRATADA deve disponibilizar, quando solicitado, todas as informações necessárias a comprovação da legitimidade dos atestados de capacidade técnica apresentados.

15.2. Certificações de Mercado

15.2.1. Para fins de comprovação da capacidade técnico a licitante deverá comprovar as seguintes certificações:

- a) **Certificação ISO/IEC 27001 - Gestão da Segurança da Informação**: válida, emitida por organismo acreditado, atestando que a empresa licitante possui um Sistema de Gestão de Segurança da Informação (SGSI) implementado, em conformidade com padrões internacionais de proteção de dados e mitigação de riscos cibernéticos.
- b) **Certificação ISO/IEC 27701 - Gestão da Privacidade da Informação**: válida, emitida por organismo acreditado, atestando que a contratada possui sistema de gestão de privacidade da informação em conformidade com a LGPD.
- c) **Certificação ISO/IEC-20000-1 - Gestão de Serviços de TI (ITSM)**: válida, emitida por organismo acreditado, comprovando que a licitante implementa um Sistema de Gestão de Serviços de TI (SGSTI) alinhado às boas práticas de governança, entrega, operação e melhoria contínua de serviços tecnológicos.

15.2.2. Será considerado *diferencial técnico* a apresentação de certificação ISO 9001 válida, emitida por organismo acreditado, comprovando que a empresa adota um Sistema de Gestão da Qualidade (SGQ) para processos operacionais, administrativos e técnicos, com foco em melhoria contínua e satisfação do cliente.

15.3. Da Vistoria

15.3.1. Se efetuada a vistoria o Licitante deverá anexar à sua habilitação a DECLARAÇÃO DE VISTORIA (Anexo III).

15.3.2. Caso a LICITANTE renuncie à vistoria técnica, deverá entregar junto à documentação de habilitação, a DECLARAÇÃO DE RENÚNCIA À VISTORIA TÉCNICA (Anexo VI), o qual deverá ser preenchido e assinado pelo interessado em participar da licitação.

15.3.2.1. A não apresentação da Declaração de Renúncia à Vistoria Técnica será motivo de inabilitação.

16. QUALIFICAÇÃO TÉCNICA PARA EXECUÇÃO DO CONTRATO

16.1. A CONTRATADA, para assinatura do Contrato, deverá atender os seguintes requisitos:

16.1.1.

Item 1 - SOC – Security Operations Center

- a) A CONTRATADA deverá compor sua equipe técnica com as seguintes certificações reconhecidas em cibersegurança:
- Certificação obrigatória - CEH - Certified Ethical Hacker;
 - Certificação obrigatória - CYSA+ - CompTIA Cybersecurity Analyst;
 - Certificação obrigatória - Microsoft Certified Solutions Expert (MCSE).
- b) Todos os serviços deverão ser prestados por meio de 1 (um) Centro de operações de SOC da CONTRATADA, conforme requisitos mínimos descritos a seguir:
- Possuir em operação SOC, no mínimo, 2 (dois) canais de comunicação IP dedicados com a Internet, com provedores distintos, para a prestação de serviços de monitoramento e suporte remoto via VPN;
 - Não serão aceitos contratos com links xDSL, devido ao baixo NMS ofertado pelas operadoras de telecomunicação para este tipo de tecnologia;
 - Possuir SOC, linha de nobreaks. Cada linha de energia que atende o SOC deverá ter sua própria linha de nobreaks;
 - Possuir SOC, com no mínimo, 2 (duas) linhas de telefonia fixa, celular ou por IP, de diferentes operadoras. Os números de telefone deverão ser fornecidos pela CONTRATANTE;
 - O perímetro do SOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido.
- c) As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

16.1.2.

Item 2 - Solução para Gestão de Vulnerabilidades

- a) A CONTRATADA deverá compor sua equipe técnica com pelo menos duas das seguintes certificações reconhecidas em cibersegurança:
- CISSP - Certified Information Systems Security Professional;
 - CCSP - Certified Cloud Security Professional;
 - CEH - Certified Ethical Hacker;
 - CYSA+ - CompTIA Cybersecurity Analyst
 - CISM - Certified Information Security Manager.
- b) As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

16.1.3.

Item 3 - Solução para Gerenciamento e Correção de Eventos de Segurança – FortiSIEM

- a) A CONTRATADA deverá compor sua equipe técnica com, no mínimo, um profissional certificado com o Fortinet Certified Solution Specialist (FCSS), bem como apresentar ao menos um profissional com pelo menos duas das seguintes certificações reconhecidas em cibersegurança:
- CEH - Certified Ethical Hacker;
 - CYSA+ - CompTIA Cybersecurity Analyst
 - CompTIA security+;
- b) As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

16.1.4.

Item 4 - Solução de Inteligência contra Ameaças (*Threat Intelligence*)

- a) A CONTRATADA deverá compor sua equipe técnica com pelo menos duas das seguintes certificações reconhecidas em cibersegurança:
- CEH - Certified Ethical Hacker;
 - CYSA+ - CompTIA Cybersecurity Analyst
 - CompTIA security+;
- b) As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

16.1.5.

Item 5 - Solução para Validade de Segurança Contínua – BAS

- a) A CONTRATADA deverá compor sua equipe técnica com pelo menos duas das seguintes certificações reconhecidas em cibersegurança:
- CEH - Certified Ethical Hacker;
 - CYSA+ - CompTIA Cybersecurity Analyst
 - CompTIA security+;
- b) As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

16.1.6.

Item 6 - Solução para Gestão de Acessos Privilegiados – PAM

16.1.6.1. Devido à criticidade das credenciais tratadas pela solução de acessos privilegiados a CONTRATADA deverá apresentar, obrigatoriamente, ATESTADO(S) DE CAPACIDADE TÉCNICA emitido(s) por pessoa jurídica de direito público ou

privado, que comprove(m) que a empresa executou, com qualidade e regularidade, serviços compatíveis com o objeto da licitação (Solução para Gestão de Acessos Privilegiados – PAM), contendo pelo menos as seguintes características mínimas:

- a) Implementação de solução de cofre de senhas voltada ao gerenciamento de credenciais privilegiadas (*PAM – Privileged Access Management*);
- b) Solução com integração mínima de 500 ativos (servidores ou equipamentos);
- c) Prestação de suporte técnico 24x7 à solução;
- d) Execução de serviços de atualização do ambiente e implementação de melhorias;

16.1.7. Item 7 - Consultoria em Serviços Especializados

16.1.7.1. A CONTRATADA deverá compor sua equipe técnica com, no mínimo, um profissional certificado com o *Fortinet Certified Solution Specialist* (FCSS).

16.1.7.2. As certificações deverão ser comprovadas no momento da assinatura do contrato, por meio de documentos oficiais emitidos pelas respectivas entidades certificadoras, sob pena de não conformidade contratual.

17. DA PARTICIPAÇÃO DE CONSÓRCIOS

17.1. Participação de Consórcios

17.1.1. Não Será Admitida a Participação em Consórcios.

17.1.2. Tal vedação fundamenta-se na necessidade de assegurar a exclusiva e incondicionada responsabilização contratual, condição essencial para a adequada prestação de serviços de segurança cibernética de alta complexidade e criticidade. O presente modelo visa garantir o atendimento integral às exigências técnicas e jurídicas atinentes ao objeto licitado, preservando, de igual modo, a efetividade da execução contratual.

17.1.3. A prestação de serviços gerenciados de segurança cibernética demanda, por sua própria natureza, atuação célere e coordenada na resposta a incidentes, requisitos estes manifestamente incompatíveis com a dispersão de responsabilidades que se verifica nos contratos firmados com consórcios. O fracionamento de obrigações, inerente à atuação consorcial, pode comprometer a mitigação de riscos, gerar insegurança jurídica na identificação de responsabilidades e dificultar, por conseguinte, a aplicação de sanções proporcionais em caso de falhas de execução.

17.1.4. Nesse cenário, a confidencialidade e a governança rigorosa requeridas para a proteção de dados e sistemas sensíveis são mais adequadamente asseguradas sob a responsabilidade unificada de um único fornecedor. Tal centralização contribui para a eficiência da fiscalização, a efetividade da auditoria e a viabilidade de adoção de medidas corretivas e punitivas sempre que necessárias. Ademais, a contratação unilateral favorece a padronização tecnológica, a interoperabilidade das soluções e a simplificação da gestão contratual, todos elementos imprescindíveis ao êxito de serviços dessa natureza.

17.1.5. A jurisprudência do Tribunal de Contas da União corrobora esse entendimento. O Acórdão nº 2430/2024-TCU-Plenário, no âmbito da Política Nacional de Cibersegurança, realça a necessidade de responsabilização clara e exclusiva do contratado, como condição para garantir a continuidade, a segurança e a integridade das soluções implementadas. Igualmente, o Acórdão nº 2808/2021 reforça a imprescindibilidade da responsabilização integral diante dos riscos inerentes à segurança nacional. No mesmo sentido, o Acórdão nº 1768/2022-Plenário adverte expressamente que a dispersão contratual típica dos consórcios constitui risco à eficiência e à integridade das soluções de segurança cibernética.

17.1.6. No campo doutrinário, Maria Sylvia Zanella Di Pietro[37] afirma que a Administração Pública pode, em razão da natureza do objeto e para resguardar o interesse público, estabelecer limitações proporcionais e justificadas ao modo de participação dos licitantes. Nas hipóteses em que se identifica elevada complexidade e risco — como se observa nos serviços críticos de segurança cibernética — reforça-se a necessidade de centralizar as responsabilidades em um único executor.

17.1.7. No caso dos serviços de segurança cibernética os riscos atinentes à proteção de dados sensíveis e à continuidade operacional demandam garantias especiais de integridade e prontidão na resposta a incidentes. A fragmentação de obrigações, neste cenário, afrontaria os princípios da proporcionalidade e da segurança jurídica, acarretando à Administração Pública o ônus de identificar corresponsáveis em eventuais situações de crise, o que seria inadmissível diante da urgência e da gravidade dos riscos.

17.1.8. Assim, a vedação proposta encontra amparo em três dimensões complementares:

- Na lei, ao atender aos princípios da legalidade, da eficiência e do interesse público, na forma do artigo 37 da Constituição Federal e da Lei nº 14.133/2021;

- Na doutrina, que reconhece a legitimidade de restrições proporcionais, desde que necessárias à preservação da efetividade contratual;

- Na jurisprudência consolidada do TCU, que recomenda a exclusão de consórcios em contratos que envolvam elevada criticidade.

18. ATA DE REGISTRO DE PREÇOS

18.1. Assinatura

18.1.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o **prazo de 05 (cinco) dias**, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

18.1.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

- I - a solicitação seja devidamente justificada e apresentada dentro do prazo; e
- II - a justificativa apresentada seja aceita pela Administração.

18.1.3. A Ata de Registro de Preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

18.1.4. Será formalizada Ata de Registro de Preços com a indicação do licitante vencedor, a descrição dos itens, as respectivas quantidades, preços registrados e demais condições.

18.2. **Vigência**

18.2.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogado por igual período, desde que comprovado o preço vantajoso, nos termos do art. 22, do Decreto nº 11.462/23.

18.3. **Alteração ou atualização dos preços registrados**

18.3.1. Com vistas à manutenção do equilíbrio econômico-financeiro da ATA, poderá ser promovida revisão dos preços registrados, desde que eventuais solicitações estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, nos termos do disposto no art. 25, do Decreto nº 11.462/2023.

18.4. **Da Adesão e Obrigações do Órgão Gerenciador/Detentor da Ata**

18.4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, 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:

- a) apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
- b) 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
- c) consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

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

18.4.3. 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.

18.4.4. 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 noventa dias, observado o prazo de vigência da ata.

18.4.5. 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.

19. **DA ADEQUAÇÃO ORÇAMENTÁRIA**

19.1. As despesas decorrentes da contratação correrão à conta dos recursos consignados abaixo, de acordo com a informação de Dotação Orçamentária:

19.2. Descrição da Dotação Orçamentária:

Órgão	715	Secretaria de Estado da Fazenda - SEFAZ
Unidade Orçamentária	001	Unidade Gestora
Programa de Trabalho	04.129.1466.1198.00.00	Modernização dos Sistemas de Arrecadação, Administração Financeira, Tributária e Contábil
Elemento de Despesa		

<i>Detalhamento da Conta Orçamentária</i>		
<i>Fonte de Recurso</i>	<i>15000.100</i>	<i>Recursos próprios do tesouro</i>

20. RESPONSABILIDADES

Elaborado por:
DIVISÃO DE PROJETOS - DIPROJ

Requisitante/Revisor
ISRAEL JORDÃO SANTOS DE MELO
Chefe do Departamento de Tecnologia da Informação
Portaria nº 13/2023

Vistos os autos, no uso de minhas atribuições, em cumprimento ao disposto no artigo 72, inciso VIII da Lei de Licitações e Contratos nº 14.133/2021, AUTORIZO a Licitação, ratificando a importância do objeto para o desempenho das atividades desta Unidade Administrativa e os elementos técnicos apresentados para fundamentar a contratação.

Encaminha-se à Diretoria de Administração e Finanças para as demais providências.

José Amarísio Freitas de Souza
Secretário de Estado da Fazenda
Decreto nº 4.059-P/2023

21. ANEXOS

21.1. Anexo I - Especificações Técnicas Mínimas dos Componentes

21.1.1. A prestação, por empresa especializada, de serviços gerenciados de segurança cibernética na modalidade SaaS (Software as a Service), com fornecimento das respectivas soluções de software e serviços técnicos especializados, para suprir as demandas da Secretaria de Estado da Fazenda do Acre, deverá atender as condições e especificações técnicas mínimas detalhadas no quadro a seguir:

1.2 CARACTERÍSTICAS GERAIS DO OBJETO

1.2.1 São os requisitos para a prestação de Serviços de Segurança Cibernética no ambiente da Sefaz AC, incluindo Serviços de Security Operations Center (SOC) e Fornecimento das respectivas ferramentas:

1.2.1.1 Serviços destinados a garantir a segurança das comunicações entre os sistemas da Sefaz AC;

1.2.1.2 O monitoramento contínuo de todos os ativos de TI e sistemas, além da identificação de vulnerabilidades e a prevenção contra ataques cibernéticos;

1.2.1.3 Verificação de potenciais vulnerabilidades de forma a mitigar ataques e consequentemente danos;

1.2.1.4 Estes serviços possibilitarão identificar imediatamente de forma Preventiva e corretiva:

1.2.1.4.1 Potenciais e futuros problemas e gargalos – Preventiva;

1.2.1.4.2 Falhas causando Degradação de desempenho e suas respectivas causas;

1.2.1.4.3 Interrupção dos Serviços e suas respectivas causas;

1.2.1.4.4 Detecção de ameaças cibernéticas à sistemas, tais como como tentativas de invasão e/ou paralisação: páginas web, aplicativos, bases de dados etc.;

1.2.1.4.5 Solução de problemas de segurança encontrados com agilidade e eficiência;

1.2.1.4.6 Monitorar e analisar processos de forma contínua para identificar riscos de segurança na infraestrutura de TI.

1.2.1.5 Além disso os serviços prestados atuarão em tempo real e sobre todos os sistemas monitorados, para:

1.2.1.5.1 Registrar e documentar todas as ocorrências acima listadas incluindo as que ameacem a segurança do ambiente de TI;

1.2.1.5.2 Acionar os respectivos responsáveis seja na própria Sefaz/AC, seja para os respectivos fornecedores da contratante, para prestação dos serviços eventualmente afetados ou responsáveis pelas falhas;

1.2.1.5.3 Acompanhar a resolução dos problemas e apontar as soluções e providências tomadas;

1.2.1.5.4 Gerar documentação através de relatórios de forma a possibilitar o acompanhamento dos chamados, tempos de resposta versus tempo contratado, possibilitando que a Sefaz/AC realize a gestão adequada e necessária a boa prestação dos serviços a seus públicos interno e externo.

1.2.1.6 Fornecimento de serviços que proporcione segurança nos sistemas da SEFAZ/AC, identificando e mitigando potenciais vulnerabilidades e ataques, pelo prazo de 60 meses, exceto item 5 (cinco) que é pelo prazo de 24 meses.

2 DETALHAMENTO DOS SERVIÇOS

2.1 SOC - SECURITY OPERATIONS CENTER

2.1.1 Requisitos Gerais

2.1.1.1 Todos os serviços deverão ser prestados por meio de 1 (um) Centro de operações de SOC da CONTRATADA.

2.1.1.2 Possuir em operação SOC, com no mínimo, 2 (dois) canais de comunicação IP dedicados com a Internet, com provedores distintos, para a prestação de serviços de monitoramento e suporte remoto via VPN.

2.1.1.2.1 Não serão aceitos contratos com links xDSL, devido ao baixo NMS ofertado pelas operadoras de telecomunicação para este tipo de tecnologia.

2.1.1.3 Possuir SOC, linha de nobreaks. Cada linha de energia que atende o SOC deverá ter sua própria linha de nobreaks.

2.1.1.4 Possuir SOC, com no mínimo, 2 (duas) linhas de telefonia fixa, celular ou por IP, de diferentes operadoras.

2.1.1.5 O perímetro do SOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido.

2.1.1.6 Possuir certificação ISO/IEC-20001.

2.1.1.7 Possuir Certificação ISO/IEC 27001.

2.1.1.8 Possuir Certificação ISO/IEC 27701.

2.1.1.9 Possuir Certificação ISO/IEC 9001.

2.1.1.10 A Contratada deverá disponibilizar "Central de Atendimento" para realização de requisições de execução de serviços ou resolução de dúvidas, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante número do tipo 0800, garantindo alta disponibilidade.

2.1.1.10.1 Esse serviço poderá ser disponibilizado em meio eletrônico e/ou e-mail.

2.1.1.11 Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

2.1.1.11.1 A sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL (Secure Socket Layer), com certificado digital emitido em nome da CONTRATADA.

2.1.1.11.2 A CONTRATADA deve garantir que os canais de comunicação, utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.

2.1.1.12 O Centro de operações SOC da CONTRATADA deverá dispor de uma solução de ITSM (*Information Technology Service Management*) - Gerenciamento de Serviços de TI.

2.1.1.12.1 A ferramenta de gestão de chamados deverá ter seus processos de gestão de incidentes, gestão de problemas, gestão de requisições e gestão de mudanças aderentes ao modelo ITIL v4.

2.1.1.12.2 A solução de gestão de chamados deverá realizar o controle automático dos ANSs (Acordos de Nível de Serviço) dos chamados, notificando e escalonando os chamados próximos de um rompimento.

2.1.1.12.3 A solução de gestão de chamados deverá possibilitar o envio automático, por e-mail, de relatórios à usuários pré-determinados pela contratante;

2.1.1.12.4 A solução de gestão de chamados deverá possuir API de integração via REST/SOAP

2.1.1.12.5 A Ferramenta de gestão de chamados deve ser um produto acabado, totalmente funcional e que atenda a todas as especificações técnicas estabelecidas neste termo de referência. Não serão aceitas versões incompletas ou beta do software. O software deve estar pronto para uso imediato, sem a necessidade de atualizações ou modificações para cumprir os requisitos estabelecidos;

2.1.1.12.6 A CONTRATADA deverá disponibilizar plataforma de gerenciamento de demandas e incidentes, denominado chamados, que deverá permitir as seguintes ações:

2.1.1.12.6.1 Encerrar automaticamente os chamados a partir do recebimento de e-mail;

2.1.1.12.6.2 Encaminhar e-mail aos usuários informando no corpo do e-mail o nome do responsável pelo atendimento do chamado, número do chamado e descrição da solução adotada;

2.1.1.12.7 O intervalo de tempo para início de atendimento do chamado, de acordo com a severidade, deverá observar os seguintes critérios:

- Severidade 1 (um): 2 (duas) horas;

- Severidade 2 (dois): 4 (quatro) horas;

- Severidade 3 (três): 8 (oito) horas; e

- Severidade 4 (quatro): 24 (quatro) horas.

2.1.1.12.8 A severidade varia de 1 (um) a 4 (quatro), sendo 1 (um) a mais crítica e 4 (quatro) a menos crítica.

2.1.1.12.9 A severidade é descrita da seguinte forma:

2.1.1.12.9.1 Severidade 1 (um) - Interrupção de serviço crítico:

- Um serviço crítico em ambiente de produção está indisponível e nenhuma solução de contingência está disponível;

- Um serviço crítico em ambiente de produção, como realização de backup (Precisa desse exemplo? Está parado ou não responde e não está sendo possível estabilizá-lo ou reiniciá-lo);

2.1.1.12.9.2 Severidade 2 (dois) - Funcionalidades principais:

- Uma ou mais funcionalidades estão severamente prejudicadas;

- O uso da ferramenta pode continuar de forma restrita, apesar da produtividade em longo prazo poder ser afetada;

- Possíveis problemas críticos antes de uma atualização;

- Existe solução de contorno temporária para o problema.

2.1.1.12.9.3 Severidade 3 (três) - Funcionalidades menores:

- Uma ou mais funcionalidades não críticas não estão funcionando, existindo solução de contorno disponível;

- Perda parcial, não crítica, de funcionalidade;

- Funcionamento de alguns componentes prejudicados, permitindo a continuidade de uso;

- Possíveis problemas não críticos antes de uma atualização.

2.1.1.12.9.4 Severidade 04 (quatro) - Perguntas gerais de utilização:

- Questões referentes à aparência do produto, incluindo erros na documentação;

- Dúvidas quanto à configuração geral ou quanto ao uso do produto;

- Notificações sobre upgrade, grandes mudanças e migração;

- Pedidos de melhorias.

2.1.1.12.10 A CONTRATANTE avaliará os serviços prestados pela CONTRATADA por meio da utilização de indicadores de desempenho, que são critérios objetivos e mensuráveis estabelecidos entre CONTRATANTE e CONTRATADA, no intuito de aferir aspectos de qualidade relacionados aos serviços realizados.

2.1.2 Serviços de Monitoramento de Segurança Cibernética - SOC

2.1.2.1 Prestação de serviços deverá ser gerenciado obrigatoriamente através de SOC – Security Operations Center/Centro de Operações de Segurança.

2.1.2.1.1 Tem por objetivo o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados a CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas a CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

2.1.2.2 Toda a prestação dos serviços se dará na modalidade “Software as a Service - SaaS”, onde os softwares necessários para a proteção do ambiente são fornecidos e operados pela contratada.

2.1.2.2.1 A CONTRATADA deverá garantir a aplicação contínua das melhores práticas. Tal modelo evidencia-se mais efetivo e possibilita a utilização de produtos, serviços, soluções de segurança por um menor custo, haja vista a possibilidade de utilização de recursos em escala, por serem compradas em grande quantidade pelo fornecedor para atender a diversos clientes e, dessa maneira obtendo vantagens de preços aquisitivos.

2.1.2.2.2 Portanto, considerando a importância dos serviços de segurança de TIC e para a proteção dos diversos ativos, serviços e sistemas da CONTRATANTE, aliado à insuficiência de profissionais especializados em seu quadro de colaboradores e necessários ao atendimento dessa demanda, torna-se essencial para a adequada proteção do ambiente tecnológico a contratação de Prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA.

2.1.2.2.3 Prestação de Serviços Gerenciados de Segurança da Informação com o fornecimento de Solução de Correlação e Gerenciamento de Eventos de Segurança (SIEM), Solução de Gestão de Vulnerabilidades, solução de Threat Intelligence, Solução de BAS, Solução de Cofre de Senhas contemplando também Suporte Técnico aos Serviços e Soluções contratadas. Atendimento de Chamados através de Sistema de Service Desk, também e inclusive a prestação concomitante dos demais Serviços, dos quais deverão ser prestados por uma única empresa vencedora deste termo de referência, descritos nos itens abaixo e no inteiro teor deste TR:

2.1.3 Centro de Operação de Operações de Segurança (SOC)

2.1.3.1 Os Serviços Gerenciados de Segurança deverão ser prestados por meio de estrutura de SOC - Security Operation Center, obrigatoriamente no Brasil.

2.1.3.2 O SOC deverá ser provido em ambiente físico próprio da CONTRATADA, para sustentar e operar toda a solução e produtos que estiverem relacionados com a Segurança da Informação, assim como do Parque Computacional da CONTRATANTE, com a realização continuada de ações proativas voltadas para mantê-lo estável, seguro, em pleno e normal funcionamento, sempre disponível e inalterada.

2.1.3.3 A CONTRATADA deve possuir ferramenta automatizada para prover os serviços de monitoramento e visibilidade de ataques cibernéticos como serviço assim como equipe técnica capacitada para analisar os indicadores fornecidos pelas ferramentas, indicando proativamente a existência de incidentes cibernéticos, sendo definido como um evento com potencial de ocasionar uma possível violação na política de segurança da informação da CONTRATANTE.

2.1.3.4 A CONTRATADA deve notificar a CONTRATANTE diante da detecção de qualquer evento suspeito, provendo todo o embasamento que respalde a notificação encaminhada.

2.1.3.4.1 As atividades de monitoramento consistem em detecção, triagem, categorização, priorização, análise inicial, notificação, contenção (quando aplicável), resposta a incidente com recomendações para contenção, mitigação, erradicação, assim como escalonamento (quando aplicável).

2.1.3.4.2 A equipe do SOC deverá ser formada por profissionais N1, profissionais N2 e Gerente de SOC;

2.1.3.5 Esse serviço será dividido em dois níveis (nível 1-N1 e nível 2-N2), com foco nos Ativos e Sistema de TIC da CONTRATANTE.

2.1.3.6 Avaliações de incidentes devem seguir Frameworks consolidados no mercado de segurança da informação, como SANS e NIST.

2.1.3.7 Incidentes devem ser enriquecidos com Threat Modelings consolidados no mercado de segurança da informação, como MITRE, CVSS e Cyber Kill Chain.

2.1.3.7.1 Essas metodologias são reconhecidas internacionalmente como as melhores práticas de segurança cibernética e devem ser aplicadas pela CONTRATADA para garantir a conformidade com as normas e regulamentações aplicáveis.

2.1.3.8 Monitorar e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados etc.), propondo ações corretivas e de melhorias.

2.1.3.9 Cabe a equipe técnica da CONTRATADA, apoiar as integrações pertinentes para que os logs de segurança sejam encaminhados adequadamente as soluções de monitoramento.

2.1.3.10 Nos processos de integrações, a CONTRATADA se compromete a aplicar sua expertise em monitoramento para a seleção dos dados que realmente se requerem para o monitoramento do ambiente TIC da CONTRATANTE.

2.1.3.11 Como processo contínuo, a CONTRATADA realizará processos de Tuning na solução ofertada, visando qualificar os eventos identificados e diminuir detecções de eventos classificados como falso positivo.

2.1.3.12 A CONTRATADA executará o monitoramento do ambiente TIC da CONTRATANTE em busca de Precursores, Incidentes e Indicadores de Comprometimento assim como qualquer alerta de segurança disponível.

2.1.3.13 Durante o processo de Triagem, comportamentos suspeitos poderão ser notificados até que comportamentos comuns sejam

identificados e documentados, evitando assim sobrecarga futura da equipe de SI da CONTRATANTE.

2.1.3.14 A Classificação e Priorização dos incidentes de segurança seguirão modelos adotados pela CONTRATADA, seguindo rigorosamente os Frameworks adotados pelo mercado de segurança cibernética.

2.1.3.14.1 Caso a CONTRATANTE requeira revisão de Classificações e Prioridades, estas devem ser realizadas em comum acordo durante o processo de contratação dos serviços.

2.1.3.15 A contenção de determinados tipos de eventos, podem ficar a cargo da CONTRATADA, desde que haja previamente um acordo entre partes, e ele seja documentado em procedimentos e playbooks.

2.1.3.16 Com base em ferramentas de Threat Intel, públicas ou privadas, os incidentes em segurança cibernética serão enriquecidos provendo o adequado insumo para a tomada de decisão da equipe de SI da CONTRATANTE.

2.1.3.17 A CONTRATADA, deve, por meio de seu documento de Resposta a Incidente, subsidiar a equipe de SI da CONTRATANTE no que tange aos procedimentos para adequada contenção, remediação e erradicação de um incidente.

2.1.3.18 Incidentes de segurança terão seus respectivos documentos de Resposta a Incidente lavrados assim como seu adequado registro em ferramenta de ITSM.

2.1.3.19 Incidentes de segurança cibernética que sejam prioritários e atendam critérios de criticidades dispostos neste documento, terão seu fluxo de escalonamento seguidos conforme alinhado entre partes interessadas.

2.1.3.20 Para incidentes críticos, equipe de CSIRT interna pode ser engajada no suporte a contenção, remediação e erradicação, sem custos adicionais a CONTRATANTE.

2.1.3.21 A CONTRATADA se dispõe a realizar buscas ativas, Threat Hunting, nas soluções de segurança ofertadas em busca de eventos anômalos que possam afetar integridade, disponibilidade e confidencialidade dos ativos TIC da CONTRATANTE.

2.1.3.22 Incidentes e requisições podem ter como natureza de contato, telefone, e-mail, chat e portal de autoatendimento.

2.1.3.23 Independente da natureza de contato realizada, o ITSM deverá gerar código único de registro para posterior acompanhamento.

2.1.3.24 A ferramenta de ITSM notificará a Contratante com número único de registro assim como permitirá a contratante o acompanhamento de seus incidentes e requisições.

2.1.3.24.1 Caso acordado previamente, o registro dos eventos pode ser realizado na ferramenta de ITSM da CONTRATANTE.

2.1.3.25 Registros nas ferramentas de ITSM, tanto para incidentes, requisições e mudanças, devem seguir as melhores práticas oferecidas por Frameworks como ITIL.

2.1.3.26 Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades.

2.1.3.26.1 É de responsabilidade da CONTRATADA a criação, revisão e manutenção de tais procedimentos operacionais, sendo de responsabilidade da CONTRATANTE apenas participar como aprovador sempre que um procedimento for criado e/ou sofrer algum tipo de alteração.

2.1.3.26.2 É de responsabilidade da CONTRATADA manter uma base de conhecimento, com todos os procedimentos pré-estabelecidos e aprovados pela CONTRATANTE.

2.1.3.26.3 Tal base de conhecimento deve fazer parte do sistema de acompanhamento de chamados, e a qualquer tempo deve estar acessível à CONTRATANTE para consultas, aprovações e alteração de novos procedimentos (conforme acordado entre as partes).

2.1.3.27 A CONTRATANTE poderá requisitar a CONTRATADA para realizar integração de sua ferramenta de ITSM, com o ITSM da CONTRATANTE, formando uma base de conhecimento de todos os incidentes e requisições de serviço unificada.

2.1.3.28 A CONTRATADA deve desenvolver e implementar uma variedade de playbooks de atendimento de incidentes que abordem os diferentes tipos de incidentes de segurança que possam ocorrer nos ativos de TIC da CONTRATANTE.

2.1.3.28.1 Esses playbooks devem incluir procedimentos claros para avaliação de incidentes, priorização, categorização, triagem e resposta.

2.1.3.29 Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração.

2.1.3.30 A CONTRATADA deve fornecer um conjunto abrangente de indicadores de segurança e dashboards personalizados para que a CONTRATANTE possa avaliar continuamente a eficácia dos serviços.

2.1.3.31 A CONTRATADA realizará reuniões periódicas visando apresentar pontos que requeiram atenção de partes interessadas, assim como alinhamento de expectativas com a CONTRATANTE.

2.1.3.32 Das atividades da equipe como sendo N1:

2.1.3.32.1 Receber alertas das soluções de segurança e de fontes de Deep e Dark Web e registrar os eventos e incidentes na ferramenta de ITSM.

2.1.3.32.2 Analisar os eventos registrados na ferramenta de ITSM, realizando a triagem dos verdadeiros positivos e falsos positivos.

2.1.3.32.3 Definir prioridade dos eventos considerados como verdadeiros positivos de acordo com escala de criticidade definidas junto a CONTRATANTE.

2.1.3.32.4 Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATADA.

2.1.3.32.5 Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA, em especial com buscas em registros de SIEM e dados de CTI.

2.1.3.32.6 Encaminhar eventos que não sejam de sua alçada ao N2 de acordo com os playbooks definidos pela CONTRATADA.

2.1.3.32.7 Acompanhar e encerrar os eventos após sua solução.

2.1.3.32.8 Sugerir ao Gerente do SOC melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.

2.1.3.32.9 O serviço deve ser prestado de segunda-feira a sexta-feira, no horário comercial, presencialmente por um analista júnior de cibersegurança e remotamente pelo restante da equipe no formato 24x7.

2.1.3.33 Das atividades da equipe com o sendo N2:

2.1.3.33.1 Tratar os eventos que forem de sua alçada de acordo com os playbooks definidos pela CONTRATANTE.

2.1.3.33.2 Reclassificar eventos como falso positivo ou rever a prioridade, quando houver divergência de entendimento com relação ao definido pelo N1.

2.1.3.33.3 Analisar os eventos identificados, criando documento de Resposta a Incidente com as devidas ações de contenção, remediação e erradicação sugeridas as equipes resolvidoras.

2.1.3.33.4 Enriquecer os dados dos eventos a partir das fontes de dados disponibilizadas pela CONTRATADA, em especial com buscas em registros de SIEM e dados de CTI.

- 2.1.3.33.5 Na ocorrência de eventos de alta criticidade, alertar o Gerente do SOC formalmente, assim como proceder com matriz de escalonamento prevista.
- 2.1.3.33.6 Redirecionar incidentes para equipe N1 após tratativas realizadas para acompanhamento e encerramento.
- 2.1.3.33.7 Realizar atividades de Threat Hunting, em busca ativa por atividades suspeitas no ambiente da CONTRATANTE.
- 2.1.3.33.8 Realizar atividades de tuning nas ferramentas oferecidas pela CONTRATADA para aprimorar a cobertura dos eventos em segurança cibernética.
- 2.1.3.33.9 Revisar atividades de parseamento, buscando que as ferramentas proporcionem dados qualitativos em seus eventos.
- 2.1.3.33.10 Acompanhar e suportar integrações entre os ativos de segurança da CONTRATANTE junto a solução oferecida da CONTRATADA.
- 2.1.3.33.11 Sugerir ao Gerente do SOC melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.
- 2.1.3.33.12 Realizar melhorias nos playbooks após alinhamento entre partes interessadas.
- 2.1.3.33.13 Gerar relatórios técnicos dos eventos e incidentes de segurança cibernética
- 2.1.3.34 Das atividades Gerenciais:
- 2.1.3.34.1 Coordenar tecnicamente os serviços e o andamento das atividades, projetos e demandas das equipes N1 e N2 do SOC;
- 2.1.3.34.2 Supervisionar os perfis profissionais do N1 e N2 delegar responsabilidades e serviços às equipes e acompanhar seu desempenho;
- 2.1.3.34.3 Gerir o cumprimento de metas e indicadores estabelecidos
- 2.1.3.34.4 Elaborar relatórios de acompanhamento dos indicadores de serviço, assim como propostas de melhorias da execução do serviço e de sua medição;
- 2.1.3.34.5 Garantir o bom desempenho da equipe
- 2.1.3.34.6 Manter a equipe N1 e N2 devidamente treinada e apta a prestar os serviços ora contratados;
- 2.1.3.34.7 Fornecer informações solicitadas pela CONTRATANTE;
- 2.1.3.34.8 Assegurar que os processos operacionais tenham melhoria contínua e atendam aos Indicadores e metas acordadas em contrato;
- 2.1.3.34.9 Realizar auditorias dos atendimentos dos eventos e incidentes cibernéticos e tickets realizados pelos perfis profissionais de N1 e N2, com o objetivo de avaliar e aferir a observância aos padrões, procedimentos e qualidade do serviço prestado, bem como o cumprimento dos scripts, playbooks, padrões de cordialidade e empatia exigidos;
- 2.1.3.34.10 Apresentar Relatório de acompanhamento de indicadores de uso de recursos, atendimento, desempenho e utilização do serviço.
- 2.1.4 Serviços de Computer Security Incident Response Team – CSIRT**
- 2.1.4.1 A CONTRATADA deve oferecer equipe multidisciplinar responsável por responder incidentes.
- 2.1.4.2 A equipe de CSIRT, deve atuar com uma equipe técnica, também corroborando com atividades que extrapolam o âmbito tecnológico, quando os eventos de um incidente carecem de interações com outras equipes como departamento jurídico, relações públicas, recursos humanos e compliance.
- 2.1.4.2.1 Este processo é fundamental para auxiliar a contratante em incidentes que envolvam exfiltração de dados sensíveis, comunicações com ANPD, incidentes que afetem confiança e reputação da marca entre outros. A contratante pode requisitar o atendimento presencial da figura do gerente de segurança a qualquer momento na sede da contratante.
- 2.1.4.3 A CONTRATADA deverá possuir sólidos conhecimentos de configuração de ORACLE DATABASE SERVER com as melhores práticas de segurança, como criptografia de dados em repouso e em trânsito para apoiar o time local da Contratante.
- 2.1.4.4 Conhecimento em autenticação forte e chaves de criptografia seguras para apoiar o time local da Contratante.
- 2.1.4.5 Conhecimento em monitoramento contínuo de atividades no ORACLE DATABASE SERVER para detectar atividades suspeitas, para que em caso de possível exfiltração de dados, apoiar o time da contratante.
- 2.1.4.6 Entender alertas para comportamentos incomuns que possam indicar uma possível violação de segurança.
- 2.1.4.7 Ajudar a planejar estratégias de backup off-site, implementar políticas de retenção de backups e garantir conformidade com regulamentos de segurança e privacidade de dados.
- 2.1.4.8 Validar procedimentos de recuperação em conjunto com a contratante. Isso inclui garantir que os backups sejam validados regularmente e que os procedimentos de restauração sejam claros, documentados e eficazes em caso de necessidade de recuperação de dados.
- 2.1.4.9 A contratada deverá auxiliar a Contratante em caso de incidente de segurança, no que tange a desenvolver e implementar estratégias de backup e recuperação que atendam às necessidades específicas da organização. Isso inclui sugerir frequência dos backups, os tipos de backup a serem utilizados (completo, diferencial, log), e onde os backups serão armazenados.
- 2.1.4.10 Planejar junto a Contratante as configurações adequadas podem melhorar significativamente o desempenho do ORACLE DATABASE SERVER. Isso inclui ajustar configurações de memória, definir tamanhos de arquivo de banco de dados apropriados, otimizar o uso de CPU e I/O, entre outros ajustes.
- 2.1.4.11 Conhecer sistemas de detecção de intrusão e anomalias no SQL Server para que junto com a contratada, possa identificar atividades suspeitas, como tentativas de acesso não autorizado, consultas SQL incomuns ou tentativas de exfiltração de dados.
- 2.1.4.12 Apoiar a contratante com um plano para validar se os backups dos bancos de dados ORACLE DATABASE SERVER sejam realizados regularmente e que sejam armazenados de maneira segura. O DBA é necessário para garantir a integridade dos backups e a capacidade de restauração rápida em caso de comprometimento dos dados.
- 2.1.4.13 Planejar junto a CONTRATANTE para manter o ORACLE DATABASE SERVER e outros componentes relacionados atualizados com os patches de segurança mais recentes para proteger contra vulnerabilidades conhecidas.
- 2.1.4.14 Conhecer ambiente Microsoft 365 para que modo de consultoria, apoiar a CONTRATANTE sobre serviços de segurança e conformidade que se integram diretamente com o Azure.
- 2.1.4.15 Desenvolver e implementar políticas de proteção de informações e garantir conformidade com regulamentos em conjunto com a CONTRATANTE.
- 2.1.4.16 Apoiar a contratante com procedimentos e soluções de proteção de informações e prevenção de perda de dados (DLP).
- 2.1.4.17 Em caso de exfiltração de dados, a CONTRATADA deverá elaborar em conjunto com a CONTRATANTE um plano para

- desenvolver e implementar políticas de proteção de informações (DLP) e Azure Information Protection (AIP).
- 2.1.4.18 Conhecer Microsoft Compliance Center para apoiar a CONTRATANTE na garantia da conformidade com regulamentos como LGPD.
- 2.1.4.19 Apoiar auditorias de conformidade e indicar à CONTRATANTE como implementar soluções de retenção e arquivamento de dados.
- 2.1.4.20 A CONTRATADA deverá auxiliar a CONTRATANTE na criação de documentação detalhada sobre políticas, procedimentos e configurações do ambiente Microsoft 365.
- 2.1.4.21 Visando assegurar a qualidade dos serviços prestados no escopo da Consultoria Especializada On Demand, especialmente no que se refere ao apoio às atividades de Resposta a Incidentes de Segurança da Informação (CSIRT), serão adotados Acordos de Nível de Serviço (SLA) conforme padrões de mercado e boas práticas de segurança.
- 2.1.4.22 Tabela SLA time CSIRT:

Classificação dos incidentes	Exemplo	Tempo Máximo de Resposta Inicial	Tempo Máximo de Resolução	Canal
Crítico (P1)	Vazamento de dados pessoais sensíveis, ransomware ativo, indisponibilidade total de serviço crítico	30 minutos (24x7)	4 horas	Telefone + e-mail
Alto (P2)	Comprometimento de credenciais privilegiadas, <i>lateral movement</i> identificado	1 hora (dias úteis)	8 horas	E-mail ou ITSM
Médio (P3)	Atividade anômala detectada, incidente sem impacto imediato	4 horas (dias úteis)	2 dias úteis	E-mail ou ITSM
Baixo (P4)	Solicitação de análise forense ou orientação técnica	1 dia útil	5 dias úteis	E-mail

- 2.1.4.22.1 Descrição:
- Tempo de Resposta Inicial: intervalo entre o aceite da solicitação e o início da análise técnica.
 - Tempo de Resolução: tempo estimado para contenção ou recomendação de remediação inicial do incidente.
- 2.1.4.22.2 A contratada deverá manter equipe capacitada para operar sob esse SLA, podendo recorrer à equipe de CSIRT interna ou de fabricantes/parceiros homologados.
- 2.1.4.22.3 Todos os incidentes deverão ser documentados, com elaboração de relatório técnico contendo: diagnóstico, impacto, causa raiz (quando aplicável), ações tomadas e recomendações de melhoria.
- 2.1.4.22.4 A CONTRATADA deverá prover um canal de atendimento prioritário (telefone/e-mail de emergência) para acionamento de incidentes críticos, 24x7.
- 2.1.5 Certificação Profissional da Equipe de Serviços de SOC**
- 2.1.5.1 Devido à complexidade das ferramentas que deverão ser suportadas pela CONTRATADA e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõe o parque de segurança do Contratante atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com profissionais que possuam ao menos três das certificações abaixo:
- CEH - Certified Ethical Hacker
 - CYSA+ - CompTIA Cybersecurity Analyst
 - Microsoft Certified Solutions Expert (MCSE): Server Infrastructure
 - NSE4 - Network Security Expert Level 4
 - FCSS - Fortinet Certified Solution Specialist
 - Fortinet FCP – Network Security
 - CISCO CCNP - Cisco Certified Network Professional
- 2.1.6 Serviços de Instalação**
- 2.1.6.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.
- 2.1.6.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;
- 2.1.6.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;
- 2.1.6.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;
- 2.1.6.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;
- 2.1.6.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;
- 2.1.6.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;
- 2.1.6.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.
- 2.1.6.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.
- 2.1.6.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da

CONTRATANTE.

2.1.6.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.1.6.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.1.6.10 A montagem e instalação de todos os componentes que compoñham solução adquirida são de responsabilidade da CONTRATADA.

2.1.6.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.1.6.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.1.6.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.1.6.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.1.6.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.1.6.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.1.6.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.1.6.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.1.6.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.1.6.18 A substituição definitiva será admitida com anuência da CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, software, peça e componente ofertado, em relação àquele que está sendo substituído.

2.2 SOLUÇÃO DE GESTÃO DE VULNERABILIDADES

2.2.1 O Serviço de Gestão de Vulnerabilidades tem por objetivo identificar possíveis vulnerabilidades de segurança da informação no parque computacional e serviços de TIC do CONTRATANTE, a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.

2.2.2 A CONTRATADA deverá realizar varreduras com periodicidade mínima mensal de todas as aplicações, ativos e recursos apresentados como escopo do CONTRATANTE.

2.2.3 É responsabilidade da CONTRATANTE informar a lista de ativos e serviços críticos de seu ambiente.

2.2.4 A CONTRATANTE disponibilizará os recursos de hardware e software para instalação do Scanner na rede e fará as devidas liberações na rede para que o scanner alcance os ativos.

2.2.5 O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. O início do processo não se limita apenas em rotinas de tempo definidas, mas poderá o CONTRATANTE também solicitar análises sob demanda a qualquer tempo.

2.2.6 A CONTRATANTE manterá informado a CONTRATADA sobre o plano de comunicação com outros prestadores de serviços, para que possam ser acionados para correção de vulnerabilidades que excedem Servidores como (infraestrutura, aplicações, banco de dados).

2.2.7 A CONTRATADA será responsável pelo tratamento contínuo das vulnerabilidades encontradas na infraestrutura de servidores (Sistema Operacional) da CONTRATANTE, executando atividades listadas, mas não se limitando a elas:

2.2.7.1 Registrar Vulnerabilidade: nesta fase uma vulnerabilidade é identificada dentre os ativos de informação da CONTRATANTE. A CONTRATADA deve utilizar as ferramentas específicas de varredura nos ativos de hardware e software da CONTRATANTE. Quando a vulnerabilidade é encontrada, a mesma deve ser registrada na ferramenta designada.

2.2.7.2 Classificar Vulnerabilidade: nesta fase a vulnerabilidade é classificada de acordo com sua criticidade. A CONTRATADA deve realizar a classificação da vulnerabilidade em conjunto com as equipes internas designadas pela CONTRATANTE.

2.2.7.3 Notificar Vulnerabilidade e Próximo Nível Hierárquico: esta fase consiste na notificação do dono do ativo, sobre a existência da vulnerabilidade, juntamente com sua criticidade. A notificação ao dono do ativo é realizada pela equipe de local, sendo que a CONTRATADA deve prestar todo o esclarecimento acerca dos problemas existentes e potenciais decorrentes de possível exploração da vulnerabilidade.

2.2.7.4 Proposta de solução: nesta fase a CONTRATADA deverá propor as soluções definitivas para o tratamento da vulnerabilidade, bem como, soluções de contorno e/ou mitigação de curto prazo.

2.2.7.5 Analisar Tratamento: a CONTRATADA poderá ser requisitada para analisar se a vulnerabilidade corrigida diretamente pelo dono do ativo atendeu as necessidades de segurança da informação, assim como apoiar no processo de tratamento. A CONTRATADA quando o ativo não estiver sob sua gestão, deverá repassar ao CONTRATANTE os procedimentos necessários que possibilitem a verificação da eliminação da vulnerabilidade e seu monitoramento.

2.2.7.6 Avaliar Risco: esta fase é realizada pelo setor de gestão de segurança da informação da CONTRATANTE que atualiza os riscos de acordo com o tratamento realizado na vulnerabilidade. A CONTRATADA pode propor controles que podem ser utilizados nos modelos de avaliação de riscos, no caso de vulnerabilidades que serão mitigadas.

2.2.8 A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional do CONTRATANTE, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado à CONTRATANTE.

2.2.9 Após a apresentação do relatório com as vulnerabilidades, caberá ao CONTRATANTE autorizar a aplicação das correções e definir a janela de aplicação das correções;

2.2.10 A CONTRATADA será responsável por acionar e assessorar as áreas internas da CONTRATANTE a respeito da melhor estratégia para mitigação das vulnerabilidades encontradas. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores.

2.2.11 Todas as correções das vulnerabilidades deverão passar por um processo de aprovação pela CONTRATANTE e realizadas em janelas de atividade disponibilizada pela CONTRATANTE.

2.2.12 Todo acesso ao ambiente da CONTRATANTE deve ser realizado via VPN através de usuários autenticados e autorizados pela

CONTRATANTE.

2.2.13 Solução de Gestão de Vulnerabilidades e Auditoria de Configuração de Ativos

2.2.13.1 Características gerais:

- A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);
 - A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
 - A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
 - A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);
 - A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;
 - Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
 - A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com aplicações terceiras.
 - A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;
 - A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);
 - A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional; Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;
 - A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;
 - A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;
 - O escaneamento para os dispositivos expostos deve ser realizado através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
 - Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
 - O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
 - A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
 - A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
 - A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);
 - A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
 - A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;
 - A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;
 - A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
 - A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
 - A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;
 - A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;
 - A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de e-mail;
 - A solução deverá proteger 300 (trezentos) ativos;
 - A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
- Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

2.2.13.2 Dos requisitos e relatórios e painéis gerenciais

- A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;
- A solução deve permitir a customização de dashboards/relatórios;
- A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- A solução deve suportar o envio automático de relatórios para destinatários específicos;
- Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

2.2.13.3 Das varreduras

2.2.13.3.1 A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

2.2.13.3.2 A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

2.2.13.3.3 A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

2.2.13.3.4 Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

2.2.13.3.5 A solução deve ser configurável para permitir a otimização das configurações de varredura;

2.2.13.3.6 A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

2.2.13.3.7 A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

2.2.13.3.8 A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

- CyberArk;
- BeyondTrust;
- Thycotic;
- Centrify;

2.2.13.3.9 A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

2.2.13.3.10 A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

2.2.13.3.11 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

2.2.13.3.12 A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:

- Cloud Services;
- Data Leakage;
- Database;
- IoT;
- Mobile Devices;
- Operating System;
- Peer-To-Peer;
- SCADA;
- Web Servers;
- Web Clients;

2.2.13.3.13 A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

2.2.13.3.14 A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

2.2.13.4 Da análise e priorização de vulnerabilidades

2.2.13.4.1 A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

2.2.13.4.2 A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

- CVSS Impact Score;
- Idade da Vulnerabilidade;
- Maturidade de códigos de exploração da vulnerabilidade encontrada;
- Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
- Disponibilidade do código de exploração da vulnerabilidade;
- Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;
- Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

2.2.13.4.3 O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

2.2.13.5 Da Análise de Risco do Ambiente

2.2.13.5.1 A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

2.2.13.5.2 O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

2.2.13.5.3 Deve ser capaz de calcular a criticidade dos ativos da organização;

2.2.13.5.4 A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

2.2.13.5.5 A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

2.2.13.5.6 A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

2.2.13.5.7 Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

2.2.13.5.8 Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

2.2.13.5.9 A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

2.2.13.5.10 A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

2.2.13.5.11 A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;

2.2.13.5.12 A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

2.2.13.5.13 Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

2.2.13.5.14 A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

2.2.13.5.15 A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

2.2.13.6 Do Gerenciamento da Análise de Ataques exploráveis

2.2.13.6.1 Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;

2.2.13.6.2 Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;

2.2.13.6.3 Deve prover a evidência relacionada a descoberta do ataque;

2.2.13.6.4 Deve mostrar o objeto relacionado ao ataque, de origem e de destino;

2.2.13.6.5 Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;

2.2.13.6.6 Deve prover quais ferramentas e possíveis malwares associados ao ataque;

2.2.13.6.7 Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;

2.2.13.6.8 Deve disponibilizar uma biblioteca com ‘Queries’ para a busca de objetos no mínimo os seguintes segmentos:

- Rede;
- Endpoint;
- Active Directory;
- Permissão;
- Ransomware;
- Vetores;
- Credenciamento;

2.2.13.6.9 Deve suportar no mínimo 90 técnicas de ataques;

2.2.13.6.10 Deve permitir analisar, ao menos, os seguintes caminhos das superfícies de ataques:

- Aplicações WEB (DAST);
- Nuvem;
- Active Directory;
- Infraestrutura (Desktops, Servidores).

2.2.13.6.11 Deve apresentar os resultados em forma ilustrativa (Dashboard).

2.2.13.6.12 O Dashboard deve oferecer uma visão dos seus ativos vulneráveis considerando:

- Número de ativos críticos vulneráveis;
- Número de caminhos de ataque que levam a esses ativos críticos;
- Número de descobertas abertas e sua gravidade;
- Matriz para visualizar caminhos com diferentes combinações de valores alvo;
- Lista de tendências de caminhos de ataque.

2.2.13.6.13 Deve listar as diferenças entre os intervalos de tempo e mostrar uma seta direcional a fim de indicar se o valor aumentou ou diminuiu.

2.2.13.6.14 Deve permitir que o caminho de ataque leve a um ativo crítico.

2.2.13.6.15 Deve apresentar o número total alcançado de ativos críticos;

2.2.13.6.16 Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares.

2.2.13.6.17 Deve ser possível identificar o host suspeito;

2.2.13.6.18 Deve ser possível identificar o usuário suspeito;

2.2.13.6.19 Deve ser possível identificar o IP suspeito;

2.2.13.6.20 Deve permitir visualização em modo ilustrativo do caminho de ataque;

2.2.13.6.21 Deve ser possível identificar qual a técnica utilizada pelo atacante, tais como:

- Network Sniffing;
- LSASS Memory;
- Remote Desktop Protocol;
- Exploração de serviços remotos;
- System Services Discovery;
- Modificação da Política de Grupo;
- Mecanismo de Controle de Elevação de Abuso.

2.2.13.6.22 Deve permitir a comunicação com o framework MITRE ATT&CK ®.

2.2.13.6.23 Deve trazer o número de identificação MITRE ATT&CK para a descoberta;

2.2.13.6.24 A descoberta no MITRE ATT&CK deve abordar as seguintes ações:

- A técnica MITRE ATT&CK associada ao achado.
- A origem da descoberta.
- O alvo da descoberta.
- O status para indicar a ação tomada na descoberta, por exemplo: Em andamento.

2.2.13.6.25 Deve ser possível exportar uma descoberta como CSV.

2.2.13.6.26 Deve ser possível arquivar uma descoberta.

2.2.13.6.27 Deve ser possível ver o histórico do log da descoberta.

2.2.13.6.28 Deve permitir alterar o status do caminho de ataque descoberto para, pelo menos:

- Em Progresso;
- Em Revisão;
- Feito;

2.2.13.7 Da descoberta de Ativos

2.2.13.7.1 A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

2.2.13.7.2 A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

- Enumeração de Hosts;
- Identificação de Sistema Operacional (SO);

- Port Scan (Portas comuns);
 - Port Scan (Todas as portas);
 - Customizado;
- 2.2.13.7.3 A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;
- 2.2.13.7.4 A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:
- Descoberta de Host;
 - Ping o host remoto;
 - Usar descoberta rápida;
 - Métodos de ping;
 - ARP;
 - TCP;
 - ICMP;
 - UDP;
 - Escaneamento de descoberta de dispositivos de OT/SCADA;
 - Escaneamento de descoberta em redes de impressora;
 - Escaneamento em redes Novell;
 - Tecnologia de Wake-on-LAN;
- 2.2.13.7.5 Port Scanning:
- Considerar portas não escaneadas como fechadas;
 - Range de portas a serem escaneadas;
 - Enumerar Portas locais:
 - SSH (netstat);
 - WMI (netstat);
 - SNMP;
- 2.2.13.7.6 Descoberta de Serviços:
- Sondar todas as portas para encontrar serviços;
 - Procurar por serviços baseado em SSL/TLS;
 - Enumerar todas as cifras SSL/TLS;
- 2.2.13.7.7 A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;
- 2.2.13.7.8 A solução deve descobrir passivamente quando um host é adicionado na rede;
- 2.2.13.8 Da avaliação de vulnerabilidade
- 2.2.13.8.1 A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
- 2.2.13.8.2 A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
- 2.2.13.8.3 A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
- 2.2.13.8.4 A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
- 2.2.13.8.5 A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
- 2.2.13.8.6 A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação;
- 2.2.13.8.7 Contas administrativas vulneráveis a Kerberoasting attack;
- 2.2.13.8.8 Utilização de criptografia vulnerável com autenticação Kerberos;
- 2.2.13.8.9 Contas com pré-autenticação do Kerberos desabilitada;
- 2.2.13.8.10 Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
- 2.2.13.8.11 Verificar validação de fragilidades do tipo “Unconstrained Delegation”;
- 2.2.13.8.12 Verificação de “Pre-Windows 2000 Compatible Access”;
- 2.2.13.8.13 Verificação de validade de chaves mestras "Kerberos KRBTGT”;
- 2.2.13.8.14 Verificação de “SID History Injection”;
- 2.2.13.8.15 Verificação de “Printer Bug Exploit”;
- 2.2.13.8.16 Verificação de “Primary Group ID”;
- 2.2.13.8.17 Verificação de usuários com Passwords em branco;
- 2.2.13.8.18 A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
- 2.2.13.8.19 A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
- 2.2.13.8.20 A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
- 2.2.13.8.21 O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
- 2.2.13.8.22 A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
- 2.2.13.8.23 A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
- 2.2.13.8.24 A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
- 2.2.13.8.25 A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
- 2.2.13.8.26 A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee etc.;
- 2.2.13.8.27 A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de

Vulnerabilidade Versão (CVSS2 e CSVSS 3);

2.2.13.8.28 A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

2.2.13.8.29 A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

2.2.13.8.30 A solução deve possuir importação de arquivos .YARA;

2.2.13.8.31 Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

2.2.13.9 Da auditoria de Configuração

2.2.13.9.1 A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

2.2.13.9.2 A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

2.2.13.9.3 A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

- Center for Internet Security Benchmarks (CIS);
- Defense Information Systems Agency (DISA) STIGs;
- Health Insurance Portability and Accountability Act (HIPAA);
- Payment Card Industry Data Security Standards (PCI DSS);

2.2.13.9.4 A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

2.2.13.9.5 A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

2.2.13.9.6 A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados Oracle, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

2.2.13.9.7 A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

2.2.13.10 Certificação Profissional da Equipe de Gestão de Vulnerabilidade

2.2.13.10.1 Devido à complexidade das ferramentas que deverão ser suportadas pela Contratada e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõem o parque de segurança do CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com profissionais que possuam ao menos duas certificações abaixo:

- CISSP - Certified Information Systems Security Professional.
- CCSP - Certified Cloud Security Professional
- CEH - Certified Ethical Hacker
- CYSA+ - CompTIA Cybersecurity Analyst
- CISM - Certified Information Security Manager
- FCSS - Fortinet Certified Solution Specialist
- Fortinet FCP – Network Security
- Fortinet NSE4 - Network Security Expert Level 4

2.2.14 Serviços de Instalação

2.2.14.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.

2.2.14.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;

2.2.14.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;

2.2.14.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;

2.2.14.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;

2.2.14.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;

2.2.14.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;

2.2.14.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

2.2.14.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

2.2.14.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da CONTRATANTE.

2.2.14.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.2.14.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.2.14.10 A montagem e instalação de todos os componentes que compõem solução adquirida são de responsabilidade da CONTRATADA.

2.2.14.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.2.14.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.2.14.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.2.14.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.2.14.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.2.14.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.2.14.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.2.14.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.2.14.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.2.14.18 A substituição definitiva será admitida com anuência da CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, software, peça e componente ofertado, em relação àquele que está sendo substituído.

2.3 SOLUÇÃO DE GERENCIAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA (FORTISIEM)

2.3.1 A CONTRATADA deverá suportar ferramenta de gerenciamento e correlação de eventos de segurança da informação FortiSIEM.

2.3.1.1 O serviço visa o monitoramento contínuo e ininterrupto do tráfego de dados e comunicação dos sistemas e da infraestrutura tecnológica da Sefaz/AC, com o objetivo de prover insumos de detecção e resposta a ataques cibernéticos.

2.3.1.2 A solução deve realizar o correlacionamento de logs, pacotes de redes, comportamento anômalo de aplicações e usuários, serviços e infraestrutura de forma a detectar e registrar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido no processo de gestão de incidentes pela Contratante

2.3.2 A CONTRATADA deverá fornecer a solução, na qual será utilizada como ferramenta durante a vigência do contrato para prestação de serviços de SOC.

2.3.3 A CONTRATADA deverá fornecer acesso a dashboards de forma unificadas das tecnologias que comporão o ecossistema de serviços e ou, acesso Ready Only das ferramentas fornecidas.

2.3.4 A CONTRATADA deve possuir ferramenta automatizada para prover os serviços de monitoramento e visibilidade de ataques cibernéticos e equipe técnica capacitada para analisar os indicadores fornecidos pelas ferramentas, indicando proativamente a existência de incidentes cibernéticos, sendo definido como um evento com potencial de ocasionar uma possível violação na política de segurança da Sefaz/AC.

2.3.5 A CONTRATADA deve notificar a CONTRATANTE diante da detecção de qualquer evento suspeito, provendo todo o embasamento que respalde a notificação encaminhada.

2.3.5.1 Além disso, mensalmente deve encaminhar relatório detalhado das atividades realizadas e do status dos indicadores de monitoramento e visibilidade de ataques cibernéticos.

2.3.6 Deve ter suporte para realizar o monitoramento dos ativos de informação conforme solicitação da CONTRATANTE, seja através da adição de agentes ou através de suporte nativo aos formatos dos logs e eventos.

2.3.7 Da Ferramenta de Gerenciamento correlação de eventos de segurança

2.3.7.1 Requisitos Mínimos de Funcionalidades

2.3.7.1.1 A solução deverá ser entregue no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V e KVM, a responsabilidade pelo fornecimento e implantação de servidor/hardware com licenciamento necessário será da CONTRATADA, devendo estar licenciado e ser compatível para atender os requisitos de performance da solução.

2.3.7.1.2 O servidor deve ser dedicado para a solução e permitir a instalação em rack de 19 polegadas, possuir trilhos deslizantes e braço para gerenciamento de cabos

2.3.7.1.3 Todos os equipamentos que compõem a solução devem ser entregues com a última versão de software homologada e recomendada pelo fabricante.

2.3.7.1.4 Ao fim do contrato de garantia, a solução deverá estar completamente funcional, capaz de criar, customizar e gerenciar políticas e regras, gerar relatórios, manipular dashboard e entre outras funções necessárias ao manuseio da solução.

2.3.7.1.5 A solução deve suportar redundância e alta disponibilidade, nos modos ativo-standby ou ativo-ativo;

2.3.7.2 Arquitetura de Implementação

2.3.7.2.1 A solução deverá permitir a implementação de maneira distribuída ou em um único servidor;

2.3.7.2.2 A arquitetura da solução permite com que seus componentes possam ser instalados em redes IPv4 e IPv6.

2.3.7.2.3 A solução deverá permitir a utilização de armazenamento de eventos local ou através de servidor NFS;

2.3.7.2.4 A solução deverá fornecer licenciamento para processamento de no mínimo 12.500 (doze mil e quinhentos) eventos por segundo (EPS), ou que não ultrapasse 500 (quinhentos) Giga/dia.

2.3.7.2.5 A solução deverá fornecer licenciamento para processamento de no mínimo 2500 (dois mil e quinhentos) dispositivos.

2.3.7.2.6 Deverá permitir o aumento da capacidade de processamento de EPS através de licenças adicionais;

2.3.7.2.7 solução deverá permitir a adição de coletores para coleta de logs e informações de performance em sites remotos;

2.3.7.2.8 A solução deve possuir a capacidade de encaminhar qualquer evento recebido em tempo real, nos formatos syslog e netflow;

2.3.7.2.9 A solução deverá suportar a filtragem dos dados coletados no nível de aplicação, identificando endereço IP, tipo do dispositivo e tipo do evento;

2.3.7.2.10 A solução deverá componentes sejam virtualizados;

2.3.7.2.11 A solução deverá suportar a virtualização nos seguintes Hypervisors: VMware ESX, Hyper-V e KVM;

2.3.7.2.12 A solução permite Failover e Disaster Recovery em ambiente físico e virtual.

2.3.7.2.13 A solução deve permitir a implementação nas seguintes nuvens públicas: Azure e AWS.

2.3.7.3 Funcionalidades Multi-tenancy

2.3.7.3.1 Deve suportar implementação em ambiente distribuídos;

2.3.7.3.2 As descobertas efetuadas devem, por padrão, atrelar novos dispositivos automaticamente à empresa/departamento/localidade a qual pertencem;

2.3.7.3.3 A solução deve permitir o monitoramento de elementos mesmo quando houver sobreposição de IP's (overlapping);

2.3.7.3.4 Deve permitir a alocação mínima (garantida) de EPS por organização, bem como alocar EPS dinamicamente entre organizações caso um número excessivo e inesperado de EPS seja recebido;

2.3.7.3.5 Deve suportar a definição de uma quantidade máxima de devices por organização;

2.3.7.3.6 Deve ser permitido criar logins de gerenciamento limitados a uma ou mais organizações, definindo níveis de privilégio para cada.

2.3.7.3.7 A solução deverá possuir coletores Multi-tenant, permitindo assim pelo menos as seguintes formas de configuração/implementação:

- Multi-tenant Agents;
- Multi-tenant Event Pulling;
- Multi-tenant Collector Pool;

2.3.7.4 Funcionalidades de Gerenciamento

2.3.7.4.1 A solução deverá permitir ser gerenciada através de interface gráfica Web;

2.3.7.4.2 Deve permitir alteração de idioma de sua interface para português;

2.3.7.4.3 Deve permitir o controle de acesso granular limitando o acesso a interface gráfica e a diversos níveis de dados;

2.3.7.4.4 Deve permitir a autenticação de usuários administrativos através dos seguintes diretórios: Local, Microsoft Active Directory, LDAP, Single Sign On and SAML via OKTA;

2.3.7.4.5 Toda a comunicação entre os módulos deverá ser feita através de HTTPS;

2.3.7.4.6 Deve permitir a auditoria completa da atividade de usuários da solução de segurança de correlação de eventos, resposta automática e remediação de incidentes;

2.3.7.4.7 Para fins de resolução de problemas, a solução deve possuir ferramentas que permitam: iniciar e parar processos individuais, executar shutdowns e reboots, validar métricas de performance da solução de segurança de correlação de eventos, resposta automática e remediação de incidentes e exportar informações de evento em CSV;

2.3.7.4.8 A solução deve permitir a visualização de usuários que estiverem logados no sistema, atividades de consulta de usuários e usuários bloqueados;

2.3.7.4.9 A solução deve permitir o backup e recuperação de arquivos de configuração e conteúdo;

2.3.7.4.10 Deverá permitir a atualização dos componentes da solução através de interface gráfica ou através do próprio sistema operacional via linha de comando;

2.3.7.4.11 A respeito da capacidade em Eventos por Segundo (EPS), se o número de EPS recebido atingir o limite da licença, a solução de segurança de correlação de eventos, resposta automática e remediação de incidentes deverá automaticamente gerar um alerta.

2.3.7.4.12 A solução deverá permitir especificar um limite de EPS por coletor;

2.3.7.4.13 Deve ser possível monitorar a saúde dos coletores exibindo as seguintes informações:

- Nome da Organização onde coletor está instalado;
- Nome do Coletor;
- Endereço IP;
- Status;
- Saúde;
- Tempo em Operação (uptime);
- Utilização de CPU e Memória;
- Versão;
- EPS Alocados;
- EPS Processados.

2.3.7.4.14 A solução deve suportar a administração centralizada em uma implementação geograficamente distribuída onde todos os componentes são monitorados e gerenciados a partir de um portal centralizado;

2.3.7.4.15 Deve permitir a visualização da utilização de licenças através da interface gráfica com, pelo menos, as seguintes informações: dispositivos, EPS e agentes;

2.3.7.4.16 Deve permitir o arquivamento de dados baseado em políticas;

2.3.7.4.17 Deve permitir o “hashing” de logs em tempo real para o não repúdio e verificação de integridade;

2.3.7.4.18 A solução deve possuir compatibilidade e integração através de APIs documentadas e homologadas pelo fabricante, com pelo menos 30 soluções de segurança do mercado, com intuito de complementar a capacidade de análise de atividade maliciosa e resposta a incidentes;

2.3.7.4.19 A solução deve prover uma console e visão intuitiva para realizar investigações sobre os dados;

2.3.7.4.20 A solução deve possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;

2.3.7.4.21 A solução deve permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

2.3.7.4.22 A solução deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;

2.3.7.4.23 O fabricante da solução deve possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;

2.3.7.4.24 A solução deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;

2.3.7.4.25 A solução deve possuir integração aberta com soluções de análise de malware;

2.3.7.4.26 A solução deve possuir capacidade nativa de gestão de centro de operações de segurança e rede (Security Operations Center – SOC e Network Operations Center) na mesma aplicação;

2.3.7.4.27 A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;

2.3.7.4.28 Possuir suporte ao framework MITRE ATT&CK, com pelo menos as seguintes características:

- Capacidade de associar uma técnica MITRE a uma regra da solução de segurança de correlação de eventos, resposta automática e remediação de incidentes (integrada ou personalizada);
- Possuir pelo menos 800 regras integradas para detectar uma ampla variedade de técnicas MITRE;
- Capacidade de atribuir técnicas e táticas às regras e pesquisar incidentes por técnicas e táticas;
- Possuir Dashboard que exibe regras associadas a uma tática ou técnica;
- Possuir dashboard que exibe incidentes associados a uma tática ou técnica;

2.3.7.5 Funcionalidade Coletores

2.3.7.5.1 A solução deverá possuir coletores para a obtenção de eventos em sites remotos;

2.3.7.5.2 A solução não deverá restringir o número de coletores utilizados através de licença;

2.3.7.5.3 O coletor deve suportar a instalação em Hypervisor VMware ESX ou diretamente em Bare Metal;

2.3.7.5.4 O coletor deve possuir a capacidade de coletar os dados, realizar “parsing”, compressão e envio através de HTTPS;

2.3.7.5.5 O coletor deve ser capaz de realizar o armazenamento local das informações caso não haja conectividade com a solução de segurança de correlação de eventos, resposta automática e remediação de incidentes. Não deverá haver restrição de tempo para o armazenamento, desde que haja disponibilidade de espaço em disco;

2.3.7.5.6 Deve permitir a atualização dos coletores através da interface gráfica da solução de segurança de correlação de eventos, resposta automática e remediação de incidentes;

2.3.7.6 Funcionalidade de Agentes

2.3.7.6.1 A solução deverá permitir a utilização de agentes para a coleta de informações mais detalhadas de servidores Windows e Linux;

2.3.7.6.2 A solução com o agente para Windows deverá ser capaz de coletar as seguintes informações:

- Agente para Windows;
- Windows Security Logs;
- Windows Application Logs;
- Windows System Logs;
- Windows DNS Logs;
- Window DHCP Logs;
- IIS logs;
- DFS logs;
- Monitoramento de Integridade de Arquivos;
- Monitoramento de Mudança de Software Instalado;
- Monitoramento de Mudança no Registro;
- Monitoramento de Arquivos;
- Monitoramento de Saída WMI;
- Monitoramento de Saída de Power Shell;
- Análise adicional de logs DNS do Windows para incluir IP de Origem, Nome do Destino, IP de Destino, Nome canônico do destino e bytes recebidos;
- Durante a atualização do agente é evitada a perda da Configuração do Agente no Gerenciador de Agentes do Windows;
- Limpeza automática de arquivos .SVC quando atinge um determinado tamanho;
- O arquivo de log não é apagado após a reinicialização do agente;
- Possuir capacidade de monitorar discos USB criptografados;
- A solução é capaz de executar verificações de certificado SSL;
- Possuir capacidade de liberar arquivos de log durante a rotação de arquivos de um arquivo monitorado.

2.3.7.6.3 O agente deverá suportar os seguintes sistemas operacionais:

- Windows Server 2008 R2;
- Windows Server 2012;
- Windows Server 2012 R2;
- Windows Server 2016;
- Windows Server 2016 R2;
- Windows Server 2019;
- Windows Server 2019 Core;
- Windows Server 2022;
- Windows 7 Enterprise & Professional;
- Windows 8;
- Windows 10.

2.3.7.6.4 A solução deverá ter um agente para Linux;

2.3.7.6.5 Sistema de Coleta (Alto Desempenho), Logs de aplicativos e logs de segurança;

2.3.7.6.6 Monitoramento de Integridade de Arquivos;

2.3.7.6.7 Monitoramento de arquivo de log do cliente;

2.3.7.6.8 CentOS 7.4 and later;

2.3.7.6.9 Red Hat Enterprise Linux 7.x and later;

2.3.7.6.10 Ubuntu 14.04, 16.04, 18.04, 20.04 e LTS;

2.3.7.6.11 Amazon Linux 1 and Amazon Linux 2;

2.3.7.6.12 SUSE Linux Enterprise Server (SLES) 12, 15;

2.3.7.6.13 O agente para Windows poderá ser gerenciado diretamente pela console GUI da solução, dispensando assim a necessidade de um gerenciador central;

2.3.7.6.14 Os agentes deverão encaminhar logs para a aplicação de gestão dos agentes através da porta TCP 443;

2.3.7.6.15 O agente deverá permitir sua instalação através de GPO;

2.3.7.6.16 A solução deverá ser fornecida com 25 (vinte e cinco) licenças de agente.

2.3.7.7 Funcionalidade de Dashboards e Relatórios

2.3.7.7.1 A solução deve prover de forma padrão dashboards para monitoramento dos elementos de rede, incluindo VM's;

2.3.7.7.2 Acessando um dispositivo no dashboard, deve ser possível visualizar informações diversas sobre eles, tais como: incidentes, disponibilidade, performance e segurança;

2.3.7.7.3 A customização dos dashboards deve ser possível, adicionando novos widgets e a forma como são exibidos, inserção de outros devices e refresh de tela;

2.3.7.7.4 Deve permitir ao administrador importar e exportar dashboards;

2.3.7.7.5 Deve possuir, por padrão, os seguintes dashboards: network, server, security, NetApp, VNX, Salesforce e Office 365;

2.3.7.7.6 Deve possuir um dashboard que informe o status de registro dos dispositivos PCI;

2.3.7.7.7 A solução deve possuir relatórios pré-definidos, envolvendo padrões como: PCI, HIPAA, SOX, ISO e GLBA, dentre outros;

2.3.7.7.8 Deve permitir a criação de novos reports;

2.3.7.7.9 Por padrão, a solução deve possuir baselines, definindo padrões de comportamento distintos para dias de semana, finais de semana e para cada hora do dia, permitindo ao operador criar alertas para eventos que fujam ao padrão;

2.3.7.7.10 Deve possuir baselines de: DNS requests por cliente, tráfego de destino a servidores e de origem, conexões permitidas e negadas pelo firewall, CPU e memória por host, I/O de disco para servidores, tráfego e erros em interfaces de rede, falhas e sucesso de logon, dentre outros baselines;

2.3.7.7.11 Deve permitir criar reports que associem IP's, endereços MAC, usuários de rede, máquinas e domínios a locais específicos como portas de switch, gateway VPN e controladora wireless;

2.3.7.7.12 Deve possibilitar o agendamento de reports, que podem ser gerados uma única vez ou de forma recorrente, além permitir notificações quando o report for gerado e até quando ele deverá estar disponível;

2.3.7.7.13 Deve permitir ao administrador da plataforma realizar auditorias sobre o bom uso dos sistemas, apontando desvios em relação ao sistema operacional utilizado, bem como softwares instalados nas máquinas, além de permitir especificar o fabricante dos equipamentos a serem submetidos à auditoria;

2.3.7.7.14 A solução deve permitir exportar o report de auditoria, tanto em PDF, CSV e RTF, bem como possibilitar o agendamento;

2.3.7.7.15 Deve ser possível integrar a plataforma à sistemas de Business Intelligence;

2.3.7.8 Funcionalidades de Ingestão de Dados

2.3.7.8.1 Deve ser capaz de receber logs de diversos dispositivos diferentes, incluindo dados estruturados como também dados não estruturados;

2.3.7.8.2 Deve ser capaz de receber logs de, pelo menos, 200 dispositivos diferentes sem necessidade de criação de parsers customizados;

2.3.7.8.3 Deve ser capaz de receber logs de dispositivos de segurança de rede, tais como: roteadores, switches, dispositivos de prevenção contra intrusão, web proxies, gateway de proteção de e-mail, DNS e servidores DHCP de diversos fabricantes;

2.3.7.8.4 Deve ser capaz de receber logs de sistemas operacionais de diversos fabricantes;

2.3.7.8.5 Deve ser capaz de receber logs de aplicações de segurança, tais como: servidores web, servidores de aplicações, banco de dados e sistemas de proteção de endpoints;

2.3.7.8.6 Deve ser capaz de receber logs via syslog, traps SNMP, Netflow, SFlow, JFlow, FTP e SCP;

2.3.7.8.7 Deve ser capaz de obter dados através de JDBC, JMX, Cisco SDEE e LEA CheckPoint;

2.3.7.8.8 Deve ser capaz de coletar qualquer arquivo de logs de sistemas operacionais Windows através de agente próprio;

2.3.7.8.9 Deve permitir que arquivos de log formatados em CSV personalizados possam ser carregados através da console GUI para análise mais detalhada;

2.3.7.8.10 Deve ser capaz de obter logs de aplicações Cloud através de API's específicas, tais como: Google Apps, Office 365 e Salesforce CRM;

2.3.7.8.11 Deve ser capaz de inserir contexto aos dados obtidos;

2.3.7.8.12 Deve ser capaz de realizar o parsing, armazenar, analisar e exibir conteúdo de pacotes TCP/UDP em eventos que são gerados por sistemas de prevenção de intrusão;

2.3.7.8.13 Capacidade de analisar arquivos de log de um diretório em nós da solução;

2.3.7.8.14 Permitir ao usuário analisar arquivos PCAP. Incluindo os atributos IP, TCP / UDP e HTTP;

2.3.7.9 Funcionalidade de Enriquecimento de Dados

2.3.7.9.1 Deve fornecer uma base de dados de localização de endereços IP (GeoIP) e ser capaz de obter informações de cada endereço de IP público recebido nos eventos, sendo cada evento enriquecido com informações de localização geográfica, tais como: cidade, país, ASN, longitude e latitude;

2.3.7.9.2 Deve permitir que os administradores da solução possam pesquisar informações sobre endereços IP e reputação de domínio de qualquer website público;

2.3.7.9.3 Deve permitir o agrupamento de ativos de rede de forma automática e realizar a sua classificação através de segmento de rede, sistema operacional, aplicação etc.;

2.3.7.9.4 Deve permitir a criação de grupos customizados e regar de mapeamento;

2.3.7.9.5 Deve ser capaz de utilizar informações de serviços de DHCP e de diretório para gerar alertas e relatórios;

2.3.7.9.6 Deve ser capaz de monitorar a atividade de servidores DNS com o objetivo de detecção de malwares;

2.3.7.9.7 Possui capacidade de verificações de reputação (Indicadores de compromisso) como IP, Domínio, URL e Hash;

2.3.7.10 Funcionalidade de Classificação de Dados

2.3.7.10.1 Deve ser capaz de classificar diferentes tipos de dados coletados para auxiliar na sua utilização em consultas analíticas ou “ad hoc” por analistas do SOC. Também deve ser capaz de classificar esses dados com base em sua sensibilidade ou proteção de segurança / privacidade necessários;

2.3.7.10.2 Deve ser capaz de agrupar dados semelhantes;

2.3.7.10.3 A solução deve ser capaz de analisar o tipo do evento e atribuí-lo a um grupo de tipo de evento;

2.3.7.10.4 Deve permitir a utilização de expressões regulares para fazer correspondência nos dados recebidos;

2.3.7.10.5 Permite a definição de tags, que podem ser usadas em regras e incidentes;

2.3.7.11 Funcionalidade de Armazenamento de Dados, Gerenciamento e Arquivamento

2.3.7.11.1 Deve prover integridade dos logs através de criptografia dos dados;

2.3.7.11.2 Deve permitir a execução de relatórios para validar a integridade dos dados e identificar possíveis blocos de dados que tenham sido modificados;

2.3.7.11.3 A solução deve prover ferramentas integradas para gestão dos dados;

2.3.7.11.4 A solução deve permitir armazenamento de dados on-line e off-line;

2.3.7.11.5 A solução deve permitir o gerenciamento da retenção de logs através de políticas. Deve permitir a criação de regras baseadas na identificação do cliente, tipo do evento, dispositivos e especificar o número de dias no armazenamento on-line e off-line;

2.3.7.11.6 Deve ser capaz de arquivar os dados em tempo real em qualquer sistema Big Data através do barramento de mensagens Kafka ou similar;

2.3.7.11.7 Deve ser capaz de tornar anônimo qualquer campo de log analisado que contenha informações (PII), incluindo endereços IP, host entre outros;

2.3.7.11.8 Deve permitir que os Eventos coletados sejam armazenados em Elasticsearch;

2.3.7.11.9 Deve pelos menos suportar as configurações do Elasticsearch: Nó Único (All-in-One);

2.3.7.11.10 Deve permitir o uso do ElasticSearch para comunicação Cloud com bases de armazenamento dos eventos na nuvem, como Amazon entre outros.

2.3.7.11.11 Deve ser capaz de arquivamentos dos eventos através de sistema de arquivo distribuído (HDFS), garantindo uma maior escalabilidade no armazenamento dos eventos arquivados;

2.3.7.12 Funcionalidade de Analytics

2.3.7.12.1 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

2.3.7.12.2 A solução deve possibilitar a busca de eventos históricos e em tempo real;

2.3.7.12.3 Efetuar a análise dos eventos em tempo real;

2.3.7.12.4 Realizar a correlação dos eventos antes dos dados serem armazenados na base de dados;

2.3.7.12.5 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

2.3.7.12.6 A solução deve fornecer atualizações predefinidas de regras de correlação e atualizações de software;

2.3.7.12.7 A solução deve suportar a realização de um filtro dos dados coletados antes de realizar a correlação;

2.3.7.12.8 A solução deve possuir regras pré-definidas, incluindo regras de segurança, disponibilidade/performance e mudanças de configuração;

2.3.7.12.9 Permitir a criação de novas regras e a edição das existentes;

2.3.7.12.10 A solução deve permitir a criação de regras de correlação unificando todos os eventos, como logs de segurança, disponibilidade, performance, storage e mudanças de configurações;

2.3.7.12.11 A solução deve ser capaz de gerar alertas automáticos e notificações quando alcançar os limites de dados coletados, sem descartar os dados;

2.3.7.12.12 Deve permitir buscas simples em raw data (não estruturadas), através de palavra-chave, bem como definir quais campos serão apresentados no resultado, o período da busca e a organização (ambientes multi-tenant);

2.3.7.12.13 Deve permitir salvar a consulta, definindo o tempo que ela estará disponível para uso futuro.

2.3.7.12.14 Deve permitir salvar e enviar por e-mail o resultado da busca, como PDF e CSV;

2.3.7.12.15 Deve possibilitar buscas estruturadas, baseadas em atributos, inserindo múltiplas condições. Deve haver opção para agrupamento de eventos;

2.3.7.12.16 Ao operador será possível definir: de qual elemento ele deseja verificar os logs, eventos cuja ação tomada pelo dispositivo foi "negar" e filtrar por dispositivos presentes em uma determinada categoria da base de conhecimento, de forma condicional (AND) ou excludente (OR);

2.3.7.12.17 Deve possibilitar uma busca que mostre mudanças em logins/grupos do domínio não executadas por usuários de um determinado grupo de admins do domínio;

2.3.7.12.18 O uso de expressões regulares deve ser permitido nas buscas;

2.3.7.12.19 A depender do tipo de informação buscada, a solução deve exibir gráficos nos formatos de: tendência, tabela, barra, dispersão (correlação entre duas variáveis) e árvore (análise de componentes dominantes) e heat map (intensidade);

2.3.7.12.20 Deve permitir, de forma simples, converter uma busca histórica em tempo real, sem que haja necessidade de reinserir os mesmos filtros para essa nova busca;

2.3.7.12.21 A partir de uma busca, deve ser possível criar uma regra reaproveitando os filtros já definidos, e gerar um alerta, a fim de notificar o administrador sobre um determinado evento;

2.3.7.12.22 As buscas simples devem aceitar os seguintes operadores: AND, OR e AND NOT;

2.3.7.12.23 As buscas estruturadas devem aceitar os seguintes operadores: =, !=, >, >=, IN, IN, BETWEEN, IS, CONTAINS e REGEXP;

2.3.7.12.24 Deve listar, por padrão, atributos que podem ser utilizados nas queries. Adicionalmente, deve permitir buscar atributos presentes na base de conhecimento, filtrando por funcionalidade e equipamento;

2.3.7.12.25 Deve mostrar, quando possível, a localização geográfica de um IP (origem ou destino), tais como: país, cidade, estado, longitude e latitude;

2.3.7.12.26 Deve exibir, em formato de mapa, os resultados da query no que tange países envolvidos no tráfego resultante do filtro;

2.3.7.12.27 O administrador deve ser capaz de salvar filtros de pesquisas, que podem ser reutilizados no futuro;

2.3.7.12.28 A solução deve suportar análise de dados históricos de segurança, eventos, dispositivos e sistemas ou dados de aplicativos de longo prazo;

2.3.7.12.29 A solução deve possibilitar o uso de "queries" em formato "SQL like" para minimizar a curva de aprendizado para administradores familiarizados em banco de dados relacionais;

2.3.7.12.30 A solução deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;

2.3.7.12.31 A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;

2.3.7.12.32 A solução deve prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;

2.3.7.12.33 A solução deve possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;

2.3.7.12.34 A solução deve possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;

2.3.7.12.35 A solução deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;

2.3.7.12.36 A solução deve ser capaz de suportar análises avançadas como anomalias estatísticas;

2.3.7.13 Funcionalidade de Monitoramento

2.3.7.13.1 A solução deve suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;

2.3.7.13.2 A solução deve ser capaz de autodescobrir dispositivos e recursos que estão sendo monitorados através de protocolos e credenciais como SNMP, WMI, SSH/Telnet e outros;

2.3.7.13.3 Para casos em que será utilizado o WMI como coletor de logs, a solução deverá ser capaz de criar filtros para obtenção dos mesmos. Estes filtros podem contemplar Todos os Logs ou logs como: Eventos de Sistema, Segurança ou Aplicação

2.3.7.13.4 A solução deve automaticamente classificar os dispositivos por tipo ou grupos, sendo depois referenciados em relatórios, regras, queries e outros;

2.3.7.13.5 A solução deve suportar a monitoração de dispositivos como disponibilidade, mudanças de configuração, performance e outros;

2.3.7.13.6 A solução deve suportar no mínimo os protocolos: TCP, UDP baseado em syslog, Netflow, Sflow, Jflow, SNMP trap, JDBC, Cisco SDEE, Microsoft WMI, Checkpoint LEA, banco de dados JDBC para Oracle, banco de dados do servidor SQL, banco de dados IBM DB2, JDBC para Snort, JDBC para McAfee Foundstone, SSH / telnet para arquivos de configuração, VMware SDK para descoberta VMware e coleção de logs. Para as métricas de desempenho e disponibilidade, a solução de segurança de correlação de eventos, resposta automática e remediação de incidentes deve usar SNMP, JMX, Windows WMI, JDBC para vários bancos de dados, NetApp ONTAP API, EMC Navisphere, VMware SDK;

2.3.7.13.7 A solução deve suportar a monitoração de seus próprios processos internos com possibilidade de geração de alertas;

2.3.7.14 Funcionalidade de Alertas e Incidentes

2.3.7.14.1 Como resultado de regras, deverá ser capaz de executar ações automáticas, tais como:

- Executar script, como reiniciar um processo, remover arquivos de um diretório, mudança de configuração ou execução de comandos dentro outros;
- Criação de um TRAP SNMP;
- Enviar e-mail para uma lista de usuários;
- Enviar mensagens para o usuário conectado no console;
- Criar um ticket no sistema de ticketing interno ou externo;

2.3.7.14.2 A solução organiza os incidentes em categorias e subcategorias, permitindo assim que esses campos possam ser usados em pesquisas.

2.3.7.14.3 A solução deve permitir a criação e acompanhamento de Incidentes de Segurança, com no mínimo as seguintes características:

- Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
- Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;
- Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
- Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
- Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2);
- Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux;
- Possuir integração nativa com ferramenta de gerenciamento de incidentes externa, tais como: ServiceNow, Sales Force, Remedy e ConnectWise;

2.3.7.14.4 A solução deverá possuir atributos para resolução de incidentes, com as seguintes opções:

- Positivo;
- Falso Positivo;
- Aberto;
- Os atributos de resolução de incidentes podem ser usados em pesquisas;
- Deve ser capaz de encaminhar logs para um sistema externo usando o formato Common Event Format (CEF) sobre UDP ou TCP;
- Deve permitir que os Incidentes detectados sejam visualizados através de todas as categorias definidas pela Matrix Enterprise do MITRE ATT&CK;
- Permite a integração com soluções externas de incidentes/Secops via JSON REST API;

2.3.7.15 Funcionalidade de CMDB

2.3.7.15.1 A solução deve possuir ou integrar-se à sistemas de CMDB (Configuration Management Database), atendendo de forma nativa ou através de composição os requisitos listados nesse documento;

2.3.7.15.2 A solução deve prover informações detalhadas sobre devices, aplicações, usuários e qualquer outro componente de rede compatível com protocolos de gerência (SNMP, SYSLOG, NETFLOW etc.), de forma nativa. Para elementos desconhecidos, deve ser

- possível a criação de scripts que permitam a correta identificação dos mesmos;
- 2.3.7.15.3 Deve permitir realizar um discovery da rede, de forma dinâmica, evitando a adição manual dos elementos ao CMDB;
- 2.3.7.15.4 O discovery deve promover categorização dinâmica, alocando os elementos nos devidos grupos;
- 2.3.7.15.5 Deve informar: nome do dispositivo gerenciado, IP, tipo, versão, protocolo utilizado para coleta dos dados e organização a qual pertence;
- 2.3.7.15.6 Deve ser capaz de mostrar os elementos gerenciados de forma tabelada e em topologia, posicionando cada elemento conforme configurações/logs analisados;
- 2.3.7.15.7 Deve mostrar estatísticas relativas à performance do dispositivo, tais como: tráfego, memória, disco e CPU;
- 2.3.7.15.8 Ao selecionar um dispositivo específico, deve permitir visualizar seus logs em tempo real (analytics), sem necessidade de criar um filtro manual para tal;
- 2.3.7.15.9 Deve permitir agregar dispositivos e aplicações que suportam um determinado serviço dando ao operador uma visão macro sobre o serviço em si;
- 2.3.7.15.10 Quando aplicável, deve informar ao operador o software, hardware e configuração utilizada pelo dispositivo;
- 2.3.7.15.11 De forma simples, deve informar os incidentes e eventos de disponibilidade, performance e segurança relacionados a um elemento monitorado.;
- 2.3.7.15.12 Deve prover, por padrão, listas de domínios (threat feeds) conhecidos por gerar spam, suportar botnets, participar de ataques DDoS e conter malwares. O operador deve ser capaz de adicionar novas listas;
- 2.3.7.15.13 Ao operador deve ser possível agrupar em listas elementos que devem ser acompanhados com maior atenção. Exemplo: logins que são constantemente bloqueados e máquinas cujos discos apresentam falta de espaço;
- 2.3.7.15.14 Deve prover reports que informem dispositivos aprovados no CMDB, usuários descobertos, sistemas operacionais utilizados, hardwares, serviços em execução em máquinas Windows, softwares e patches instalados, dentre outros;
- 2.3.7.16 Funcionalidade de Controle de Acesso
- 2.3.7.16.1 Dado o grande escopo abordado pela solução, se torna difícil a um único administrador gerenciar performance, disponibilidade, mudanças e segurança em equipamentos de rede, servidores e aplicações. A solução ofertada deve permitir a divisão de tarefas por função (RBAC), localidade/área, dispositivos/sistemas e nível de criticidade da informação;
- 2.3.7.16.2 A solução deve possuir controle de acesso baseado em perfis de usuários e ser multi-tenant;
- 2.3.7.16.3 Por padrão, a plataforma deve disponibilizar os seguintes tipos de gerência: escrita e leitura, equipamentos de rede, sistemas, servidores, Windows, segurança, helpdesk e apenas leitura;
- 2.3.7.16.4 Deve permitir a criação de funções customizadas;
- 2.3.7.16.6 Deve suportar o uso de logins locais e externos para autenticação na gerência da solução. Nesse último caso: LDAP, RADIUS e SAML via Okta;
- 2.3.7.16.7 Suporte à duplo fator de autenticação em logins de gerência;
- 2.3.7.17 Funcionalidade de UEBA (User & Entity Behavior Analytics)
- 2.3.7.17.1 A solução deve suportar agente UEBA para usuários Windows.
- 2.3.7.17.2 Deve suportar eventos de Usuário, máquina, arquivos e unidade de montagem.

2.3.8 Certificação Profissional da Equipe de SIEM

2.3.8.1 Devido à complexidade das ferramentas que deverão ser suportadas pela Contratada e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõem o parque de segurança do CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com profissionais que possuam ao menos duas certificações abaixo:

- CEH - Certified Ethical Hacker;
- CYSA+ - CompTIA Cybersecurity Analyst
- FCSS - Fortinet Certified Solution Specialist
- CompTIA security+
- FCSS - Fortinet Certified Solution Specialist
- Fortinet FCP – Network Security
- Fortinet NSE4 - Network Security Expert Level 4

2.3.9 Serviços de Instalação

2.3.9.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.

2.3.9.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;

2.3.9.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;

2.3.9.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;

2.3.9.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;

2.3.9.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;

2.3.9.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;

2.3.9.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

2.3.9.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

2.3.9.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da CONTRATANTE.

2.3.9.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.3.9.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.3.9.10 A montagem e instalação de todos os componentes que compoñham solução adquirida são de responsabilidade da CONTRATADA.

2.3.9.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.3.9.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.3.9.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.3.9.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.3.9.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.3.9.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.3.9.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.3.9.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.3.9.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.4 SOLUÇÃO DE THREAT INTELLIGENCE

2.4.1 A solução deverá suportar a obtenção de informações de inteligência de ameaças.

2.4.2 Deve ser capaz de obter, pelo menos, as seguintes informações: domínio de malware, IP de malware, URL de malware, Hash de malware, redes anônimas incluindo proxies abertos e VPN, User Agent de malware;

2.4.3 A solução deverá prover importação via STIX/TAXII;

2.4.4 Deve ser capaz de obter informações de inteligência de ameaças nativamente das seguintes fontes: Emerging Threat, Malware Domain List, Zeus e Threat Stream (Anomali);

2.4.5 Deve ser capaz de obter informações de inteligência de ameaças nativamente da fonte AlienVault OTX pelos menos os seguintes itens:

- IPs Maliciosos;
- Urls Maliciosas;
- Hashs de Ameaças;

2.4.6 A solução deverá monitorar e realizar o processo de remoção de fraudes digitais como phishing scam, perfis falsos, aplicativos falsos ou uso indevido de marca, na internet superficial ou em qualquer ambiente onde um consumidor possa ser enganado.

2.4.7 A solução deverá monitorar e, sempre que possível, realizar o processo de remoção de conteúdo de propriedade da organização que esteja exposto, ou que tenha sido vazado, incluindo bases de dados internas (de clientes ou colaboradores), credenciais corporativas, credenciais roubadas por malwares, dados de cartão de crédito, código fonte em repositórios públicos contendo segredos (ex. tokens, senhas ou arquivos críticos de configuração).

2.4.8 A solução deverá monitorar dados expostos, vazados ou a venda, referente a executivos e VIPs da organização, bem como perfis falsos em redes sociais.

2.4.9 A solução deverá monitorar a citação da marca da organização e de seus ativos digitais em grupos e/ou fóruns da deep e dark web.

2.4.10 A CONTRATADA deverá ter serviços especializados de inteligência sobre riscos digitais (como novas técnicas usadas por criminosos e vulnerabilidades) e ameaças (grupos, quadrilhas etc.)

2.4.11 A solução deverá realizar o processo de remoção de conteúdo infrator ou fraudulento da internet.

2.4.12 A CONTRATADA deverá viabilizar a operação de todos os processos de forma unificada, centralizada e simplificada, garantindo eficiência, transparência e controle total para o time da operação.

2.4.13 A CONTRATADA deverá viabilizar a integração com os sistemas internos e automação de tarefas.

2.4.14 A CONTRATADA deverá suportar atividades operacionais para o time da organização.

2.4.15 A CONTRATADA deverá fornecer monitoramento de postura de segurança externa (ativos voltados à internet) da empresa e de seus fornecedores e terceiros.

2.4.16 Solução de Threat Intelligence

2.4.16.1 Monitoramento de Fraude Digital

2.4.16.1.1 Requisitos para Detecção de Estelionato:

2.4.16.1.1.1 Páginas que se passam pela empresa e oferecem produtos ou serviços em seu nome (estelionato);

2.4.16.1.1.2 Anúncios em buscadores que utilizam como palavras-chave as marcas da empresa e direcionam para sites falsos ou perfis falsos no WhatsApp.

2.4.16.1.2 Requisitos para Detecção de Phishing

2.4.16.1.2.1 Páginas falsas (phishing scam) que contenham testes de acesso com base em geolocalização;

2.4.16.1.2.2 Anúncios pagos em redes sociais que direcionam para páginas falsas (phishing scam), contemplando minimamente a cobertura dos sites Facebook e Instagram;

2.4.16.1.2.3 Anúncios em buscadores que utilizam como palavras-chave as marcas da empresa e direcionam para páginas falsas (phishing scam).

2.4.16.1.3 Requisitos para Detecção de Malware

2.4.16.1.3.1 Detecção de artefatos de malware direcionados aos domínios e/ou sistemas da empresa;

2.4.16.1.3.2 Análise de malware (engenharia reversa), extração de IOC (Indicators of Compromise) e endereços de comunicação utilizados pelo artefato;

2.4.16.1.3.3 Análise comportamental de malware (análise dinâmica) e elaborar relatório detalhado de seu funcionamento.

2.4.16.1.4 Requisitos para Detecção de Perfis Falsos em Redes Sociais

2.4.16.1.4.1 Perfis que se passam pela CONTRATANTE no TikTok;

2.4.16.1.4.2 Perfis que se passam pela CONTRATANTE no Twitter;

2.4.16.1.4.3 Perfis que se passam pela CONTRATANTE no Instagram;

2.4.16.1.4.4 Perfis que se passam pela CONTRATANTE no Facebook.

2.4.16.1.5 Requisitos para Monitoramento de Nomes de Domínio Similares

2.4.16.1.5.1 Domínios similares (typosquatting);

2.4.16.1.5.2 Domínios exatos em diferentes TLDs;

2.4.16.1.5.3 Domínios utilizando homógrafos (punycodes).

2.4.16.1.6 Requisitos para Monitoramento de Lojas Oficiais de Aplicativos e de Agregadores de Aplicativos

2.4.16.1.6.1 Loja Apple App Store e Google Play Store por aplicativos utilizando a marca da empresa;

2.4.16.1.6.2 Mínimo de 300 (trezentos) sites agregadores de aplicativos (APKs Mirrors).

2.4.16.1.7 Requisitos para Canais de Denúncia e Monitoramento de Sites Oficiais

2.4.16.1.7.1 Canal de Denúncia para que os clientes possam, através de interface web, denunciar páginas suspeitas e colocá-las no fluxo de validação automática ou manual;

2.4.16.1.7.2 Processa todas as denúncias recebidas através de canal de denúncia da empresa em regime 24/7, dispondo de opções de automatização;

2.4.16.1.7.3 Marcação das páginas da empresa para detectar a criação de páginas clonadas que utilizam a mesma estrutura das páginas de login da empresa;

2.4.16.1.7.4 Analisa automaticamente o tráfego de entrada às páginas da empresa para detectar irregularidades de referer.

2.4.16.1.8 Lista de Sites, Domínios, Aplicativos e Perfis Oficiais (Conteúdos Oficiais):

2.4.16.1.8.1 Oferece interface para gerenciar a lista com todos os sites, domínios, aplicativos e perfis oficiais, dentre outros conteúdos, da empresa e de seus parceiros externos;

2.4.16.1.8.2 Evita automaticamente a realização de takedowns de um conteúdo oficial cadastrado;

2.4.16.1.8.3 Mostra, dentro da plataforma, a lista de conteúdos oficiais, para que a empresa verifique se todos os seus conteúdos estão corretamente adicionados.

2.4.16.1.9 Requisitos para Processamento dos Incidentes

2.4.16.1.9.1 Armazena evidências de todos os incidentes coletados, como screenshot (no momento da captura), cópia do WHOIS e código HTML da página capturada;

2.4.16.1.9.2 Indica grau de risco associado ao incidente;

2.4.16.1.9.3 Indica evidências de risco associados ao incidente, como idioma, presença do logo e/ou do nome da marca;

2.4.16.1.9.4 Indicar no incidente a data exata da detecção, o código MD5 do HTML no momento da detecção, as informações disponíveis sobre o nome de domínio e os dados sobre o provedor;

2.4.16.1.9.5 Possui a capacidade de manter histórico individual de cada incidente detectado para atender a auditoria.

2.4.16.2 Monitoramento de Dados Vazados e Expostos

2.4.16.2.1 Requisitos para Detecção de Credenciais Corporativas Vazadas

2.4.16.2.1.1 Detecta credenciais corporativas (e-mail + senha ou HASH) de domínios da empresa que foram vazadas na Web superficial;

2.4.16.2.1.2 Detecta credenciais corporativas (e-mail + senha ou HASH) de domínios da empresa que foram vazadas na deep & darkweb;

2.4.16.2.1.3 Detecta credenciais corporativas (e-mail + senha ou HASH) de domínios da empresa que foram vazadas em sites de paste;

2.4.16.2.1.4 Detecta credenciais corporativas (e-mail + senha ou HASH) de domínios da empresa que foram vazadas em grandes vazamentos públicos (big leaks);

2.4.16.2.1.5 Envia alerta da senha vazada para a empresa (no ato da detecção);

2.4.16.2.1.6 Oferece relatório mensal com a síntese de todos os vazamentos e credenciais detectadas e suas respectivas fontes;

2.4.16.2.1.7 Analisa credenciais detectadas (utilizando modelo de machine learning) para excluir falsos positivos em tempo real, mostrando apenas casos de credenciais reais;

2.4.16.2.1.8 Mostra apenas credenciais que tragam e-mail corporativo e senha;

2.4.16.2.1.9 Identifica o tipo de HASH associado a senha detectada.

2.4.16.2.2 Requisitos para API & Webhook

2.4.16.2.2.1 Possui webhooks para alertar vazamentos de credenciais corporativas da empresa em tempo real;

2.4.16.2.2.2 Possui API para consulta de credenciais corporativas vazadas com sistemas utilizados pela empresa (logs de malware do tipo credential stealers que referenciam domínios da empresa).

2.4.16.2.3 Requisitos para Detecção de Cartões de Crédito Vazados

2.4.16.2.3.1 Cartões emitidos vazados com BINs da empresa na web superficial;

2.4.16.2.3.2 Cartões emitidos vazados com BINs da empresa na deep & dark web;

2.4.16.2.3.3 Cartões emitidos vazados com BINs da empresa em sites de paste;

2.4.16.2.3.4 Alerta em tempo real para o tratamento do cartão emitido vazado;

2.4.16.2.3.5 Relatório automatizado com todos os cartões emitidos vazados e fontes dos vazamentos;

2.4.16.2.3.6 Alerta via webhook vazamentos de cartões emitidos;

2.4.16.2.3.7 API para consulta de cartões emitidos pela CONTRATANTE, presentes na base de dados vazados;

2.4.16.2.3.8 Detecta e apresenta apenas cartões de crédito com CVV e data de expiração.

2.4.16.2.3.9 Requisitos para Tokens, Senhas ou Segredos em Código Fonte

2.4.16.2.3.10 Detecta chaves de código (tokens, senhas, arquivos críticos de configuração) expostos pela empresa na web superficial em, minimamente, 50 padrões diferentes de segredo e/ou token;

2.4.16.2.3.11 Detecta chaves de código (tokens, senhas, arquivos críticos de configuração) expostos pela empresa em códigos ou commits públicos no Github com SLA inicial de 5 minutos, a depender do tipo de detecção;

2.4.16.2.3.12 Apresenta um score de risco associado a chave exposta, encontrada em repositórios com menção aos domínios da CONTRATANTE.

2.4.16.2.4 Requisitos para Proteção contra credenciais de clientes vazadas

2.4.16.2.4.1 Fornece lista de credenciais vazadas (de usuários que tiveram seus dados vazados na internet) para que a empresa possa validar a existência de uma mesma credencial em sua base, com o objetivo de forçar o usuário a trocar a senha vazada. Esse serviço é disponibilizado via API e webhook com base histórica de no mínimo 7 anos.

2.4.16.2.5 Requisitos para Detecção de Documentos Vazados

2.4.16.2.5.1 Detecta e classifica compartilhamento de documentos e cyberlockers (ex: Scribid, 4shared);

2.4.16.2.5.2 Detecta e classifica informações compartilhadas em plataformas de gerenciamento de atividades (ex: Trello, Asana).

2.4.16.2.6 Requisitos para Detecção de Bases de Dados Expostas através de Fichas ou Tokens de Rastreamento

2.4.16.2.6.1 Monitora fichas ou tokens de rastreamento, com o objetivo de identificar bases internas que tenham sido expostas na web superficial, deep e darkweb. ou grandes vazamentos;

2.4.16.2.6.2 Alerta em tempo real da detecção de exposição de rastreadores de base de dados.

2.4.16.2.6.3 Requisitos para Detecção de Checkers

2.4.16.2.6.4 Detecta checkers que testam acesso (login) as áreas logadas da empresa.

2.4.16.2.7 Requisitos para Detecção de Logins roubados

2.4.16.2.7.1 Detecta logins (e-mail, username, telefone, cpf) e senhas que acessam aplicações da empresa que foram vazadas em logs de malware;

2.4.16.2.7.2 Alerta através da plataforma de logins expostos com informação de login, senha e url de acesso;

2.4.16.2.7.3 Detecta logins (e-mail, username, telefone, cpf) e senhas em grupos de Telegram;

2.4.16.2.7.4 Detecta logins (e-mail, username, telefone, cpf) e senhas na fonte IntelX.

2.4.16.3 Monitoramento de Executivos e VIPs

2.4.16.3.1 Requisitos para Detecção de Documentos pessoais

2.4.16.3.1.1 Vazamentos de nome, RG, CPF, CNH, e-mail e telefone de pessoas físicas na web superficial;

2.4.16.3.1.2 Vazamentos de nome, RG, CPF, CNH, e-mail, telefone e cartões de pessoas físicas em sites de paste;

2.4.16.3.1.3 Vazamentos de RG, CPF, CNH, e-mail e telefone de pessoas físicas na deep & dark web;

2.4.16.3.1.4 Vazamentos de RG, CPF, CNH, e-mail e telefone de pessoas físicas em grandes vazamentos públicos;

2.4.16.3.1.5 Exposição de dados de contatos pessoais em sites de vendas de leads;

2.4.16.3.1.6 Notifica entidades solicitando remoção de dados de contatos pessoais expostos em sites de vendas de leads.

2.4.16.3.2 Requisitos para Detecção de credenciais

2.4.16.3.2.1 Credenciais pessoais e corporativas (associadas a e-mails pessoais dos executivos) e corporativas na web superficial;

2.4.16.3.2.2 Credenciais pessoais e corporativas (associadas a e-mails pessoais dos executivos) e corporativas na deep & dark web.

2.4.16.3.3 Requisitos para Detecção de cartões de crédito

2.4.16.3.3.1 Dados vazados de cartões de crédito de propriedade dos executivos na web superficial;

2.4.16.3.3.2 Dados vazados de cartões de crédito de propriedade dos executivos na deep & dark web.

2.4.16.3.4 Requisitos para Detecção de Perfis pessoais falsos em redes sociais

2.4.16.3.4.1 Perfis que se passam pelos Executivos e VIPs no Twitter;

2.4.16.3.4.2 Perfis que se passam pelos Executivos e VIPs no Instagram;

2.4.16.3.4.3 Perfis que se passam pelos Executivos e VIPs no Facebook;

2.4.16.3.4.4 Perfis que se passam pelos Executivos e VIPs no LinkedIn;

2.4.16.3.4.5 Mecanismo anti-falso positivo para filtrar falsas ameaças através de tecnologia de reconhecimento facial, capaz de identificar o uso da imagem do Executivo ou VIP na ameaça;

2.4.16.3.4.6 Notifica automaticamente entidades solicitando remoção de perfis falsos de pessoas físicas em redes sociais.

2.4.16.3.5 Requisitos para Detecção de Dados de sócios, executivos e conselheiros

2.4.16.3.5.1 Exposição de dados pessoais de sócios de empresas em sites de informações sobre pessoas jurídicas (ex. Jusbrasil, Escavador);

2.4.16.3.5.2 Notifica automaticamente entidades solicitando remoção de dados pessoais de sócios de empresas em sites de informações sobre pessoas jurídicas.

2.4.16.3.6 Requisitos para Orientações de remediação (playbooks)

2.4.16.3.6.1 Apresenta orientações de tratamento e remediação para todos os casos detectados, inclusive aqueles que não são passíveis de remoção;

2.4.16.3.6.2 Gera relatório, no mínimo mensalmente, com consolidação dos dados expostos a respeito das pessoas físicas cadastradas.

2.4.16.3.7 Requisitos para Aquisição e custódia de dados sensíveis

2.4.16.3.7.1 Cadastra e custódia os dados sensíveis dos executivos, em conformidade com a LGPD, garantindo que o dado estará criptografado tanto in-rest quanto in-transit, ou seja, que o dado original só estará visível para o seu detentor ou quando requisitado.

2.4.16.4 Monitoramento de Deep & Dark web

2.4.16.4.1 Requisitos para Coletores e fontes

2.4.16.4.1.1 Coleta e alerta menções a marca, termos de monitoramento e fraudes em grupos infiltrados de mensagens;

2.4.16.4.1.2 Coleta e alerta menções a marca, termos de monitoramento e fraudes em fóruns e markets da Deep & Dark Web;

2.4.16.4.1.3 Coleta e alerta menções a marca, termos de monitoramento e fraudes em diversos sites suspeitos da Deep & Dark Web;

2.4.16.4.1.4 Coleta e envia menções dos termos monitorados de forma automatizada em real time (a partir da data de publicação das mensagens nas plataformas);

2.4.16.4.1.5 Coleta indicadores de comprometimento de diversas fontes como fóruns da Deep & Dark Web, grupos infiltrados em aplicativos de mensageria e pastes.

2.4.16.4.2 Requisitos para Plataforma

2.4.16.4.2.1 Classifica automaticamente os alertas por nível de risco e por categoria por meio de inteligência artificial;

- 2.4.16.4.2.2 Configura recebimento de alertas por e-mail e por nível de risco;
- 2.4.16.4.2.3 Disponibiliza permissionamento de usuários de acordo com os tipos de alertas;
- 2.4.16.4.2.4 Agrupa mensagens similares e idênticas, dando mais eficiência ao processo de análise das ameaças;
- 2.4.16.4.2.5 Permite a realização de buscas abertas no histórico de alertas;
- 2.4.16.4.2.6 Possibilita a filtragem de alertas por diversos atributos, permitindo encontrar casos prioritários de forma mais rápida;
- 2.4.16.4.2.7 Ordena os resultados de acordo com a data de detecção;
- 2.4.16.4.2.8 Exporta dados de alertas no padrão CSV;
- 2.4.16.4.2.9 Disponibiliza para consumo diretamente na plataforma os Global Threat Alert (GTAs) e Reports;
- 2.4.16.4.2.10 Permite a conexão de contas de Telegram já infiltradas em grupos de interesse para monitoramento automático destes.
- 2.4.16.4.3 Requisitos para Busca aberta
 - 2.4.16.4.3.1 Disponibiliza a busca aberta para pesquisa livre conforme necessidade do usuário, não restringindo aos assets contratados;
 - 2.4.16.4.3.2 Permite a utilização de operadores lógicos para buscas mais assertivas;
 - 2.4.16.4.3.3 Agrupa mensagens idênticas, dando mais eficiência ao processo de pesquisa;
 - 2.4.16.4.3.4 Ordena os resultados de acordo com relevância ou data de detecção;
 - 2.4.16.4.3.5 Possibilita a filtragem dos resultados por diversos atributos, como plataforma, atores maliciosos e grupos específicos;
 - 2.4.16.4.3.6 Possibilita o salvamento de uma determinada busca combinada com seus filtros e permite que ela seja recuperada no futuro sem que seja necessário reconfigurar.
- 2.4.16.4.4 Requisitos para Configuração de coletas
 - 2.4.16.4.4.1 Possibilita a configuração de coleta pelo usuário com base nos termos de interesse para que sejam gerados tickets de detecção sempre que houver match com qualquer postagem em grupos, canais, fóruns e markets;
 - 2.4.16.4.4.2 Disponibiliza configuração de acordo com o tipo de conteúdo da postagem, permitindo a exclusão de alertas indesejados.
- 2.4.16.4.5 Requisitos para Alertas
 - 2.4.16.4.5.1 Identifica e disponibiliza a plataforma onde a postagem foi encontrada com a sua URL, se existir;
 - 2.4.16.4.5.2 Identifica e disponibiliza o ator e grupo onde a mensagem de WhatsApp, Telegram e Discord foi encontrada;
 - 2.4.16.4.5.3 Identifica e disponibiliza o contexto das postagens em mensagerias, permitindo visualizar as mensagens anteriores e posteriores à detectada;
 - 2.4.16.4.5.4 Categoriza os alertas por nível de risco, para facilitar o tratamento;
 - 2.4.16.4.5.5 Categoriza os alertas a partir do tipo de conteúdo contido no mesmo, utilizando inteligência artificial;
 - 2.4.16.4.5.6 Exibe a coleta responsável pela geração do alerta, facilitando a análise para ajustes nas configurações;
 - 2.4.16.4.5.7 Possibilita a adição de comentários nos alertas para registros históricos;
 - 2.4.16.4.5.8 Possibilita a adição de tags nos alertas para organização interna.
- 2.4.16.4.6 Requisitos para Perfil do Ator Malicioso
 - 2.4.16.4.6.1 Apresenta informações detalhadas sobre o emissor das mensagens (ator malicioso) de WhatsApp, Telegram e Discord com a volumetria das suas interações ao longo do tempo;
 - 2.4.16.4.6.2 Apresenta a correlação do ator com outros perfis similares;
 - 2.4.16.4.6.3 Apresenta o score de risco de cada ator associado ao potencial de distribuição de informação do ator;
 - 2.4.16.4.6.4 Apresenta quando o ator foi visto pela primeira e última vez, auxiliando na análise se aquele ator segue ativo;
 - 2.4.16.4.6.5 Exibe os principais grupos e canais onde o ator realiza suas atividades;
 - 2.4.16.4.6.6 Identifica as indústrias-alvo do ator;
 - 2.4.16.4.6.7 Permite a visualização de todas as mensagens e posts detectadas do ator;
 - 2.4.16.4.6.8 Permite a visualização de todas os alertas do ator que foram criados para os seus ativos;
 - 2.4.16.4.6.9 Apresenta outros números e nomes que um mesmo ator pode utilizar em diferentes plataformas.
- 2.4.16.4.7 Requisitos para Análise usando Inteligência Artificial
 - 2.4.16.4.7.1 Analisa as imagens usando algoritmos de visão computacional para identificar textos e viabilizar a busca dentro do conteúdo textual das imagens;
 - 2.4.16.4.7.2 Analisa e transcreve áudios e vídeos para viabilizar a busca dentro do conteúdo textual dessas mídias;
 - 2.4.16.4.7.3 Resume principais menções à marca usando LLM.
- 2.4.16.4.8 Requisitos para Solicitação de investigação
 - 2.4.16.4.8.1 Permite a solicitação de serviços de investigação de alertas, atores maliciosos e boletins diretamente na plataforma.
- 2.4.16.4.9 Requisitos para Monitoramento de Infraestrutura Exposta
 - 2.4.16.4.9.1 Permite a configuração de IPs e range de IPs para monitoramento de vulnerabilidades e portas expostas desses dispositivos;
 - 2.4.16.4.9.2 Permite filtrar por alertas que contém CVEs (Common Vulnerabilities and Exposures) para encontrar e tratar os casos mais críticos de forma mais rápida;
 - 2.4.16.4.9.3 Disponibiliza como arquivo anexo mais detalhes sobre o IP com vulnerabilidades, detalhes da CVE, quando tiver, entre outras informações que ajudam no tratamento do caso;
 - 2.4.16.4.9.4 Oferece recomendações sobre como tratar os cenários de vulnerabilidade e disponibiliza referências sobre cada CVE encontrada.
- 2.4.16.4.10 Requisitos para Notificação por e-mail
 - 2.4.16.4.10.1 Notificação por e-mail de criação de ticket de detecção;
 - 2.4.16.4.10.2 Possibilita a configuração por parte do usuário para ser notificado de acordo com o grau de risco selecionado.
- 2.4.16.4.11 Requisitos para Relatórios
 - 2.4.16.4.11.1 Envia relatórios mensais contendo informações gerais sobre os dados de monitoramento do cliente e fazendo comparativos com meses anteriores;
 - 2.4.16.4.11.2 Envia relatório com fraudes gerais na deep & dark web;
 - 2.4.16.4.11.3 Acesso a lista de número de telefone de usuários participantes de grupos de fraude;
 - 2.4.16.4.11.4 Relatórios com detalhamento de ameaças com alta abrangência no mercado.
- 2.4.16.4.12 Requisitos para Alerta de anomalias

2.4.16.4.12.1 Permite a configuração de alertas quando ocorrer uma anomalia no volume de eventos a partir de uma query na busca aberta;

2.4.16.4.12.2 Permite a visualização da regra aplicada e deleção de alertas já existentes;

2.4.16.4.12.3 Verifica por novas anomalias a cada 1 hora;

2.4.16.4.12.4 Os alertas podem ser configurados considerando uma variação percentual a partir da média histórica ou considerando um valor absoluto de eventos;

2.4.16.4.12.5 Alertas enviados via notificação na plataforma e por e-mail para os usuários do time;

2.4.16.4.12.6 Opção aos usuários de optarem pelo recebimento dos alertas de anomalia por e-mail ou desabilitação desse tipo de envio.

2.4.16.5 Cyber Threat Intel

2.4.16.5.1 Requisitos para Pesquisa e Investigação

2.4.16.5.1.1 Realiza análise de artefatos maliciosos de modo a extrair IOCs (Indicadores de Comprometimento) e TTPs a serem utilizados para o entendimento da ameaça;

2.4.16.5.1.2 Constrói estratégias de contrainteligência customizadas e exclusivas para apoio as investigações cibernéticas;

2.4.16.5.1.3 Apoia as equipes internas no entendimento de fraudes e incidentes cibernéticos;

2.4.16.5.1.4 Monitoramento ativo dos principais grupos e atores envolvidos em casos de ameaças de ransomware;

2.4.16.5.1.5 Fornece verificação em tempo real de números de telefones atribuídos a contas de Whatsapp de atores ofensores de modo a permitir integração sistêmica através de API;

2.4.16.5.1.6 Adquire insumos de modo a apoiar investigações cibernéticas no sentido de entendimento dos TTPs dos ataques direcionados a organização.

2.4.16.5.2 Requisitos para Monitoramento e Alerta

2.4.16.5.2.1 Envia alertas emergenciais e/ou críticos relacionados a ameaças cibernéticas setoriais;

2.4.16.5.2.2 Envia alertas emergenciais e/ou críticos relacionados a ameaças cibernéticas que impactem a organização e/ou seus colaboradores;

2.4.16.5.2.3 Fornece de forma automatizada o compartilhamento de IOCs focados na região de atuação da organização, diretamente na plataforma, sem a necessidade de criar uma instância no MISP;

2.4.16.5.2.4 Realiza infiltrações em fóruns e darkmarkets;

2.4.16.5.2.5 Realiza infiltrações em canais de comunicação comumente utilizado por atores tais como IRC, Skype, Discord, Whatsapp, Telegram, Signal, Jabber, ICQ, TOX dentre outros.

2.4.16.5.3 Requisitos para Resposta a Incidentes

2.4.16.5.3.1 Apoia o cliente na resposta a questionamentos por agentes da lei nos casos investigativos;

2.4.16.5.3.2 Apoia de forma estratégia e tática casos de resposta a incidente que demandem entendimento externo da ameaça;

2.4.16.5.3.3 Apoia de forma estratégia e tática casos de resposta a incidente que demandem análise de artefatos maliciosos (ex. ransomware).

2.4.16.5.4 Requisitos para Relatórios

2.4.16.5.4.1 Elabora relatórios contendo TTPs (Táticas, Técnicas e Procedimentos) dos atores;

2.4.16.5.4.2 Fornece relatórios situacionais relacionados a ameaças cibernéticas que impactem a organização e/ou seus colaboradores;

2.4.16.5.4.3 Fornece relatórios situacionais relacionados a ameaças cibernéticas setoriais.

2.4.16.6 Takedown & SLA

2.4.16.6.1 Requisitos para Notificação

2.4.16.6.1.1 Notifica perfis ou páginas falsas em redes sociais (Facebook, Instagram, Tiktok, Youtube, Twitter, Pinterest, entre outras);

2.4.16.6.1.2 Notifica casos de Phishing, Malware;

2.4.16.6.1.3 Notifica entidades de navegadores e antivírus sobre Phishings e Malwares para mitigação do risco e bloqueio de acesso em navegadores;

2.4.16.6.1.4 Renotificar dos casos que continuam ativos;

2.4.16.6.1.5 Capacidade de gerenciar templates de notificação para os diferentes tipos de ameaças digitais ou fraudes;

2.4.16.6.1.6 Notifica automaticamente plataformas e provedores de hospedagem;

2.4.16.6.1.7 Notifica automaticamente 24/7;

2.4.16.6.1.8 Preenchimento automático de formulários com informações do cliente para notificações;

2.4.16.6.1.9 Adiciona evidências que comprovem a atividade fraudulenta que afeta a marca oficial;

2.4.16.6.1.10 Confirma denúncias recebidas por e-mail de entidades;

2.4.16.6.1.11 Define fluxos de notificação automatizados para diversos contatos e meios (API, formulário).

2.4.16.6.1.12 SLA de primeira notificação em até 5 minutos após a solicitação de Takedown.

2.4.16.6.2 Requisitos para Cobrança e Pacotes

2.4.16.6.2.1 Não contabiliza casos interrompidos ou não resolvidos no contador de Takedown;

2.4.16.6.2.2 Reabre casos que voltarem a ter atividade fraudulenta em até 15 dias após o tratamento.

2.4.16.6.3 Requisitos para SLAs de 1ª notificação, renotificação, transparência e verificação

2.4.16.6.3.1 Informa o tempo médio para a primeira notificação para casos de perfis e páginas falsas de Facebook, Instagram e Tiktok;

2.4.16.6.3.2 Informa o tempo médio para a primeira notificação de phishings;

2.4.16.6.3.3 Tempo para primeira notificação de, no mínimo, 5 minutos;

2.4.16.6.3.4 Informa o tempo médio para renotificação de perfis ou páginas falsas em Facebook, Instagram e Tiktok;

2.4.16.6.3.5 Informa o tempo médio para renotificação para phishing e malware;

2.4.16.6.3.6 Informa a frequência com a qual as URLs são verificadas para detectar se o conteúdo foi removido.

2.4.16.6.4 Requisitos para Questões legais

2.4.16.6.4.1 Utiliza o endereço do e-mail da empresa nas notificações.

2.4.16.6.5 Requisitos para Evidências e plataforma

2.4.16.6.5.1 Possibilita o acompanhamento de notificações e verificações para cada ameaça em tempo real diretamente da plataforma;

2.4.16.6.5.2 Possibilita o entendimento sobre o motivo de interrupção em casos com tratativas interrompidas diretamente na plataforma;

2.4.16.6.5.3 Disponibiliza para download de evidências das notificações realizadas, caso necessário, para processo judicial ou outras demandas internas da CONTRATANTE.

2.4.16.6.6 Requisitos para Relatórios

2.4.16.6.6.1 Disponibiliza em tempo real dados atualizados de tempo médio de remoção, volume de takedowns por situação de tratamento.

2.4.16.7 Plataforma

2.4.16.7.1 Requisitos para Acessos e gestão de usuários

2.4.16.7.1.1 Possui autenticação de dois fatores (2FA) para realização do acesso à plataforma;

2.4.16.7.1.2 Possibilita o uso da plataforma em inglês, espanhol e português;

2.4.16.7.1.3 Quantidade ilimitada de usuários;

2.4.16.7.1.4 Oferece configurações avançadas de acesso de usuários;

2.4.16.7.1.5 Possui capacidade de personalização de alertas por e-mail;

2.4.16.7.1.6 Possui capacidade de consulta às atividades que os usuários realizaram e exportação em formato CSV desses dados.

2.4.16.7.2 Requisitos para Gestão de ameaças detectadas

2.4.16.7.2.1 Possui listas para classificação e acompanhamento das ameaças conforme seu status;

2.4.16.7.2.2 Ordenação de acordo com o grau de risco das ameaças;

2.4.16.7.2.3 Realiza ações em lote;

2.4.16.7.2.4 Exportação dos dados das ameaças;

2.4.16.7.2.5 Adição de anotações nas ameaças detectadas;

2.4.16.7.2.6 Exibe a origem de detecção de cada ameaça e o critério de match;

2.4.16.7.2.7 Capacidade de gestão através da utilização de tags nas ameaças;

2.4.16.7.2.8 Capacidade de detectar que conteúdo apresenta inatividade e encerrar ticket automaticamente.

2.4.16.7.3 Requisitos para Quarentena

2.4.16.7.3.1 Quarentena para monitoramento de alterações no conteúdo das ameaças detectadas;

2.4.16.7.3.2 Alerta para conteúdo em quarentena que sofreram alguma alteração, sendo ela de inclusão, exclusão ou atualização do conteúdo;

2.4.16.7.3.3 Alerta para perfis de redes sociais em quarentena que receberam o logo da instituição nas fotos de perfil.

2.4.16.7.4 Requisitos para Evidências das ameaças

2.4.16.7.4.1 Coleta screenshots das páginas detectadas como ameaças;

2.4.16.7.4.2 Coleta informações sobre o domínio de cada ameaça detectada;

2.4.16.7.4.3 Coleta o HTML das páginas detectadas como ameaças;

2.4.16.7.4.4 Atribui grau de risco de cada ameaça com a utilização de machine learning;

2.4.16.7.4.5 Identifica características da ameaça com base em modelos de machine learning;

2.4.16.7.4.6 Detecta campos para coleta de dados automaticamente (campos de preenchimento de dados de cartão de crédito e de senha) usando algoritmos de machine learning.

2.4.16.7.5 Requisitos para Gestão de automações

2.4.16.7.5.1 Automatiza ações sobre ameaças detectadas com base em critérios pré-definidos, inclusive realização de takedowns;

2.4.16.7.5.2 Identifica padrões em ameaças a partir de modelos de machine learning, como logo, menção à marca monitorada, entre outros, para utilização nos critérios para automação.

2.4.16.7.6 Requisitos para Gestão de configurações de monitoramento

2.4.16.7.6.1 Gestão dos termos monitorados;

2.4.16.7.6.2 Gestão dos termos excluídos do monitoramento;

2.4.16.7.6.3 Possui termos sugeridos para o monitoramento;

2.4.16.7.6.4 Exporta os dados em formato CSV;

2.4.16.7.6.5 Gestão dos ativos monitorados (marcas, domínios e executivos) que permita, minimamente, criar, editar e desabilitar ou remover tal ativo;

2.4.16.7.6.6 Gestão dos escopos e monitoramento por ativo;

2.4.16.7.6.7 Listagem das fontes monitoradas e status do monitoramento.

2.4.16.7.7 Requisitos para Gestão de conteúdos oficiais

2.4.16.7.7.1 Gestão dos conteúdos oficiais (domínios, urls, aplicativos oficiais, redes sociais oficiais);

2.4.16.7.7.2 Gestão de conteúdos de parceiros (domínios, urls, aplicativos, redes sociais);

2.4.16.7.7.3 Gestão de conteúdos idôneos (domínios, urls, aplicativos, redes sociais);

2.4.16.7.7.4 Possui capacidade de exportar os dados em formato CSV.

2.4.16.7.8 Requisitos para Relatórios de resultados

2.4.16.7.8.1 Interface para visualização de gráficos com dados relacionados aos takedowns solicitados;

2.4.16.7.8.2 Interface para visualização de gráficos com dados relacionados às etapas do ciclo de vida das detecções;

2.4.16.7.8.3 Interface para visualização de gráficos com dados relacionados à cada tipo de solução oferecida;

2.4.16.7.8.4 Interface para visualização de gráficos com dados comparativos de mercado;

2.4.16.7.8.5 Capacidade de filtro dos resultados por período e por tipo de ameaça.

2.4.16.8 Integrações e APIs (SIEM e SOAR)

2.4.16.8.1 Requisitos para API HTTP

2.4.16.8.1.1 Disponibiliza API devidamente documentada que permite aplicativos externos acessem e manipulem informações;

2.4.16.8.1.2 Possui documentação com exemplos de utilização das APIs disponibilizadas;

2.4.16.8.1.3 Possui níveis de permissionamento, proporcionando certas operações de acordo com permissões dos usuários;

2.4.16.8.1.4 Capacidade de fazer buscas avançadas por ameaças;

2.4.16.8.1.5 Retorna detalhes sobre as ameaças a partir das operações de busca;

2.4.16.8.1.6 Possui capacidade de realizar ações em ameaças detectadas, como criar incidente e solicitar takedown;

2.4.16.8.1.7 Possui capacidade de gestão completa de ameaças.

2.4.16.8.2 Requisitos para outras integrações

2.4.16.8.2.1 Possui capacidade de integração com protocolo SAML para autenticação SSO;

2.4.16.8.2.2 Possui capacidade de integração com a plataforma The Hive.

2.4.17 Certificação Profissional da Equipe de Threat Intelligence

2.4.17.1 Devido à complexidade das ferramentas que deverão ser suportadas pela Contratada e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõem o parque de segurança do CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com profissionais que possuam ao menos uma das certificações abaixo:

- CEH - Certified Ethical Hacker;

- CISA - CompTIA Cybersecurity Analyst

- CompTIA security+

- FCSS - Fortinet Certified Solution Specialist

- Fortinet FCP – Network Security

- Fortinet NSE4 - Network Security Expert Level 4

2.4.18 Serviços de Instalação

2.4.18.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.

2.4.18.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;

2.4.18.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;

2.4.18.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;

2.4.18.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;

2.4.18.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;

2.4.18.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;

2.4.18.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

2.4.18.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

2.4.18.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da CONTRATANTE.

2.4.18.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.4.18.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.4.18.10 A montagem e instalação de todos os componentes que compoem solução adquirida são de responsabilidade da CONTRATADA.

2.4.18.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.4.18.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.4.18.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.4.18.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.4.18.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.4.18.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.4.18.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.4.18.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.4.18.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.5 SOLUÇÃO PARA VALIDAÇÃO DE SEGURANÇA CONTÍNUA (BAS)

2.5.1 Contratante disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.5.2 Requerimentos Gerais

2.5.2.1 A solução deve proporcionar simulação, avaliação e gestão estendida da postura de segurança da organização, permitindo medir a efetividade através de testes e avaliações do nível de proteção do perímetro e de ambientes internos para que haja uma compreensão completa quanto a efetividade dos controles de segurança.

2.5.2.2 A solução deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.

2.5.2.3 A plataforma deve fornecer capacidades diferentes que permitam escalabilidade sem troca futura, atendendo minimamente

conceitos como validação de brechas e simulações de ataques (BAS), automatização de Red e Purple Teaming (CART), gerenciamento da superfície de ataques (ASM) e priorização e contextualização de vulnerabilidade.

2.5.2.4 A plataforma deve se alinhar ao programa de gerenciamento contínuo de ameaças - CTEM do Gartner, atendendo minimamente 4 das etapas deste programa: escopo, descoberta, priorização, validação e mobilização.

2.5.2.5 A solução deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.

2.5.2.6 A solução deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:

2.5.2.6.1 Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalção de privilégio.

2.5.2.6.2 Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

2.5.2.6.3 Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais.

2.5.2.6.4 Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

2.5.2.6.5 A solução deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

2.5.2.6.6 A solução deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

2.5.2.6.7 A solução deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

2.5.2.6.8 As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

2.5.2.6.9 A solução deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

2.5.2.6.10 A solução deve possuir suporte e licenciamento realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

2.5.2.6.11 A solução deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

2.5.3 Requerimentos funcionais e arquitetura

2.5.3.1 A solução deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD, OKTA, JumpCloud entre outros.

2.5.3.2 A solução deve permitir a integração com diferentes plataformas de segurança via API.

2.5.3.2.1 Todos os componentes da solução devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

2.5.3.2.2 Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

2.5.3.3 A solução deve suportar a comunicação dos componentes instalados por meio de um proxy web.

2.5.3.4 O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

2.5.3.5 A solução não deve possuir limitações em seus agentes, simuladores ou atores de ataque.

2.5.3.6 A solução deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

2.5.3.7 A solução deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

2.5.3.8 A solução deve ser capaz de poder trocar informações com outras tecnologias de segurança do ambiente para fornecer, melhor visibilidade na detecção, gestão de vulnerabilidades, automação de playbooks e validação de processos internos. Permitindo no mínimo as seguintes integrações:

- Azure Sentinel
- BlackBerry Cylance OPTICS
- BlackBerry Cylance PROTECT
- Carbon Black
- CrowdStrike Falcon
- CrowdStrike Falcon LogScale
- Chronicle
- Cynet
- IBM Qradar
- InsightVM
- LogRhythm
- McAfee ESM SIEM
- MicroFocus ArcSight
- Microsoft Defender ATP
- Microsoft Defender TVM
- Nexpose
- Palo Alto Cortex XDR
- Palo Alto Cortex XSOAR
- Palo Alto Firewall
- Qualys VM
- RSA Archer
- RSA Netwitness

- SentinelOne
- Service Now
- Securonix
- Splunk
- Sumo logic SIEM
- Tenable IO
- Tenable SC
- Trellix EDR
- Trellix HX
- Trend Micro Vision One
- Tanium

2.5.3.9 Todos os produtos de segurança que não possuem integração direta, devem poder ser integrados por meio soluções de correlacionamento de eventos (SIEM), permitindo a integração com produtos não homologados.

2.5.3.10 A solução deve fornecer suporte a regras SIGMA e suportar através de uma interface amigável capacidade de conversão das regras para padrões que possam ser utilizados em diferentes plataformas através da geração de scripts ou queries, suportando conversão para minimamente as seguintes tecnologias:

- Arcsight
- Azure Sentinel
- ElastAlert
- Elastic Search
- Humio
- IBM Qradar
- Kibana
- Limacharlie
- Logpoint
- Netwitness
- Splunk
- Sumologic

2.5.3.11 A solução deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.

2.5.3.12 A solução deve permitir avaliar as capacidades de defesa da organização contra táticas, técnicas e procedimentos utilizados por grupos criminosos conhecidos.

2.5.3.13 A solução deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.

2.5.3.14 A solução deve permitir a criação de perfis de adversários.

2.5.3.15 O portfólio de ataques da solução deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS, Microsoft DRAPE e NIST.

2.5.3.16 As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.

2.5.3.17 A solução deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:

2.5.3.18 Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:

- Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.
- Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo estes realizar a descoberta de hosts vulneráveis e simular a proliferação para eles através de técnicas utilizando protocolos tais como SMB.
- Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.
- Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.
- MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

2.5.3.19 Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

- Phishing: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção de ataques de phishing, acessando IPs e URLs reais associados a ataques de phishing identificados recentemente.
- Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.
- C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.
- Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.
- Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.
- Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares que simulam o comportamento de worms,

trojans e ransomware.

2.5.3.20 Para validação do vetor de e-mail gateway a plataforma deve oferecer simulações de ataque para:

- Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.
- Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.
- Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente
- Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.
- Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.
- Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.
- True File Type Detection: Validação da efetividade dos recursos de proteção de e-mail através do envio de arquivos com diferentes extensões não pertencentes ao seu formato de arquivo original, este teste deve apoiar na identificação de possíveis brechas que podem ser utilizadas para comprometer o ambiente através da falsificação de formatos originais de arquivos.

2.5.3.21 Para validação de vazamento de dados (DLP) a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

- HTTP & HTTPS: Exfiltração de dados por HTTP/S, injetando dados confidenciais em cabeçalhos de solicitação HTTP/S enviados para um servidor remoto.
- Browser HTTP & HTTPS: Exfiltração de dados através de navegadores como IE, Edge e/ou Chrome.
- DNS: Exfiltração de dados pela porta 53.
- Tunelamento DNS: Exfiltração de dados sobre o protocolo DNS (túnel através de servidores DNS públicos). Injetando dados confidenciais em uma solicitação de DNS enviada a servidores DNS públicos.
- Tunelamento ICMP: Exfiltração de dados sobre cabeçalhos ICMP. Injetando dados confidenciais em um pacote de eco (ECHO) enviado para um servidor remoto.
- Telnet: Exfiltração de dados pela porta de rede Telnet 23.
- SFTP: Exfiltração de dados sobre o protocolo SFTP.
- Outras Portas: Exfiltração através do upload de dados confidenciais para servidores de hospedagem de arquivos externos por meio de portas de rede abertas.
- E-mail: Usando e-mail corporativo no Outlook para transmitir dados confidenciais.
- Serviços de nuvem: Exfiltração de dados confidenciais para ou por meio de serviços e aplicativos em nuvem.
- Dispositivos Removíveis: Exfiltração de dados confidenciais através da cópia para dispositivos de mídia removíveis, como USB.

2.5.3.22 Para validação de movimentação lateral a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

- Pass-the-Password
- Pass-the-Ticket
- Pass-the-Hash
- Brute Force
- LLMNR/NBT-NS Poisoning and Relay
- Kerberoast
- Password Spraying
- Steal LAPS passwords

2.5.3.23 A solução deve fornecer a possibilidade de criar modelos customizados nos vetores de ataque sem causar impactos ao ambiente.

2.5.3.24 Para o cenário de movimentação lateral, o agente da solução deve poder atuar exatamente como um atacante no ambiente, não devendo este depender da implementação de outros agentes para validação dos diferentes métodos. A plataforma deve possuir capacidade de realizar um “pivoting” na rede e fornecer um mapa de toda trilha percorrida e alvos alcançados, podendo os alvos serem considerados ou não joias da coroa (Crown Jewels).

2.5.3.25 A solução deve fornecer um caminho para validação completa da cadeia de ataque (Full Kill-chain), permitindo assim que seja avaliadas fases tais como pré-exploração, exploração e pós-exploração.

2.5.3.26 A solução deve permitir a criação de campanhas de phishing customizadas para avaliação da conscientização dos colaboradores em cenários reais, as campanhas devem minimamente permitir que sejam criados conteúdos através da plataforma em português.

2.5.3.27 Cada um dos testes ou ações hospedadas na base de conhecimento da solução, deve ter uma descrição e o código da técnica ou das táticas de acordo com a nomenclatura do MITRE.

2.5.3.28 A solução deve ter a capacidade de repetir periodicamente os testes que o usuário deseja e comparar os resultados de cada execução com um resultado esperado, permitindo definir se o ataque foi detectado, bloqueado e que tipo de registro foi detectado no SIEM ou nas tecnologias de segurança testadas.

2.5.3.29 Os componentes de ataque devem poder ser instalados, minimamente, nos seguintes ambientes:

- Windows 11 build 22000+, 10 build 1067, 8.1, 7 SP1 Server 2012 ou superior;
- Linux Alpine 3.12, Ubuntu 16.04, Debian 10, CentOS 7, RHEL 7, Fedora 33, openSUSE 15 e SUSE Enterprise 12 SP2 ou versões superiores;
- MacOS 10.15x ou superior;

- A solução deve realizar as simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

2.5.4 Requerimentos de gestão e relatório

2.5.4.1 A solução deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

2.5.4.2 O painel principal (dashboard) deve apresentar de forma clara os vetores licenciados assim também como informações sobre controles de segurança, ameaças emergentes, integrações e outros detalhes importantes que possam ser utilizados para melhor compreensão dos testes realizados.

2.5.4.3 A console de gerenciamento deve permitir a criação de painéis dinâmicos aos quais permitam a customização e manipulação de dados a serem apresentados no novo painel (dashboard).

2.5.4.4 A console de gerenciamento deve possuir um dashboard que exiba todas as informações de vulnerabilidades baseadas em ataques, incluindo proteção geral de controles de segurança, principais vulnerabilidades encontradas em ativos de rede, principais ativos vulneráveis, principais CVEs e muito mais.

2.5.4.5 A console deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

2.5.4.6 A console deve fornecer uma visão global dos itens que foram identificados.

2.5.4.7 A console deve fornecer uma visão detalhada após integração com plataformas de gestão

2.5.4.8 A solução deve possuir uma interface amigável em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

2.5.4.9 Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

2.5.4.10 A solução deve permitir a geração de relatórios técnicos ou gerenciais aos quais devem conter minimamente:

- Informações sobre o score de risco atual;

- Descrição e recomendação para correção dos problemas encontrados;

2.5.4.11 A solução deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

2.5.4.12 A solução deve permitir a geração, download e envio de relatórios por e-mail através de sua interface.

2.5.4.13 A solução deve permitir a geração de relatórios e visão detalhada por ambientes.

2.5.4.14 A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

2.5.4.15 A solução deve fornecer um caminho simples para minimamente:

- Realizar a abertura de chamados;

- Gerenciar usuários da plataforma;

- Acessar documentações do produto;

- Gerenciar logs e atividades em execução.

2.5.4.16 A console deve fornecer uma guia para download e gestão dos agentes implementados.

2.5.5 Certificação Profissional da Equipe de BAS

2.5.5.1 Devido à complexidade das ferramentas (fornecidas como serviço) que deverão ser suportadas pela CONTRATADA e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõem o parque de segurança do CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com profissionais que possuam ao menos uma das certificações abaixo:

- CEH - Certified Ethical Hacker;

- CYSA+ - CompTIA Cybersecurity Analyst

- CompTIA security+

- FCSS - Fortinet Certified Solution Specialist

- Fortinet FCP – Network Security

- Fortinet NSE4 - Network Security Expert Level 4

2.5.6 Serviços de Instalação

2.5.6.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.

2.5.6.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;

2.5.6.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;

2.5.6.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;

2.5.6.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;

2.5.6.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;

2.5.6.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;

2.5.6.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

2.5.6.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

2.5.6.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da

CONTRATANTE.

2.5.6.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.5.6.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.5.6.10 A montagem e instalação de todos os componentes que compoñham solução adquirida são de responsabilidade da CONTRATADA.

2.5.6.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.5.6.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.5.6.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.5.6.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.5.6.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.5.6.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.5.6.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.5.6.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.5.6.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.6 SOLUÇÃO DE GESTÃO DE ACESSOS PRIVILEGIADOS (PAM)

2.6.1 A solução de Gerenciamento de Acessos Privilegiados (PAM) tem como objetivo reforçar a segurança dos sistemas críticos da instituição, por meio da proteção, controle e auditoria dos acessos administrativos e privilegiados realizados por usuários internos, terceiros ou sistemas automatizados.

2.6.2 A solução deverá proporcionar:

- Armazenamento seguro e controle do ciclo de vida de credenciais privilegiadas;
- Monitoramento em tempo real e gravação de sessões privilegiadas, com possibilidade de bloqueio de ações suspeitas;
- Aplicação de políticas de acesso baseadas em risco, tempo, escopo e autorização;
- Rastreamento completo e geração de evidências de uso privilegiado, com foco em conformidade e auditoria;
- Integração com sistemas de autenticação existentes (como diretórios corporativos e mecanismos de autenticação multifator);
- Mitigação de riscos operacionais e redução da superfície de ataque associada ao uso indevido de credenciais críticas.

2.6.3 Essa contratação visa atender às diretrizes de segurança da informação, conformidade legal (incluindo LGPD) e boas práticas recomendadas por normativos como ISO/IEC 27001 e frameworks de governança pública.

2.6.4 Para fins de planejamento, licenciamento e implantação da solução de Gerenciamento de Acessos Privilegiados (PAM), considera-se como base o ambiente tecnológico atualmente em operação na CONTRATADA, composto aproximadamente por:

- 800 (oitocentos) usuários ativos, com credenciais integradas a um diretório corporativo;
- 50 (cinquenta) usuários com perfil de acesso privilegiado, que deverão ser incluídos no escopo de controle e monitoramento da solução de PAM;
- 30 (trinta) contas de serviço ou técnicas, utilizadas por sistemas, scripts e integrações automatizadas;
- 105 (cento e cinco) servidores Windows e 180 (cento e oitenta) servidores Linux, operando em infraestrutura física e virtualizada;
- 3 (três) florestas e 3 (três) domínios únicos no Active Directory, com autenticação centralizada e políticas de segurança aplicadas em nível de domínio.

2.6.5 A abrangência mínima da solução de PAM deverá contemplar integralmente os usuários com perfil de acesso privilegiado e os servidores gerenciados, garantindo controle, proteção, rastreabilidade e conformidade para os acessos a esses ativos críticos.

2.6.6 O escopo dos serviços de implementação contratados deverá incluir a configuração e integração da solução de PAM com todos os elementos acima descritos, abrangendo a oneração inicial de contas privilegiadas, mapeamento de fluxos de acesso, políticas de uso, workflows de aprovação, gravação de sessões e autenticação segura para os ativos e usuários listados.

2.6.7 A CONTRATADA deverá concluir a implantação da solução em até 06 (seis) meses, contados a partir da assinatura do contrato. Após essa etapa, será iniciado o período de suporte técnico e manutenção evolutiva/corretiva, totalizando um prazo de 60 (sessenta) meses de vigência contratual, contados desde a assinatura.

2.6.8 As empresas concorrentes poderão solicitar informações complementares sobre o ambiente durante o período definido no edital de licitação, conforme os prazos e regras previstos no instrumento convocatório, caso necessário para suas estimativas de licença ou serviço.

2.6.9 Requisitos gerais da solução

2.6.9.1 A solução de gerenciamento privilegiado deverá controlar, monitorar e governar contas e atividades de usuários privilegiados para identificar possíveis atividades maliciosas, detectar riscos de direitos e fornecer evidências à prova de violação.

2.6.9.2 A solução deverá auxiliar na investigação de incidentes, no trabalho forense e nos esforços de conformidade.

2.6.9.3 Os pontos analisados esperados nesta solução são:

- Solução completa para todas as necessidades de gerenciamento de acesso privilegiado;
- Fácil de implantar e integrar;
- Profundidade de gravação;
- Análise de risco abrangente de direitos e atividades;
- Governança completa para conta privilegiada;

2.6.9.4 A solução deve automatizar, controlar e proteger o processo de concessão de credenciais privilegiadas com gerenciamento de acesso baseado em função e fluxos de trabalho automatizados, através de cofre de senhas, chaves e segredos para proteger ativos, incluindo computadores, servidores, dispositivos de rede, diretórios e aplicativos.

2.6.9.5 A solução deve gerenciar sessões privilegiadas, fornecendo controle de acesso, bem como monitoramento e gravação de sessões para evitar o uso indevido de contas privilegiadas, facilitar a conformidade e acelerar as investigações forenses.

2.6.9.6 A solução deve capturar os dados de atividade necessários para a criação de perfil do usuário e permitir o detalhamento completo da sessão do usuário para investigações forenses.

2.6.9.7 A solução deverá incluir um provedor de identidade (IDP) integrado, capaz de autenticar usuários por meio de Single Sign-On (SSO) e autenticação multifator (MFA) com adaptação ao risco. O mecanismo de autenticação deverá suportar critérios de risco como localização, tipo de dispositivo, horário de acesso e comportamento do usuário, possibilitando decisões dinâmicas de autenticação.

2.6.9.8 A solução deverá suportar autenticação federada com diretórios corporativos por meio de protocolos como SAML 2.0, RADIUS ou LDAP seguro, permitindo autenticação única (SSO) integrada ao login da rede. A autenticação transparente via navegador, como o uso de login já autenticado no domínio, será considerada diferencial técnico.

2.6.9.9 A solução deverá incorporar recursos de análise comportamental para usuários privilegiados, utilizando algoritmos de avaliação de risco com base em padrões históricos de uso. A solução deverá ser capaz de detectar desvios e anomalias, atribuir pontuação de risco e permitir que esses dados apoiem decisões de segurança, como aprovação condicional de acessos ou bloqueio preventivo.

Algoritmos mais avançados, como os baseados em horário, comandos ou padrões de autenticação, serão considerados diferenciais técnicos.

2.6.9.10 A solução deve ser composta por appliances virtuais.

2.6.9.11 Deve ser possível realizar o particionamento da solução. As partições permitem que seja configurado vários gerenciadores de ativos independentes, cada um com a capacidade de definir diretrizes de senha para os sistemas gerenciados em seu próprio espaço de trabalho. Por exemplos ativos por localização geográfica, proprietário, função ou sistema operacional.

2.6.9.12 Deve ser possível gerenciar senhas e chaves SSH para contas em plataformas não suportadas através de customizações.

2.6.9.13 Deve possuir suporte aos virtualizadores:

- Microsoft Hyper-V (VHDX) versão 8 ou superior
- VMware vSphere com vSphere Hypervisor (ESXi) versões 6.5 ou superior
- VMware Workstation versão 13 ou superior

2.6.9.14 Deve possuir suporte à implantação em nuvens públicas AWS, Azure e OCI (Oracle Cloud Infraestrutura);

2.6.9.15 Deve possuir suporte aos navegadores:

- Apple Safari 13.1 para desktop (ou posterior)
- Google Chrome 80 (ou posterior)
- Microsoft Edge 80 (ou posterior)
- Mozilla Firefox 69 (ou posterior)

2.6.9.16 Navegadores de dispositivos móveis:

- Browser do Apple iOS 13 (ou posterior)
- Google Chrome no Android versão 80 (ou posterior)

2.6.10 Disponibilidade e Recuperação

2.6.10.1 A solução deverá ser agrupada em cluster e/ou HA (High Availability) para garantir alta disponibilidade.

2.6.10.2 O cluster deverá permitir a recuperação ou continuação de infraestruturas e sistemas tecnológicos vitais após um desastre natural ou induzido pelo homem.

2.6.10.3 O Administrador do Appliance poderá definir redes gerenciadas (segmentos de rede) para gerenciar efetivamente ativos, contas e solicitações de acesso a serviços em um ambiente em cluster para distribuir a carga de tarefas.

2.6.10.4 O dispositivo só pode pertencer a um único cluster, sendo que todos os dados vitais armazenados no dispositivo primário também são armazenados nas réplicas. No caso de um desastre, em que o dispositivo primário não esteja mais funcionando poderá ser promovido uma réplica para ser o novo dispositivo primário.

2.6.10.5 Na réplica poderá ser possível executar operações de verificação e alteração de senhas e chaves SSH, definir senha e definir chave SSH (importadas e geradas). Os usuários podem fazer login nas réplicas para solicitar acesso, gerar relatórios ou auditar os dados. Além disso, senhas, chaves SSH e sessões podem ser solicitadas de qualquer dispositivo em um cluster.

2.6.10.6 O módulo de gravação de sessões deverão possuir também alta disponibilidade (HA), com ao menos duas unidades com configurações idênticas estão operando simultaneamente. O nó primário deve compartilhar todos os dados com o nó secundário e, se o nó primário parar de funcionar, o outro se tornará imediatamente ativo, de modo que os servidores estejam continuamente acessíveis.

2.6.11 Capacidade e Desempenho

2.6.11.1 A solução deverá ser dimensionada e precificada para atender aos requisitos especificados com margem adequada, o crescimento adicional pode exigir recursos adicionais, o que não poderá acarretar custos adicionais.

2.6.11.2 O cluster deverá garantir a distribuição de carga, garantindo que os dispositivos mais próximos do ativo de destino sejam usados para executar a tarefa.

2.6.12 Patches e lançamentos

2.6.12.1 Todas as atualizações de produtos, patches e lançamentos de hot-fix deverão estar publicadas no portal de suporte do fabricante e deve possuir a opção para que sejam enviados por e-mail após registro.

2.6.12.2 As atualizações devem seguir os padrões abaixo:

- Liberação Principal: A cada 1-2 anos
- Liberação Menor: A cada 6-12 meses
- Service Packs por ano (mínimo)

2.6.12.3 A solução deve ser continuamente monitorada, vulnerabilidades e CVEs que podem afetar os componentes da solução e publicar atualizações de segurança e anúncios conforme necessários.

2.6.12.4 A solução deve fornecer ferramentas de autoajuda para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano.

2.6.12.4.1 O Portal de Suporte do fabricante deve permitir:

- Enviar e gerenciar uma solicitação de serviço
- Ver artigos da Base de Conhecimento
- Inscreva-se para notificações de produtos

- Baixar o software e a documentação técnica
- Vídeos de instruções
- Envolver-se em discussões da comunidade
- Canal com comunicação direta com engenheiros de suporte online
- Solicitações de aprimoramento do produto, poderá ser realizada através de solicitação de serviço e submetida ao sistema de revisão de melhorias e um número de identificação será fornecido. A solicitação de serviço deverá permanecer aberta até que seja tomada uma decisão sobre a solicitação.

2.6.13 Prestação de Serviços e Governança

2.6.13.1 A proponente deverá designar um responsável técnico e comercial para gerenciar todos os assuntos de contratos e serviços.

2.6.13.2 O fabricante deverá disponibilizar o suporte 24x7x365.

2.6.13.3 Deve ser fornecida contas individuais para abrir Solicitações de Serviço diretamente no fabricante.

2.6.13.4 Os chamados poderão são relatados por meio de qualquer combinação dos três métodos a seguir: telefone, e-mail e bate-papo online.

2.6.13.5 O cliente indica o nível de prioridade ao enviar a Solicitação de Serviço.

2.6.13.6 A qualquer momento, o cliente pode escalar um problema se sentir que não está sendo resolvido em tempo hábil.

2.6.13.7 Todos os casos registrados devem receber um nível de gravidade de 1 a 4 com base no impacto nos negócios.

2.6.13.8 Os níveis de gravidade podem ser alterados após o contato inicial e a avaliação do problema por um engenheiro de suporte de identidade única, desde que o cliente esteja de acordo.

- Nível de gravidade 1 - Resposta inicial: dentro de 1 hora

- Nível de gravidade 2 - resposta inicial: dentro de 2 horas

- Nível de gravidade 3 - resposta inicial: dentro de 4 horas

- Nível de gravidade 4 - resposta inicial: dentro de 1 dia útil

2.6.14 Relatórios

2.6.14.1 A solução deve disponibilizar de relatórios programados sobre a atividade dos administradores, suas informações de sistema, bem como o tráfego processado.

2.6.14.2 Criar relatórios personalizados de estatísticas de conexão.

2.6.14.3 O modulo de gerenciamento de senhas deve permitir agendamento, personalização, visualização e exportação de relatórios de direitos, propriedade e ações do usuário.

2.6.14.4 O modulo de gerenciamento de sessões deve permitir criar relatórios programados sobre a atividade dos administradores, suas informações de sistema, bem como o tráfego processado. Além disso, você pode usar o banco de dados de conexão para criar relatórios personalizados de estatísticas de conexão.

2.6.14.5 Todos os relatórios podem ser executados ad hoc."

2.6.14.6 Todos os relatórios, incluindo relatórios personalizados, podem ser acessados sob demanda e de forma programada.

2.6.14.7 Os relatórios operacionais devem estar disponíveis em Adobe Portable Document Format (PDF), contendo ao menos as seguintes informações:

- Alterações de configuração: Lista o número de alterações de configuração do modulo de gravação de sessão por página e por usuário.

A frequência das alterações de configuração deve exibida em gráfico.

- Relatórios principais: contém estatísticas sobre o tráfego total que passou no modulo de gravação de sessão, incluindo o número de sessões que passaram para cada política de conexão, os nomes de usuário usados, clientes e servidores.

- Relatórios por conexão: contém estatísticas separadas sobre cada política de conexão configurada no modulo de gravação de sessão.

- Informações de integridade do sistema: Exibe informações sobre o sistema de arquivos e o uso da rede do modulo de gravação de sessão, bem como a carga média.

- Deve ser possível customizar o relatório com o logotipo da organização na capa do relatório, através de seleção de arquivo de logotipo no formato de imagem.

2.6.15 Backup e Restauração

2.6.15.1 A solução deve dispor de mecanismo para realização de backups em um servidor de arquivamento externo ao dispositivo, para que a imagem de backup esteja disponível para restauração mesmo se houver uma falha catastrófica de disco ou hardware.

2.6.15.2 Deve ser possível definir o número máximo de arquivos de backup retidos no appliance.

2.6.15.3 Os dados de backup devem possibilitar configuração de chave pública do cluster ou a criptografia de senha. Qualquer um deles deverá proteger todos os backups subsequentes gerados de cada dispositivo no cluster.

2.6.15.4 A solução de gerenciamento de acessos privilegiados deverá possuir mecanismos robustos de backup e restauração que garantam a continuidade operacional, a segurança dos dados e a integridade das informações armazenadas.

2.6.15.5 Os requisitos mínimos de backup e restauração da solução deverão contemplar todos os dados críticos da solução, incluindo:

- Configurações operacionais e de segurança (workflows, regras de senha, direitos, certificados, fuso horário, status de serviços);

- Dados de identidade e controle de acesso (contas, usuários, grupos, diretórios e tags);

- Recursos gerenciados (ativos, servidores de arquivos, plataformas personalizadas, partições);

- Logs de auditoria, histórico de transações e configuração de ingressos;

- Informações de licenciamento.

2.6.15.6 A solução deverá criptografar e assinar os dados antes de disponibilizá-los para exportação. A descriptografia deverá ser possível apenas em um dispositivo genuíno da mesma fabricante, assegurando a verificação da assinatura e a autenticidade do backup.

2.6.15.7 Deverá ser possível configurar políticas de backup para armazenamentos externos utilizando protocolos NFS, SMB ou CIFS, tanto para dados operacionais quanto exclusivamente para arquivos de sistema (configurações).

2.6.15.8 Após o arquivamento dos dados do módulo de gravação de sessões, a solução deverá permitir sua transferência para repositórios externos, com a opção de exclusão automatizada dos arquivos antigos.

2.6.15.9 Deve ser possível configurar políticas de limpeza com agendamento recorrente, visando a otimização do armazenamento.

2.6.15.10 A CONTRATADA deverá fornecer documentação completa sobre os procedimentos de backup e restauração de todos os módulos da solução, incluindo opções de restauração parcial (somente configuração) e total (configuração e dados).

2.6.15.11 A solução deve suportar linguagem em português.

2.6.16 Criptografia de dados

2.6.16.1 A solução de gravação de sessões deve tornar todas as atividades do usuário rastreáveis, registrando-as em trilhas de auditoria de alta qualidade, invioláveis e facilmente pesquisáveis. Todos os dados devem ser armazenados em arquivos criptografados, com carimbo de data/hora e assinados, evitando qualquer modificação ou manipulação.

2.6.16.2 As trilhas de auditoria de filmagem devem conter estar acessíveis para análises ad hoc ou relatórios de auditoria.

2.6.16.3 Deve ser utilizada criptografia validada FIPS 140-2 para em todas as criptografias de dados.

2.6.17 Gerenciamento de acesso

2.6.17.1 A solução deve possuir controle de acesso baseado em função, utilizando conjuntos de permissões de administrador, permitindo delegação granular e fluxos de trabalho juntamente com acesso menos privilegiado.

2.6.17.2 Deve suportar modelo RBAC de separação de tarefas por meio de direitos, sendo que um direito é um conjunto de políticas de solicitação de acesso que restringem o acesso do sistema a usuários autorizados. Portanto, deve garantir:

2.6.17.3 Os direitos de liberação consistem em usuários, grupos de usuários e políticas de solicitação de acesso.

2.6.17.4 Os direitos de solicitação de sessão consistem em usuários, grupos de usuários, ativos, grupos de ativos e políticas de solicitação de acesso.

2.6.17.5 As políticas de solicitação de acesso fornecem um mecanismo de fluxo de trabalho que oferece suporte a restrições de tempo, vários aprovadores, revisores, acesso de emergência e expiração da política.

2.6.17.6 A solução deverá implementar mecanismo de controle de acesso baseado em função (RBAC – Role-Based Access Control), com hierarquia de permissões que permita restringir e delegar responsabilidades conforme o perfil de cada usuário, garantindo o controle seguro dos ativos gerenciados pelo departamento de TI.

2.6.17.7 Deverão ser contempladas, no mínimo, as seguintes categorias de permissões administrativas:

- Administração de dispositivos;
- Administração de ativos;
- Auditoria e visualização de registros;
- Administração de aprovações (autorizador);
- Administração de suporte técnico (HelpDesk);
- Administração de operações e tarefas automatizadas;
- Administração de políticas de segurança;
- Administração de identidades e usuários.

2.6.17.8 A solução deverá permitir a atribuição granular dessas permissões, de forma centralizada e auditável.

2.6.17.9 As diretivas da solução, devem garantir a concessão dos acessos aos usuários, grupos de usuários ou ambos. Um direito inclui uma ou mais políticas de solicitação de acesso e pode estar relacionado a funções de trabalho, como suporte de suporte técnico ou administradores de Unix. Esses grupos de usuários podem ser mapeados para a delegação de função de suporte do AD por meio da associação ao grupo.

2.6.18 Registro, monitoramento e alerta de eventos de segurança

2.6.18.1 A solução deve registrar todas as atividades no log de auditoria de atividades, possuindo um local para visualizar os detalhes de eventos específicos ou atividades do usuário.

2.6.18.2 A solução deve possuir critérios de pesquisa para recuperar informações específicas do log de auditoria de atividades. Os critérios de pesquisa disponíveis incluem:

- Categoria de atividade;
- Prazo;
- Usuário;
- Ativo;
- Conta;
- Pesquisar palavra-chave ou valor.

2.6.18.3 A solução poderá registrar informações relacionadas à conexão localmente e para vários destinos de syslog remotos, enquanto as trilhas de auditoria são armazenadas localmente no dispositivo. As políticas de backup/arquivamento/limpeza podem ser configuradas e aplicadas a trilhas de auditoria com base na política de conexão.

2.6.18.4 Logs de segurança, trilhas de auditoria, logs de auditoria, gravações de sessões indexadas e relatórios devem ser armazenados nos dispositivos de forma segura e não podem ser adulterados por usuários privilegiados, cujas atividades de sessão estão sendo monitoradas. Os tempos de retenção podem ser definidos pelo administrador da solução.

2.6.19 Auditabilidade do sistema

2.6.19.1 Toda a atividade da sessão - até o pressionamento de tecla, movimento do mouse e janelas visualizadas – deve ser capturada, indexada e armazenada em trilhas de auditoria compactadas e invioláveis que podem ser visualizadas como um vídeo e pesquisadas como um banco de dados. As equipes de segurança devem poder pesquisar eventos específicos nas sessões e reproduzir a gravação a partir do local exato em que os critérios de pesquisa ocorreram.

2.6.19.2 Alertas em tempo real podem ser gerados para tipos ou classes de eventos definidos por meio de políticas.

2.6.19.3 As trilhas de auditoria devem ser criptografadas, com carimbo de data/hora e assinadas por criptografia para fins de análise forense e de conformidade.

2.6.20 Descoberta de ativos, contas e serviços gerenciáveis pela solução

2.6.20.1 A solução deve contar com serviço de descoberta, onde podem localizar ativos, contas, chaves SSH e serviços no ambiente de rede para simplificar a implantação inicial e a manutenção contínua das contas privilegiadas no ambiente de rede.

2.6.20.2 Deve ser possível encontrar ativos por descoberta em diretório associados ao Active Directory, Azure Active Directory, Intervalos de IP de rede e máquinas virtuais em Hyper-V.

2.6.20.3 As descobertas podem ser agendadas para execução em intervalos regulares. O trabalho de descoberta pode ser configurado com modelos para definir configurações padrão em ativos recém-criados, incluindo detalhes de conexão. Um ativo com informações de conexão válidas pode ser usado para descoberta de conta.

2.6.20.4 Os ativos de diretório poderão ser descobertos em qualquer partição.

2.6.20.5 Deve ser possível fazer rastreio de contas pesquisando ativos de diretório, como o Active Directory, ou verificando bancos de

dados de contas locais em ativos Windows e Unix (/etc/passwd)

2.6.20.6 Deve ser possível fazer descoberta de contas de serviço.

2.6.20.7 A solução poderá atualizar a configuração do serviço do Windows para corresponder à senha quando a senha for alterada e reiniciar o serviço automaticamente.

2.6.20.8 Deve ser possível fazer descoberta de chaves SSH por pesquisas em diretórios de usuários.

2.6.20.9 A solução deve possuir plataforma de hospedagem de código-fonte e arquivos com controle de versão para desenvolvimento de novas integrações de descoberta, como operações de descoberta de contas e integração em AWS, Azure, ESX, HP ILO, Hyper-v, ServiceNow e bancos de dados.

2.6.21 Rotação e verificação de senha

2.6.21.1 A solução deve oferecer suporte à verificação e sincronização de senhas, de forma manual ou automática. Um painel operacional deve mostrar quais senhas falharam no teste.

2.6.21.2 A solução deve oferecer suporte a regras de senha de conta, que são regras de complexidade que regem a construção de uma nova senha criada ou durante uma alteração. Os requisitos de complexidade de senha podem ser configurados para cumprir a política da empresa. Os requisitos para configurar devem seguir pelo menos os seguintes parâmetros:

- Comprimento da senha
- Digitar o primeiro de caractere
- Digitar o Último de caractere
- Permitindo caracteres repetidos consecutivamente
- Permitindo letras maiúsculas
- Número mínimo de caracteres maiúsculos obrigatórios
- Permitindo letras minúsculas
- Número mínimo de caracteres minúsculos obrigatórios
- Permitindo numérico (0-9)
- Número mínimo de números obrigatórios
- Permitindo símbolos (por exemplo, !@#\$%^)
- Número mínimo de símbolos obrigatórios
- Símbolos válidos

- Deve ser possível configurar para não alternar senhas para contas específicas em ativos específicos.

- Deve ser possível alternar as senhas no check-in ou automaticamente de forma programada. As políticas e fluxos de trabalho podem ser configurados por conta para alterar as senhas em intervalos de tempo específicos (por exemplo, a cada 30 dias) para alinhar com a política existente.

- Pode ser configurado para alterar senhas após o último uso, garantindo total responsabilidade e fornecendo efetivamente senhas de contas compartilhadas de uso único.

2.6.22 Inscrição (Enrollment)

2.6.22.1 A solução deve possuir um conjunto de políticas de solicitação que restringem o acesso do sistema a usuários autorizados.

Deve poder criar direitos para várias funções de trabalho; ou seja, atribuir permissões para executar determinadas operações a funções específicas, como Administrador de Help Desk, Administrador Unix ou Administrador Oracle.

2.6.22.2 Os direitos de liberação de senha e chave SSH devem consistir em usuários, grupos de usuários e políticas de solicitação de acesso. Os direitos de solicitação de acesso à sessão consistem em usuários, grupos de usuários, ativos, grupos de ativos e políticas de solicitação de acesso.

2.6.22.3 A solução deve oferecer suporte ao acesso a contas compartilhadas para vários usuários privilegiados. Como um usuário privilegiado está solicitando o uso de uma conta compartilhada em um ponto final para uma data e hora específicas, deve poder vincular o uso dessa conta compartilhada a esse usuário privilegiado, para o ponto final para fins de relatório/auditoria.

2.6.22.4 O acesso a qualquer aplicativo deve ser controlado a nível de rede, protocolo e sessão, podendo definir quais usuários podem acessar credenciais seguras para estabelecer uma sessão privilegiada.

2.6.22.5 Os usuários privilegiados podem ser importados em massa de um arquivo de banco de dados no formato .csv.

2.6.22.6 Não deve exigir a instalação de software cliente ou componentes de software servidor e, portanto, não há restrições ou dependências de plataforma.

2.6.22.7 O acesso privilegiado deve ser gerenciado no nível da sessão e do protocolo. As sessões que usam os seguintes protocolos devem ser suportadas:

- Secure Shell (SSH, incluindo tráfego X11 encaminhado),
- Secure Copy (SCP),
- SSH File Transfer Protocol (SFTP),
- Remote Desktop (RDP),
- HTTP,
- Independent Computing Architecture (Citrix ICA),
- Telnet,
- VMware Horizon View,
- Conexões MSSQL,
- Conexões VNC.

2.6.22.8 Deve ser disponibilizada suporte a API baseada em uma arquitetura REST, que permite que outros aplicativos e sistemas se conectem e interajam.

2.6.22.9 Interfaces gráficas WEB que permitem gerenciar solicitações de acesso, aprovações e revisões para suas contas e sistemas gerenciados.

2.6.22.10 Fornecer console de gerenciamento Web para a configuração inicial.

2.6.22.11 Controlar exibição do fundo de tela no uso de RDP a partir de uma solicitação de sessão iniciada pela solução.

2.6.23 Solicitação e Aprovação de Acesso Privilegiado

2.6.23.1 Fornecer mecanismo de fluxo de trabalho que suporte as restrições de tempo, vários aprovadores, revisores, acesso de

emergência e expiração de política.

2.6.23.2 Deve possuir a capacidade de inserir números de chamados e integrar diretamente com sistemas ITSM.

2.6.23.3 O portal inicial deve fornecer uma visualização rápida das tarefas de solicitação de acesso que precisam de atenção imediata.

2.6.23.4 O perfil de Administrador pode configurar alertas para serem enviados aos usuários quando houver tarefas pendentes que precisem de atenção.

2.6.23.5 O perfil de solicitantes deve visualizar tarefas relacionadas ao envio de novas solicitações de acesso, bem como as ações a serem executadas após a aprovação de uma solicitação (por exemplo, visualizar senhas, copiar senhas, iniciar sessões e verificar solicitações concluídas).

2.6.23.6 Os solicitantes podem definir solicitações favoritas, que aparecem em sua página inicial para uso posterior. Isso pode ser feito a partir do cliente de desktop ou do cliente da web. Pelo menos três fluxos de trabalho devem estar disponíveis:

- Fluxo de trabalho de solicitação de liberação de senha;
- Fluxo de trabalho de solicitação de liberação de chave SSH;
- Fluxo de trabalho de solicitação de sessão;

2.6.23.7 Capacidade de acionar um fluxo de trabalho de aprovação usando recursos de aprovação de fluxo de trabalho nativos.

2.6.23.8 Quando uma Conta Privilegiada da Solução é retirada, a Conta Privilegiada deve ser rastreável até durante o check-out.

2.6.23.9 As restrições de acesso condicional podem ser configuradas ao fazer check-out de uma conta privilegiada. Exemplos: hora do dia, endereço IP.

2.6.23.10 O administrador da solução deve ter a opção de encerrar sessões inativas.

2.6.24 Validação de acesso

2.6.24.1 Ao se comunicar com o Windows Active Directory, a solução de gerenciamento de senhas deverá utilizar autenticação segura, como Kerberos com GSSAPI (via SASL), e assegurar a criptografia da sessão (seja por meio de StartTLS na porta 389 ou utilizando LDAPS na porta 636) garantindo a proteção da chave de sessão negociada.

2.6.24.2 Ao interagir com contas locais do Windows em servidores autônomos e membros, a solução deverá usar a comunicação NTLM(SSP) pela porta 445.

2.6.24.3 A solução deverá ser prover com os mecanismos de autenticação nativa com os recursos de autenticação de multi-fator (MFA) e Acesso unificado (SSO):

- OTP Mobile App (Android, Android Wear, Apple iOS, and Apple watchOS)
- Verify Push
- SMS Text
- Voice MFA

2.6.25 Revogação de Acesso Privilegiado

2.6.25.1 A solução deve prover mecanismo de automação para permitir JIT (just-in-time), sem privilégios permanentes, pois as credenciais do usuário podem ser provisionadas por JIT para uma tarefa específica e, em seguida, desprovisionadas imediatamente após a conclusão da tarefa. Como o acesso do usuário a contas privilegiadas é baseado no status e nas credenciais atuais do usuário em seu banco de dados de autenticação de usuário, um usuário removido não poderá mais estabelecer uma sessão em nenhum ativo ou conta privilegiada.

2.6.25.2 O Mecanismo de JIT, deve fornecer as condições para ingresso e remoção automática de grupos de acesso no Active Directory durante o check-in e check-out da conta e suspender a mesma após a utilização.

2.6.26 Gerenciamento de acesso privilegiado para contas de aplicativos

2.6.26.1 Aplicativos e scripts podem ser configurados para extrair credenciais da solução usando o serviço Application to Application (A2A). Espera-se que este serviço possa ser utilizado a partir de commandlets do PowerShell, bash-shell ou por meio de chamadas de API REST padrão.

2.6.26.2 Aplicativos que utilizam credenciais incorporadas e possui uma API que pode ser aproveitada, a solução ofertada poderá aproveitar seu serviço de agente DevOps para realizar essa tarefa.

2.6.27 Gravação e Notificações de Sessão

2.6.27.1 Uma sessão privilegiada pode ser aberta por meio de uma solicitação de fluxo de trabalho e, em seguida, controlada e monitorada usando serviço embarcada na solução.

2.6.27.2 A solução deve monitorar, controlar, registrar e fornecer análises para sessões feitas por usuários privilegiados a ativos críticos. Não deverá possuir agente instalado no do cliente (estações de trabalho do usuário final) ou nos sistemas e servidores de destino.

2.6.27.3 O monitoramento e controle de sessão são configuráveis usando perfis de conexão e políticas.

2.6.27.4 A solução deve inspecionar o tráfego, podendo ser gerenciado de forma granular, quem poderá acessar o quê e quando nos servidores. Por exemplo, permitir ou negar seletivamente o acesso a canais de protocolo: habilitar sessões de terminal em SSH, mas desabilitar o encaminhamento de porta e transferências de arquivos, ou habilitar o acesso à área de trabalho para RDP, mas desabilitar o compartilhamento de arquivos.

2.6.27.5 Deve suportar acesso remoto (shadow) em tempo real, permitindo que um autorizador acompanhe a sessão do administrador em tempo real e encerre sua conexão no caso de detectar uma violação de política.

2.6.27.6 Deve ser possível realizar a autorização adicional mediante o acompanhamento de sessão (shadow), ou seja, somente será liberado a início da sessão de acesso remoto caso o autorizador, previamente configurado, esteja acompanhando a mesma sessão com o requisitante autorizado. Desta forma:

- O autorizador poderá reproduzir o tempo da sessão gravada durante o acompanhamento da sessão.
- O autorizador poderá terminar a sessão caso necessário.

2.6.27.7 Deve ser possível controlar o acesso às conexões por meio de um conjunto de cadência de políticas, onde a primeira política que possuir completamente a solicitação de conexão é aplicada à conexão.

2.6.27.8 Deve ser possível enviar notificação ao usuário que o que a sessão será gravada.

2.6.27.9 Gravações de sessão devem ser indexadas.

2.6.27.10 O conteúdo das trilhas de auditoria deve pesquisado na interface nativa da solução.

2.6.27.11 As gravações da sessão podem ser visualizadas com controles de vídeo completos, incluindo:

- Reproduzir, pausar, retroceder
- Saltar para o evento anterior,
- Saltar para o próximo evento
- Ajuste a velocidade de reprodução
- Tempo desde o início da trilha de auditoria
- Duração da trilha de auditoria.
- Lista de eventos de teclado. Caracteres especiais como ENTER, F1 e assim por diante devem ser exibidos como eventos realizados
- Ativamento de clicks do mouse
- Possuir captura de tela dos eventos.

2.6.27.12 A solução deverá monitorar em tempo real o conteúdo das conexões estabelecidas pelos usuários, com capacidade de identificar padrões de risco e aplicar ações automáticas, como envio de alertas, término da sessão ou bloqueio imediato da conexão, conforme políticas configuráveis.

2.6.27.13 A solução deverá permitir a definição de padrões e políticas de segurança em nível de protocolo e de aplicação, como comandos sensíveis em protocolos baseados em texto ou a execução de aplicações suspeitas em sessões gráficas. Ao detectar comportamentos maliciosos, a solução deverá agir preventivamente para bloquear a atividade em tempo real, e não apenas registrá-la ou alertar.

2.6.28 Uso de inteligência artificial e Algoritmos

2.6.28.1 Deve ser possível analisar o comportamento do usuário com a ajuda de algoritmos, também chamados de analytics.

2.6.28.2 Os algoritmos são métodos matemáticos que podem ser usados para analisar os dados da sessão de vários ângulos. Os algoritmos devem ser treinados usando um histórico de dados de sessão. Com base nesse treinamento, um algoritmo pode criar uma linha de base do comportamento de um determinado usuário e pontuar novas sessões. As pontuações indicarão se o comportamento de um determinado usuário é normal ou incomum, em comparação com a linha de base.

2.6.28.3 Os algoritmos devem fornecer visualização para exibir informações sobre o comportamento do usuário.

2.6.28.4 Minimamente, os seguintes algoritmos devem ser suportados:

2.6.28.5 O algoritmo de pressionamento de tecla. Capaz de dizer se um usuário é realmente quem diz ser com base em sua dinâmica de digitação. O algoritmo de pressionamento de tecla deve analisar os dados do teclado provenientes de sessões RDP ou SSH e os compara com o perfil do usuário.

2.6.28.6 Deve analisar perfil de comandos para o usuário com base nos comandos que ele costuma executar. O algoritmo de comando determina a probabilidade de ocorrência de determinados comandos dentro de uma sessão.

2.6.28.7 Deve possuir algoritmo de hora de login, criando um perfil com base na hora exata do dia em que um usuário faz login. Com base no perfil do usuário, ele pode dizer o quão incomum é a hora de login, dada a distribuição diária dos eventos de login do usuário no passado.

2.6.28.8 Analisar a semelhança entre dois hosts com base nos usuários que efetuam login. Quando um usuário faz login em um host no qual nunca ou raramente faz login, isso não será considerado uma anomalia se esse host for semelhante a outros hosts que o usuário usa com frequência.

2.6.28.9 Utilizar algoritmo de conjunto de itens frequentes (FIS), para examinar vários atributos de sessões e encontrar valores que frequentemente aparecem juntos. Usando essas informações, o algoritmo FIS é capaz de descobrir padrões no comportamento do usuário, como "essa pessoa só usa RDP no meio da noite a partir deste endereço IP".

2.6.28.10 Suportar análise dos títulos das janelas para descobrir o comportamento incomum do usuário, ou seja, identificar os usuários com base nos títulos das janelas que eles geralmente têm na tela e utiliza.

2.6.28.11 Suportar algoritmo de autenticação do usuário para analisar o movimento do mouse e a autenticidade do usuário com base nos históricos de movimentos.

2.6.28.12 Realizar a detecção de sessão com script, determinando se as atividades em uma sessão apontam para ser uma sessão através script. Os seguintes algoritmos internos em segundo plano devem determinar se uma sessão está programada em:

2.6.28.13 Possuir algoritmo “clockmaster” capaz de detectar sessões anormalmente precisas que começam repetidamente em determinados minutos de pico de uma hora. O algoritmo sinaliza como sessões com script. A razão por trás disso é que os minutos nos registros de data e hora das atividades humanas em um período mais longo supostamente têm distribuição aleatória uniforme ou estão muito próximos disso.

2.6.28.14 Possuir algoritmo tipo “gapminder” capaz de detectar sessões com script com base nos intervalos de tempo entre as sessões que pertencem a uma determinada conta. Quando os intervalos de tempo entre as sessões têm valores típicos e repetidos, isso sugere um comportamento periódico não natural. Se houver quatro sessões consecutivas com intervalos de tempo iguais entre elas e forem seguidas por uma quinta sessão com o mesmo intervalo de tempo, o algoritmo sinalizará a quinta sessão como uma sessão com script.

2.6.28.15 Analisar em relação ao tamanho dos intervalos de tempo e quão grande um intervalo se qualifica como um intervalo de tempo que vale a pena monitorar, o algoritmo considera o tempo decorrido entre duas sessões como um intervalo de tempo se a duração do intervalo for igual ou superior a 10 minutos e igual a ou menos de dois dias.

2.6.28.16 A solução deve executar automaticamente avaliação de algoritmo todos os dias para avaliar quão bem esses algoritmos de análise estão funcionando no conjunto de dados atual residente na implantação.

2.6.28.17 Deve ser possível a reindexação das sessões históricas de forma manual.

2.6.28.18 A solução deve bloquear logins paralelos na UI da web para o mesmo usuário. Caso o usuário fizer login em um navegador ou computador diferente, o SPS invalidará imediatamente a sessão anterior.

2.6.29 Proteção e Integração com Aplicações e Pipelines DevOps

2.6.29.1 A solução deverá incluir funcionalidade de gerenciamento seguro de secrets, com suporte a APIs e SDKs para integração com pipelines de desenvolvimento e ferramentas de automação. Deverá ser possível recuperar credenciais de forma segura para uso por aplicações ou scripts, com suporte a autenticação robusta, criptografia, versionamento e controle de acesso baseado em função. Funcionalidades como sincronização bidirecional com outros cofres, múltiplas instâncias de plugins e fluxo reverso de secrets serão consideradas diferenciais técnicos.

2.6.29.2 Exigir certificado SSL tanto para comunicação com o Secrets Broker para DevOps.

2.6.29.3 Os certificados com suas chaves privadas correspondentes podem ser gerados externamente e carregados no formato PFX ou

o Broker poderá gerar uma chave privada e CSR que pode ser assinado e carregado.

2.6.29.4 Visando a facilidade de integração com aplicações existentes ou com práticas de desenvolvimento vigentes, a solução deve fornecer bibliotecas de integração em linguagens variadas, incluindo minimamente .NET e Java, Python e JavaScript.

2.6.30 Segurança de Cofres em Ambientes Segregados (DMZ)

2.6.30.1 O arquivo do backup deve ter a opção de ser criptografado com uma senha para recuperação.

2.6.30.2 A solução deve permitir que um ambiente segregado seja configurado, ou seja, incluir uma instância autônoma do Cofre de Senha colocada em uma rede desmilitarizada (DMZ), onde poderá conter apenas algumas contas e credenciais específicas. Todas essas contas ainda são gerenciadas e alternadas pelo cluster do Cofre de Senhas corporativo.

2.6.30.3 O cluster do cofre de senha corporativo deve gerenciar todas as contas do ambiente desmilitarizado, registrar e fazer a rotação das credenciais conforme necessário.

2.6.30.4 O Cofre de Senhas corporativo deve controlar todas as credenciais quanto à liberação por meio de políticas e em conformidade com um fluxo de trabalho de auditoria.

2.6.31 Certificação Profissional da Equipe de Serviços PAM

2.6.31.1 A CONTRATADA deverá apresentar, no momento da contratação ou habilitação, declaração emitida pelo fabricante da solução de Gerenciamento de Acessos Privilegiados (PAM), atestando que:

- A empresa contratada está registrada como revendedora ou parceira autorizada do fabricante, com autorização expressa para comercializar, implementar e prestar suporte técnico para os produtos ofertados;

- Possui profissionais certificados ou treinados diretamente pelo fabricante, aptos a configurar, implementar e suportar tecnicamente a solução proposta.

2.6.31.2 A declaração deverá ser emitida por representante legal ou autoridade competente, contendo ao menos: razão social da contratada, nome dos profissionais autorizados e a identificação clara dos produtos abrangidos.

2.6.31.3 A CONTRATADA deverá promover a atualização contínua das habilidades da equipe de serviços PAM, oferecendo treinamentos e reciclagens para acompanhar as evoluções tecnológicas e manter a eficácia e segurança na gestão de acessos privilegiados.

2.6.32 Serviços de Instalação

2.6.32.1 A instalação da solução será conduzida em formato de projeto seguindo as melhores práticas estabelecidas pelo PMI através do guia PMBOK.

2.6.32.2 A CONTRATADA será responsável pela elaboração de um Projeto de Instalação, que deverá, no mínimo, consistir em uma análise preliminar de escopo após o alinhamento das expectativas das equipes envolvidas, determinação dos recursos necessários, estrutura analítica, cronograma, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e detalhamento técnico da solução, inclusive com entendimento do ambiente atualmente em produção;

2.6.32.3 O responsável designado pela CONTRATADA terá como responsabilidade gerenciar a execução do Projeto de Instalação, monitorar e controlar as atividades (prazo e escopo), reportar (documentando) o andamento do projeto a cada três dias e é responsável pela comunicação entre as partes interessadas;

2.6.32.4 A CONTRATADA deverá apresentar também um Plano de Treinamento, que será parte integrante do Projeto de Instalação;

2.6.32.4.1 O Projeto de Instalação deverá conter um cronograma com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes;

2.6.32.4.2 A entrega do Projeto de Instalação deve ocorrer em até cinco dias após o recebimento da ordem de serviço pela Contratada;

2.6.32.4.3 A CONTRATADA deverá entregar o Projeto de Instalação em formato digital e, quando em instalação presencial, em formato impresso para a Contratante;

2.6.32.5 Compreende-se nesta etapa a instalação das soluções a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

2.6.32.6 No momento anterior da assinatura do termo de recebimento provisório, a CONTRATADA será requisitada para reunião de kickoff do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

2.6.32.7 Durante esta etapa, a equipe da CONTRATADA deverá estar disponível nos horários de instalação definidos pela equipe da CONTRATANTE.

2.6.32.8 As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial.

2.6.32.9 Para esta etapa a CONTRATANTE disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

2.6.32.10 A montagem e instalação de todos os componentes que componham solução adquirida são de responsabilidade da CONTRATADA.

2.6.32.11 Os componentes de software deverão estar na versão mais atualizada da solução.

2.6.32.12 A CONTRATADA deverá listar à CONTRATANTE todas as informações necessárias para a correta instalação e configuração da solução.

2.6.32.13 A CONTRATANTE deverá providenciar as informações necessárias para a correta instalação da solução.

2.6.32.14 A CONTRATADA deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

2.6.32.15 A CONTRATANTE acompanhará e contabilizará a utilização de dias/horas.

2.6.32.16 A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

2.6.32.16.1 Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

2.6.32.16.2 Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

2.6.32.17 No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo.

2.7 CONSULTORIA EM SERVIÇOS ESPECIALIZADOS (On demand)

2.7.1 O serviço de horas de Consultoria será executado on demand até o limite de 2000 (duas mil) Horas de Serviço Técnico (HST), dentro do período de vigência contratado e, tem o objetivo de atender a eventuais melhorias nas soluções que compõe este Termo de Referência.

2.7.1.1 Hora de Serviço Técnico (HST): métrica baseada na quantidade de horas necessárias para se alcançar um resultado ou entregar um produto, por meio de atividades executadas por um ou mais perfis profissionais, e aferidas por meio de indicadores de níveis mínimos de serviço e critérios de aceitação previamente estabelecidos, nos termos de subitem 2.2.1, letra “h” da Portaria SGD/MGI nº 750, de 20 de março de 2023.

2.7.2 O serviço de Consultoria deverá ser prestado por meio de emissão de uma ordem de serviço.

2.7.3 A contratante emitirá uma nota contendo os serviços que deseja incluir nesse pacote, na qual contempla o parque tecnológico especificado neste documento.

2.7.4 A CONTRADA deverá possuir capacidade técnica plena para executar esse tipo de serviço exigido.

2.7.5 O serviço poderá ser prestado de modo remoto, cabendo a CONTRATANTE fornecer todos os acessos necessários para a execução do serviço.

2.7.6 O total de horas de Consultoria especificado é estimativo, sendo somente efetuados pagamentos contra as horas efetivamente utilizadas.

2.7.7 As horas utilizadas serão abatidas do total previsto neste documento, podendo as horas restantes serem utilizadas dentro do prazo contratado.

2.7.8 As horas começaram a ser contabilizadas quando a equipe da CONTRATADA estiver recebido o aceite da CONTRATANTE para acessar o ambiente/devices.

2.7.9 A utilização das horas deverá ser formalizada pela SEFAZ/AC através de e-mail ou em formato a ser acordado.

2.7.10 As seguintes atividades poderão ser solicitadas para a CONTRATADA, como serviço de consultoria especializado:

- Manutenção evolutiva e integração de soluções segurança;
- Apoio nas definições do produto para composição de soluções;
- Suporte no desenvolvimento de novas soluções que utilizem o produto;
- Avaliações, diagnósticos e proposições de soluções de melhoria;
- Geração de relatórios e análise das soluções;
- Implementações adicionais;
- Alterações da configuração nos equipamentos não previstas na manutenção e suporte técnico;
- Apoio à arquitetura de segurança, com sugestões de melhorias e boas práticas;
- Apoio na definição de requisitos e configuração de novas funcionalidades.
- Revisão e ajustes de configuração em soluções existentes;
- Proposição de ações corretivas ou mitigatórias frente a incidentes de segurança para as soluções existentes;
- Apoio em planos de resposta a incidentes, backups e recuperação;
- Atualização de versões de softwares e firmwares, desde que tenha contrato ativo de garantia com o fabricante;
- Recomendações para segmentação de rede;
- Avaliação de vulnerabilidades e gaps de configuração.

2.7.10.1 Ao final de cada atendimento por HST, deverá ser preenchido o formulário conforme modelo pactuado entre as partes.

2.7.10.2 O formulário devidamente assinado por representante da CONTRATANTE designado para acompanhar a atividade deverá ser enviado ao final do mês posterior a execução.

2.7.11 O prazo máximo para início deste atendimento será de 3 (três) dias úteis.

2.7.12 O técnico disponibilizado deve ser certificado pelo fabricante na solução fornecida e já ter conhecimento das soluções implantadas no parque tecnológico da Contratada.

2.7.13 A equipe de prestação de serviço da contratada não precisa ser exclusiva, porém é estritamente necessário e rigoroso que cumpra as metas de serviços exigidas pela Contratante

2.7.14 Caso alguma métrica de serviço não seja executada de maneira a contento da CONTRATANTE, a CONTRATADA deverá refazê-lo sem custo adicional a Contratante.

2.7.15 Poderá auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento pelas demais áreas de TI;

2.7.16 Poderá sugerir novas tecnologias e procedimentos de Segurança da Informação;

2.7.17 Executar, com o apoio dos fabricantes, a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a segurança da informação;

2.7.18 *Certificação Profissional da Equipe de Serviços de consultoria especializada*

2.7.18.1 Devido à complexidade das ferramentas que deverão ser suportadas pela CONTRATADA e com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõem o parque de segurança do CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor a equipe com ao menos um profissional que possua a certificação abaixo:

- FCSS - Fortinet Certified Solution Specialist
- Fortinet FCP – Network Security
- Fortinet NSE4 - Network Security Expert Level 4
- CISCO CCNP Security
- CISCO CCIE
- Comptia Security+

2.8 PRESENÇA FÍSICA NO LOCAL

2.8.1 Considerando a criticidade dos serviços a serem contratados — incluindo atividades de monitoramento de segurança cibernética (SOC), resposta a incidentes, gestão de vulnerabilidades, acesso privilegiado, inteligência de ameaças e consultoria técnica —, justifica-se a necessidade de presença física no Estado do Acre, seja por meio de estrutura local de apoio, seja pela alocação presencial de profissional técnico junto à sede da CONTRATANTE, pelos seguintes motivos:

2.8.1.1 Atendimento a incidentes críticos com necessidade de resposta imediata e presencial, como interrupções em serviços essenciais, investigação de eventos complexos e análise de dispositivos físicos ou isolados da rede.

2.8.1.2 Suporte às atividades presenciais de coordenação, validação técnica e integração com equipes locais de segurança da informação e infraestrutura, especialmente em contextos com baixa maturidade tecnológica ou ausência/falha de conectividade redundante.

2.8.1.3 Facilidade na gestão contratual, comunicação com equipes internas e apoio às auditorias, fiscalizações e ações coordenadas com órgãos de controle, que demandam acesso físico e conhecimento da estrutura institucional.

2.8.1.4 Garantia de maior comprometimento da CONTRATADA, com alinhamento contínuo, melhoria na troca de informações e redução de riscos operacionais decorrentes de falhas de comunicação ou ausência de suporte imediato.

2.8.2 A exigência segue precedentes do Tribunal de Contas da União (TCU), como nos Acórdãos nº 1.867/2011, nº 1.554/2016 e nº 3.512/2020, que admitem a presença física desde que tecnicamente justificada e proporcional à complexidade do objeto.

2.8.3 A medida não restringe a participação de empresas de outras regiões, uma vez que a presença local pode ser atendida por filial, representação ou alocação de recurso técnico específico, mantendo-se o equilíbrio competitivo entre fornecedores.

2.8.4 Dessa forma, a presença física no Estado do Acre — ainda que representada por um profissional técnico alocado — é condição relevante para assegurar a continuidade, a eficácia e a segurança na prestação dos serviços contratados.

21.2. Anexo II - Modelo de Termo de Confidencialidade

TERMO DE CONFIDENCIALIDADE

Pelo presente Termo de Confidencialidade, eu _____, CPF nº _____, RG nº _____, expedida pelo (a) _____, representante da empresa _____,

CNPJ nº _____, declaro ter recebido da Secretaria de Estado da Fazenda do Acre - SEFAZ/AC informações confidenciais e reservadas do ambiente tecnológico, incluindo dados quantitativos e qualitativos da estrutura e topologia da rede, de sistemas, de métodos e processos atualmente utilizados, entre outras informações, todas obtidas com a intenção de fundamentar a proposta comercial, que se expostas ao domínio público permitem a ação deletéria de softwares maliciosos e hacker's, razão pelo qual, por meio do presente termo de confidencialidade a empresa signatária, participante da licitação em epígrafe, compromete-se a manter sob sigilo as informações e dados obtidos, e a eliminar todas as informações obtidas caso não seja sagrada vencedora do certame, sob as penas da Lei, comprometo-me a não divulgar as informações a que tive acesso.

Para os fins deste Termo, “informação confidencial” significa todos os esclarecimentos técnicos, minutas de documentos, documentos, dados, estudos, especificações técnicas, inovações ou aperfeiçoamento de que venham a ter acesso, ou que venham a lhes ser confiado em razão deste Termo, incluindo-se previsões, gráficos e todas e quaisquer outras informações, escritas, orais ou visuais, relacionadas com a apuração necessária ao conhecimento do ambiente de TIC e a formulação da proposta comercial da licitante, acerca do objeto da licitação, seja de natureza técnica, operacional, financeira, comercial e/ou legal, que possua valor tangível ou intangível para ao órgão CONTRATANTE, incluindo, mas não se limitando, a existência deste Termo e suas condições, mas excluindo: a) informações que estejam ou venham a estar em domínio do público em geral por outra forma que não seja a violação deste Termo; ou b) informações que a licitante pode comprovar que não foi adquirida,

direta ou indiretamente, em caráter confidencial, neste ato; ou c) informações de propriedade dos órgãos, por eles divulgada, de maneira irrestrita e não confidencial; ou d) informações que tenham sua divulgação exigida por lei, incluindo por qualquer tribunal ou órgão regulatório com competência para tanto

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]
Empresa/CNPJ

21.3. **Anexo III - Modelo de Declaração de Vistoria Técnica**

DECLARAÇÃO DE VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO SRP Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida _____ no(a) _____,

como seu representante legal, para os fins da presente declaração, compareci perante o representante do SEFAZ em Rio Branco/AC e vistoriei o ambiente computacional do mesmo, assim como inteirei-me sobre as condições e grau de dificuldades existentes envolvendo o parque tecnológico da CONTRATANTE e os serviços a serem executados com apoio dos profissionais, tomando plena ciência das condições e grau de dificuldade existentes e das condições para prestação dos serviços, estando satisfeita com as informações e esclarecimentos obtidos durante a visita, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]

Visto:
Representante da SEFAZ-AC

21.4. **Anexo VI - Modelo de Declaração de Renúncia da Vistoria Técnica**

DECLARAÇÃO DE RENÚNCIA DA VISTORIA TÉCNICA

Declaro, em atendimento ao previsto no Edital xx/xxxx e seus anexos do PREGÃO ELETRÔNICO SRP Nº XX/XXXX, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida _____ no(a) _____,

como seu representante legal, para os fins da presente declaração,, optamos pela não realização de vistoria técnica assumindo inteiramente a responsabilidade ou consequências por essa omissão, mantendo as garantias que vincularem nossa proposta ao presente processo licitatório, em nome da empresa que represento, estando plenamente capaz de elaborar proposta para a licitação em tela, de modo a não incorrer em omissões que jamais poderão ser alegadas em favor de eventuais pretensões de inclusão de serviços ou acréscimos de preços.

Rio Branco - AC, [Data].

[Nome e cargo do representante da Contratada]

Visto:
Representante da SEFAZ-AC

21.5. Anexo V - Modelo de Termo de Compromisso e Manutenção do Sigilo

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Pelo presente instrumento a Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), inscrita no CNPJ sob o n.º 04.034.484/0001-40, com sede temporária à Rua Vinte e Quatro de Janeiro, nº 35, Bairro Seis de Agosto - Rio Branco/AC, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 13.709, de 14 de agosto de 2018 e demais normativos que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo na Administração Pública.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:
INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade

para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.
CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da _____, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Rio Branco - AC, [Data].

[Contratada]

[Contratante]

[Testemunhas1] / [Testemunhas2]

21.6. Anexo VI - Modelo de Termo de Ciência

TERMO DE CIÊNCIA
1 - INTRODUÇÃO
Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade.
No caso de substituição ou inclusão de empregados da contratada, o preposto deverá

entregar ao Fiscal do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.2 - identificação

CONTRATO Nº	
OBJETO	
CONTRATADA/CNPJ	
PREPOSTO	
GESTOR DO CONTRATO (Matrícula)	

3 - CIÊNCIAPor este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.4 -

FUNCIONÁRIOS DA CONTRATADA

NOME	MATRÍCULA	ASSINATURA

<local>, <dia> de <mês> de <ano>.



Documento assinado eletronicamente por **ZANIR NILSON DO NASCIMENTO DUARTE, Chefe de Divisão**, em 10/12/2025, às 12:25, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **JOSE AMARÍSIO FREITAS DE SOUZA, Secretário(a) de Estado**, em 11/12/2025, às 09:17, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **ISRAEL JORDAO SANTOS DE MELO, Chefe(a) de Departamento**, em 11/12/2025, às 10:47, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0018642278** e o código CRC **230643AE**.

MINUTA DA ATA DE REGISTRO DE PREÇOS Nº ____/202__

O Estado do Acre, por meio da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), denominada **ÓRGÃO GERENCIADOR**, **RESOLVE** registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as 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 futura e eventual **contratação de empresa especializada para prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS (Software as a Service), com o fornecimento das respectivas soluções de software e serviços técnicos especializados**, visando atender às demandas da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), conforme especificações e condições constantes no Edital e anexos e, ainda, a documentação, as propostas de preços, os lances apresentados pelo licitante classificado em primeiro lugar e os demais fornecedores que tiveram seus preços registrados para a formação de cadastro de reserva (incisos I e II do art. 11 do Decreto nº 7.892/2014), a fim de atender ao quantitativo total estimado para a contratação, observado o preço da proposta vencedora, visando contratações futuras.

2. DOS PREÇOS, DESCRIÇÃO E QUANTITATIVOS

2.1. O preço registrado, a descrição 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:

2.1.1. **Tabela 01** - Descrição dos itens e quantidades:

ITEM	DESCRIÇÃO	UNID	QUANT	R\$ UNITÁRIO	R\$ TOTAL
1	SOC – <i>Security Operations Center</i>	Mês			
2	Solução para Gestão de Vulnerabilidades	Mês			
3	Solução para Gerenciamento e Correção de Eventos de Segurança – FortiSIEM	Mês			
4	Solução de <i>Inteligência contra Ameaças (Threat Intelligence)</i>	Mês			
5	Solução para Validade de Segurança Contínua – BAS	Mês			
6	Solução para Gestão de Acessos Privilegiados – PAM	Mês			
7	Consultoria em Serviços Especializados (<i>on demand</i>)	HST			

3. ORGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1. O órgão gerenciador será a Secretaria de Estado da Fazenda - SEFAZ/AC.

3.2. Além do gerenciador, não há órgãos e entidades públicas participantes do registro de preços.

4. DA ADESAO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, 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:

- a) apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
- b) 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
- c) 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.

4.3. 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.

4.4. 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 noventa dias, observado o prazo de vigência da ata.

4.5. 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.

5. DOS LIMITES PARA AS ADESÕES

5.1. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

5.2. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

5.3. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias, não ficando sujeita ao limite de que trata o item 5.1, desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021.

6. VEDAÇÃO A ACRÉSCIMO DE QUANTITATIVOS

6.1. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

7. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

7.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogado por igual período, desde que comprovado o preço vantajoso, nos termos do art. 22, do Decreto nº 11.462, de 31 de março de 2023.

7.2. 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.

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

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

7.5. O instrumento contratual de que trata o item 7.2. deverá ser assinado no prazo de validade da ata de registro de preços.

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

7.7. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

7.8. 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;

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

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

7.11. Mantiverem sua proposta original.

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

7.13. 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.

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

7.15. 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

7.16. Quando houver o cancelamento do registro do licitante ou do registro de preços, 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.

7.17. 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.

7.18. 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.

7.19. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

7.20. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, 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.

7.21. Na hipótese de nenhum dos licitantes 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:

7.22. 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

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

7.24. 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.

8. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

8.1. 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:

8.2. 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;

8.3. 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;

8.4. 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.

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

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

9. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

9.1. 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.

9.2. 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.

9.3. 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.

9.4. 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.

9.5. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

9.6. 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.

9.7. 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.

9.8. Não 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, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

9.9. 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

9.10. 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.

9.11. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

9.12. 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.

10. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS

10.1. As quantidades previstas para os itens com preços registrados nas atas 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.

10.2. O remanejamento somente poderá ser feito:

- a) De órgão ou entidade participante para órgão ou entidade participante; ou
- b) De órgão ou entidade participante para órgão ou entidade não participante.

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

10.4. 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.

10.5. 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.

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

11. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR

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

- a) Descumprir as condições da ata de registro de preços, sem motivo justificado;
- b) Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;
- c) Não aceitar manter seu preço registrado; ou
- d) Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

11.2. 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 poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

11.3. O cancelamento de registros será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

11.4. 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.

11.5. 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:

- a) Por razão de interesse público;
- b) A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou
- c) Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado.

12. DAS PENALIDADES

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

12.2. 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.

12.3. 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 participante a aplicação da penalidade.

12.4. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

13. CONDIÇÕES GERAIS

13.1. 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 aviso de contratação direta.

13.2. 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.

13.3. Para firmeza e validade do pactuado, a presente Ata depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos demais órgãos participantes (se houver).

XXXX
Órgão Gerenciador

XXXXX
Representante Legal



Documento assinado eletronicamente por **ZANIR NILSON DO NASCIMENTO DUARTE, Chefe de Divisão**, em 10/12/2025, às 12:26, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **ISRAEL JORDAO SANTOS DE MELO, Chefe(a) de Departamento**, em 11/12/2025, às 10:47, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0018642308** e o código CRC **6D60CA30**.

ANEXO III DO EDITAL - MINUTA DO CONTRATO

MINUTA DE CONTRATO nº 1/2026/SEFAZ - DIPROJ

MINUTA DE CONTRATO Nº ____/202__

CONTRATO DE PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA, COM O FORNECIMENTO DAS RESPECTIVAS SOLUÇÕES DE SOFTWARE E SERVIÇOS TÉCNICOS ESPECIALIZADOS, QUE CELEBRAM ENTRE SI A SECRETARIA DE ESTADO DA FAZENDA E A [.....].

Processo nº: 0715.007435.00055/2025-41

O **Estado do Acre**, por meio da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), inscrita no CNPJ sob o n.º 04.034.484/0001-40, com sede temporária à Rua Vinte e Quatro de Janeiro, nº 35, Bairro Seis de Agosto - Rio Branco/AC, representada neste ato por seu Secretário de Estado da Fazenda, o Sr., inscrito no CPF nº, domiciliado nesta capital, no uso das atribuições legais que lhe confere o Decreto nº, dede 202....., publicado no Diário Oficial do Estado nº, de de de 202....., denominado simplesmente **CONTRATANTE**, e do outro lado a empresa, devidamente inscrita no CNPJ Nº, estabelecida na, neste ato representada pelo Sr.(a), portador da cédula de identidade nº inscrito no CPF/MF nº, domiciliado e residente cidade de, denominada simplesmente **CONTRATADA**, pactuam o presente **CONTRATO** em conformidade com o que dispõe a Lei nº 14.133/2021 e suas alterações, mediante as cláusulas e condições a seguir:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Constitui objeto do presente a **contratação de empresa especializada para prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS (Software as a Service), com o fornecimento das respectivas soluções de software e serviços técnicos especializados**, visando atender às demandas da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC), nos termos da tabela abaixo, conforme condições e exigências estabelecidas no Edital e seus anexos.

1.2. **Tabela 1.** A solução de serviços:

ITEM	DESCRIÇÃO	UNID	QUANT	R\$ UNITÁRIO	R\$ TOTAL
1	SOC – <i>Security Operations Center</i>	Mês			
2	Solução para Gestão de Vulnerabilidades	Mês			
3	Solução para Gerenciamento e Correção de Eventos de Segurança – FortiSIEM	Mês			
4	Solução de <i>Inteligência contra</i>	Mês			

	Ameaças (Threat Intelligence)				
5	Solução para Validade de Segurança Contínua – BAS	Mês			
6	Solução para Gestão de Acessos Privilegiados – PAM	Mês			
7	Consultoria em Serviços Especializados (on demand)	HST			

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Vinculam esta contratação, independentemente de transcrição:

- O Termo de Referência;
- O Edital de Licitação;
- A Proposta do Contratado;
- Eventuais anexos dos documentos supracitados.

3. CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. Da Vigência

3.1.1. O prazo de vigência da contratação para os **itens 1, 2, 3, 4, 6 e 7** será de **60 (sessenta) meses** e para o **item 5** será de **24 (vinte e quatro) meses**, contados da data da assinatura do contrato, de acordo com o que prescreve o art. 106 da Lei 14.133/21, *verbis*:

"Art. 106. A Administração poderá celebrar contratos com prazo de até 5 (cinco) anos nas hipóteses de serviços e fornecimentos contínuos, observadas as seguintes diretrizes:

I - a autoridade competente do órgão ou entidade contratante deverá atestar a maior vantagem econômica vislumbrada em razão da contratação plurianual;

II - a Administração deverá atestar, no início da contratação e de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção;

III - a Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

§ 1º A extinção mencionada no inciso III do caput deste artigo ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

§ 2º Aplica-se o disposto neste artigo ao aluguel de equipamentos e à utilização de programas de informática.

3.1.2. O contrato poderá ser prorrogável na forma do artigo 107 da Lei nº 14.133, de 2021, vejamos:

Art. 107. Os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes."

3.1.3. No período de vigência do Contrato estão incluídos todos os prazos necessários à perfeita execução do objeto nos termos pactuados entre as partes, ressalvados os casos referentes às garantias do objeto, que extrapolam o referido prazo de vigência.

3.2. Da Eficácia

3.2.1. A eficácia do contrato estará condicionada à publicação do extrato no Diário Oficial do Estado do Acre e no Portal Nacional de Contratações Públicas (PNCP).

3.2.2. A divulgação no Portal Nacional de Contratações Públicas (PNCP) é condição indispensável para a eficácia do contrato e de seus aditamentos e deverá ocorrer nos seguintes prazos, contados da data de sua assinatura:

- a) 20 (vinte) dias úteis, no caso de licitação;
- b) 10 (dez) dias úteis, no caso de contratação direta.

4. CLÁUSULA QUARTA – MODELO DE EXECUÇÃO DO OBJETO

4.1. Reunião Inicial

4.1.1. A CONTRATANTE convocará a CONTRATADA imediatamente após assinatura do contrato para reunião de kickoff, visando alinhamento de escopo, definição de responsáveis, cronograma e esclarecimento de dúvidas. Outros assuntos pertinentes poderão ser tratados nessa reunião.

4.1.2. Reuniões de monitoramento ou extraordinárias poderão ser convocadas durante a execução, sendo obrigatória a participação da CONTRATADA.

4.1.3. Todas as atas e comunicações entre as partes, bem como intercorrências contratuais, serão arquivadas em processo próprio para manutenção do histórico e rastreabilidade da gestão do contrato.

4.1.4. Na reunião inicial, a CONTRATADA deverá:

4.1.4.1. Apresentar formalmente o preposto responsável.

4.1.4.2. Entregar o Termo de Ciência, assinado por todos os funcionários alocados, conforme modelo no Anexo VI.

4.1.4.3. Entregar o Termo de Compromisso, assinado pelo representante legal, conforme modelo no Anexo V.

4.1.5. Havendo uso de solução complementar para execução dos serviços, a CONTRATADA deverá apresentar declaração do fabricante autorizando comercialização, instalação, configuração e suporte, constando data e número do edital.

4.1.6. A CONTRATADA deverá, em até 5 dias úteis da assinatura, apresentar o cronograma de execução dos serviços, que será aprovado formalmente pela CONTRATANTE e servirá como parâmetro para início das atividades.

4.2. **Mecanismos Formais de Comunicação**

4.2.1. São considerados mecanismos oficiais de comunicação: Ordem de Serviço, correio eletrônico, mensageria instantânea, sistema de chamados, registro de incidente e ofício.

4.3. **Procedimentos de Encaminhamento e Controle de Solicitações**

4.3.1. A abertura de chamados será realizada por canais definidos (telefone, e-mail, portal web), com categorização por gravidade de 1 a 4 (crítico a baixo), e prioridade atribuída pela CONTRATANTE.

4.3.2. Todo chamado deverá ser registrado com histórico, tempos de resposta e providências, gerando relatório mensal para auditoria.

4.3.3. Providenciar mecanismo de escalonamento para casos de insatisfação com tratamento dos chamados.

4.4. **Prazos, Horários da Prestação dos Serviços**

4.4.1. A CONTRATADA deverá considerar o horário de 7 horas às 18 horas como de horário normal de expediente da Contratante, para os dias úteis.

4.4.2. Deve ser possível a comunicação com o preposto fora do horário de atendimento.

4.4.3. A CONTRATADA deverá disponibilizar números de celular e escala do(s) profissional(ais) que responderão pelo papel de preposto(s), os supervisores e seu substitutos, mesmo fora do horário de expediente, sem que com isso ocorra qualquer ônus extra para o CONTRATANTE.

4.4.4. As atividades deverão estar disponíveis para o CONTRATANTE, no regime 24/7/365 (todos os dias do ano em horário integral, de forma ininterrupta).

4.4.5. Nos casos de ocorrências de incidentes e problemas graves, poderá ser exigida a presença do supervisor na “Sala de Crise” da CONTRATANTE.

4.4.6. Todos os níveis mínimos de serviço especificados neste documento deverão ser atendidos, independentemente do momento de abertura do chamado.

4.4.7. A CONTRATADA poderá realizar os serviços de forma remota, por meio de acesso seguro em qualquer horário de atendimento, desde que este método de acesso esteja previamente autorizado pela SEFAZ e que sejam atendidas as determinações da Política de Segurança.

4.4.8. Quando necessário os serviços técnicos (que necessitem da presença de técnicos para o atendimento) serão realizados aos finais de semana e feriados, inclusive no período noturno, e em dias úteis durante o período noturno e não deverá acarretar ônus para a CONTRATANTE.

4.4.9. Os custos decorrentes de deslocamento e hospedagem dos profissionais da CONTRATADA correrão por conta exclusiva da CONTRATADA.

4.4.10. Nos serviços prestados no âmbito da presente solução, inclusive nos serviços com execução presencial, não se caracteriza a subordinação direta e nem pessoalidade, uma vez que não se requer a exclusividade dos profissionais e sim, meramente, a disponibilidade do serviço de determinados perfis profissionais. Dessa forma, não há óbice ao compartilhamento de qualquer profissional com outros contratos que porventura a CONTRATADA possua, desde que preservados os níveis mínimos de serviços estipulados no Termo de Referência, e, além disso, não haverá qualquer relação de subordinação jurídica entre os profissionais da CONTRATADA e o CONTRATANTE.

4.5. **Locais de Entrega**

4.5.1. O fornecimento dos serviços serão executados, quando realizados na modalidade presencial, na sede da SEFAZ, situada na Rua Benjamim Constant, nº 946, Centro, Rio Branco – AC.

4.6. **Manutenção de Sigilo e Segurança**

4.6.1. A CONTRATADA 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.

4.6.2. Todos os profissionais da CONTRATADA deverão assinar Termo de Compromisso e Ciência, comprometendo-se a guardar sigilo absoluto sobre dados, informações e sistemas acessados no escopo do contrato, inclusive após seu término.

4.7. **Auditoria, Relatórios e Revisões**

4.7.1. A CONTRATADA deverá manter, durante a vigência contratual e pelo prazo mínimo de 5 anos, toda documentação e logs dos serviços prestados, acessível à auditoria e fiscalização da CONTRATANTE.

4.7.2. Relatórios consolidados de desempenho, históricos de chamados e conformidade deverão ser encaminhados periodicamente.

4.7.3. O modelo de execução poderá ser aprimorado por aditivo diante de novas demandas técnicas, legais ou de evolução tecnológica, mediante justificativa e aprovação formal da CONTRATANTE.

4.8. **Continuidade contratual**

4.8.1. A CONTRATADA deverá garantir a plena continuidade dos serviços contratados, independentemente de paralisação, greve, falhas internas, falta de pessoal, eventos de força maior ou quaisquer intercorrências, mediante plano de contingência e providências imediatas, previamente aprovado pela CONTRATANTE.

4.8.2. É obrigatória a substituição imediata de profissionais, materiais, equipamentos ou soluções que comprometam a regularidade do serviço, sem interrupção ou prejuízo à CONTRATANTE.

4.8.3. Em caso de transição contratual, a CONTRATADA promoverá transferência ordenada do conhecimento, capacitação de equipe interna, quando solicitada, e apoio técnico à nova empresa, até encerramento regular dos serviços.

5. **CLÁUSULA QUINTA – MODELO DE GESTÃO DO CONTRATO**

5.1. **Princípios Gerais e Execução**

5.1.1. O contrato deverá ser executado fielmente pelas partes, em estrita conformidade com as cláusulas avençadas, observando integralmente as disposições da Lei nº 14.133/2021 e regulamentos aplicáveis.

5.1.2. Em situações de impedimento, ordem de paralisação ou suspensão formal do contrato, o prazo de execução será automaticamente prorrogado pelo período correspondente, devendo tais circunstâncias ser formalizadas por apostila no processo.

5.1.3. Todas as comunicações relevantes para a execução contratual deverão ser realizadas por escrito, admitindo-se o uso de mensagem eletrônica, assegurando-se rastreabilidade e arquivamento nos autos do processo do contrato.

5.1.4. A CONTRATANTE poderá demandar, a qualquer tempo, providências imediatas por parte da CONTRATADA, convocando representantes para reuniões presenciais ou virtuais, sempre que necessário.

5.2. **Fiscal do Contrato**

5.2.1. São atribuições do fiscal do contrato, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos, regulamentos e normas internas:

a) Conferir a execução do serviço e o cumprimento das obrigações contratuais, atestando mediante documento próprio a efetiva prestação dos serviços após conferência do objeto contratado, especificações técnicas e resultados entregues;

b) Controlar a efetividade, qualidade e conformidade dos serviços executados, exigindo a correção de eventuais vícios, imperfeições, deficiências ou omissões, bem como solicitar medidas corretivas à contratada;

c) Registrar todas as ocorrências, intercorrências, falhas, não conformidades e eventos relevantes havidos durante a execução do contrato, em sistema próprio ou processo administrativo específico, informando dia, mês, ano e, quando aplicável, os profissionais envolvidos;

d) Apresentar, periodicamente ou quando solicitado, relatório circunstanciado de acompanhamento da execução do serviço, com avaliação crítica de desempenho, cumprimento dos níveis mínimos de serviço e registro de fatos relevantes;

e) Encaminhar à autoridade superior, ao gestor do contrato ou à assessoria técnica, quando necessário, questões que ultrapassem sua esfera de atuação ou demandem deliberação específica;

f) Solicitar, sempre por escrito, esclarecimentos, auxílio, documentações, suporte técnico ou informações adicionais relativas à execução contratual, inclusive em casos em que houver dúvidas sobre providências a adotar;

g) Emitir atestados, certidões, pareceres técnicos ou registro de avaliação dos serviços prestados, conforme demanda administrativa ou regulatória;

h) Informar imediatamente o gestor do contrato sobre irregularidades, descumprimentos ou situações que exijam providências administrativas, inclusive para glosa de pagamentos, aplicação de sanções ou revisão contratual;

i) Participar das reuniões periódicas de acompanhamento e alinhamento contratual, promovendo o registro de questões técnicas, operacionais e administrativas relevantes à boa execução do contrato;

j) Guardar sigilo sobre informações, processos e documentos acessados no exercício da fiscalização, assegurando a confidencialidade dos dados institucionais e respeitando os termos de sigilo e compromisso exigidos pela Administração;

k) Zelar pela observância de todas as normas técnicas, legais, de segurança da informação, ambientais e de boas práticas aplicáveis ao serviço fiscalizado, promovendo o atendimento integral às exigências do instrumento contratual.

5.3. **Gestor do Contrato**

5.3.1. Compete ao Gestor do Contrato, sem prejuízo das demais previstas no Manual de Gestão e Fiscalização dos Contratos Administrativos, regulamentos e normas internas:

- a) Assegurar que todas as obrigações contratuais assumidas pela contratada estejam sendo cumpridas dentro dos padrões de qualidade, conformidade técnica e observância à legislação vigente;
- b) Solicitar periodicamente ao fiscal do contrato o envio de relatórios circunstanciados, ocorrências relevantes e indicativos de não conformidade para avaliação e eventual adoção de medidas corretivas.
- c) Analisar e homologar as glosas, descontos ou retenções sugeridas pelo fiscal do contrato, deliberando sobre descontos nos pagamentos mensais e notificando a área financeira para os devidos ajustes;
- d) Encaminhar formalmente demandas, ordens de serviço ou de fornecimento ao preposto da contratada, assegurando o registro e rastreabilidade dessas comunicações nos autos do processo;
- e) Repassar ao fiscal do contrato todas as informações, documentos e ocorrências relevantes à execução contratual, facilitando o exercício eficiente da fiscalização;
- f) Monitorar rigorosamente a vigência contratual, providenciando prorrogações, encerramentos, aditivos ou resoluções, conforme justificativas técnicas, zelo pelo interesse público e observância aos prazos legais e regulatórios;
- g) Propor e implementar medidas que visem a melhoria contínua da gestão e da execução do contrato, inclusive revisão de processos, indicadores de desempenho e adoção de melhores práticas administrativas e técnicas;
- h) Providenciar, sempre por escrito, a obtenção de esclarecimentos, auxílio ou suporte técnico sobre dúvidas, divergências ou situações complexas relativas à execução do contrato, consultando setores técnicos, jurídicos ou de controle quando necessário;
- i) Negociar, dentro dos limites legais e de mercado, condições contratuais previamente estabelecidas com o fornecedor, especialmente durante processos de prorrogação contratual ou em situações que exijam revisão de condições técnicas e comerciais;
- j) Informar periodicamente a administração superior sobre o andamento do contrato, eventuais problemas ocorridos, providências adotadas, conclusões de processos de pagamento, sanções e regularidade documental;
- k) Notificar a contratada, por ordem da autoridade competente, sobre irregularidades, não conformidades ou descumprimentos identificados no curso da execução contratual;
- l) Promover reuniões de acompanhamento da execução contratual, debate de indicadores de desempenho, análise de resultados e alinhamento de expectativas entre todas as partes envolvidas, registrando atas e deliberações nos autos do processo;
- m) Participar ativamente de auditorias internas, externas e de órgãos de controle quanto à gestão do contrato, prestando informações, documentação e esclarecimentos sempre que requisitado.

5.4. **Avaliação de Resultados e Níveis de Serviço**

5.4.1. A avaliação da execução contratual será realizada com base nos indicadores de desempenho (KPIs), metas, percentuais e Níveis Mínimos de Serviço (NMS), definidos nas Especificações Técnicas Mínimas e seus anexos, observando-se os seguintes parâmetros:

a) *Tempo de Resposta de Chamados:*

- Para incidentes críticos, resposta inicial em até 2 horas;
- Para incidentes tratados pela equipe CSIRT, resposta inicial em até 30 minutos;
- Para consultoria on demand, início do atendimento em até 3 dias úteis;
- Para chamados de menor severidade, resposta inicial em até 24 horas;
- Primeira notificação de *Takedown* (*Threat Intelligence*): máximo de 5 minutos após solicitação formal.

b) *Tempo de Solução Técnica:*

- Para incidentes críticos, solução inicial em até 4 horas após registro;
- Para demais chamados, solução conforme gravidade: até 8 horas (alto), até 24 horas (médio), até 1 dia útil (baixo).

c) *Disponibilidade dos Serviços:*

- Operação e suporte técnico em regime 24x7x365, sem tolerância para interrupções não programadas.

d) *Requisitos de Substituição de Componentes:*

- Obrigatoriedade de substituição de componentes/equipamentos que apresentem 3 ou mais chamados corretivos em 30 dias ininterruptos, ou acumularem tempo de paralisação superior a 20 horas neste período, com prazo máximo de substituição de 10 dias úteis.

e) *Atualização, Monitoramento e Manutenção:*

- Atualização automática das bases de dados, regras de correlação e ferramentas de defesa/monitoramento, conforme ciclo semanal mínimo;
- Avaliação/tuning dos controles para redução de falsos positivos e melhoria contínua da eficácia dos controles.

f) *Relatórios de Desempenho e Conformidade:*

- Entrega de relatório mensal consolidado, contendo: histórico de chamados, ocorrências relevantes, incidentes tratados, tempo de resposta, tempo de solução, status dos indicadores, medidas de contenção e proposta de melhorias.
- Manutenção de registros eletrônicos e logs acessíveis para fiscalização/auditoria pelo prazo legal mínimo de 5 anos.

g) *Avaliação e Sanções:*

- Descumprimento de qualquer indicador ou meta acarretará aplicação imediata de glosa proporcional, desconto em pagamento, comunicação formal à contratada e registro em processo próprio para análise de sanções administrativas e contratuais.
- Ocorrências de indisponibilidade superior a 0,5% ao mês ou descumprimento de prazos críticos ensejam sanções, inclusive rescisão.

h) *Certificações e Perfis Técnicos:*

- Equipe e serviços certificados em normas ISO/IEC 27001, 20000, 9001, 27701 e profissionais com CEH, CYSA, NSE4, CISSP, CISM;
- Adoção de frameworks, metodologias e controles NIST, SANS, MITRE e demais padrões internacionais de segurança e resposta a incidentes.

i) *Reunião de Avaliação:*

- Realização obrigatória de reuniões periódicas entre a CONTRATANTE, gestor, fiscal e representantes técnicos da contratada para análise dos resultados, planos de alinhamento e definição de metas de melhoria contínua.

5.4.2. Todos os indicadores, metas e SLA's contratualmente pactuados estão detalhados no Anexo I deste Termo de Referência, podendo ser revisados e atualizados mediante justificativa técnica e aditamento contratual.

5.5. Encerramento Contratual

5.5.1. Para o encerramento do contrato, será observada a conferência completa de obrigações, entrega definitiva dos serviços, transferência de conhecimento, liquidação das pendências técnicas e emissão do termo de recebimento definitivo, com ciência das partes.

6. CLÁUSULA SEXTA - SUBCONTRATAÇÃO

6.1. Não será admitida a subcontratação do objeto contratual.

7. CLÁUSULA SÉTIMA - PREÇO

7.1. O valor total do presente contrato é de R\$. (.....), já incluídos todos os impostos, taxas e quaisquer outras despesas que sejam pertinentes ao objeto contratado.

8. CLÁUSULA OITAVA – LIQUIDAÇÃO E PAGAMENTO

8.0.1. O pagamento pelos serviços efetivamente prestados dar-se-á em parcelas e será creditado mensalmente à empresa CONTRATADA, ocorrendo no prazo não superior a 5 (cinco) dias úteis, contados do recebimento do documento fiscal e devido ateste da Nota Fiscal/Fatura - que deverá conter o endereço, o CNPJ, os números do Banco, da Agência e da Conta Corrente da Empresa contratada, o número da Nota de Empenho e a descrição clara do objeto - em moeda corrente nacional, de acordo com as condições constantes na proposta da Empresa contratada e aceita pela Administração contratante.

8.0.2. A emissão da ordem bancária será efetivada após o documento fiscal ser conferido, aceito e atestado por servidor responsável, caracterizando o recebimento definitivo, e ter sido verificada a regularidade da Empresa contratada, mediante consulta on-line ao Sistema Unificado de Cadastro de Fornecedores (SICAF), ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do CNJ e à Certidão Negativa (ou Positiva com efeito de Negativa) de Débitos Trabalhistas (CNDT), para comprovação, dentre outras coisas, do devido recolhimento das contribuições sociais (FGTS e Previdência Social) e demais tributos estaduais, federais e municipais, conforme cada caso.

8.0.3. O documento fiscal deverá ser emitido em nome da Secretaria de Estado da Fazenda (SEFAZ) - CNPJ nº 04.034.484/0001-40.

8.0.4. Na ocorrência de rejeição do documento fiscal motivado por erro ou incorreções, ele será devolvido à empresa contratada para retificação e reapresentação, acrescendo-se, no prazo fixado para pagamento, os dias que se passarem entre a data da devolução e a da reapresentação.

8.0.5. Nos casos de eventuais atrasos injustificados de pagamento, desde que a Empresa contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pela Administração contratante, desde a data limite fixada para pagamento até a data do efetivo pagamento, será a seguinte: $EM = (N \times VP \times I / 365)$, onde: EM = Encargos moratórios a serem pagos pelo atraso de pagamento; N = Número de dias de atraso contados entre a data limite prevista para o pagamento e a data do efetivo pagamento; VP = Valor da parcela em atraso; e I = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE) / 100.

8.0.6. Os documentos de cobrança deverão ser entregues pela empresa contratada, na SEFAZ, no horário de expediente da CONTRATANTE, ou por e-mail a ser informado quando da assinatura do contrato.

8.0.7. Em nenhuma hipótese será efetuado pagamento de documento fiscal com o número do CNPJ/MF diferente do que foi apresentado na proposta de preços, mesmo que sejam empresas consideradas matriz e filial ou vice-versa, ou pertencentes ao mesmo grupo ou conglomerado.

8.0.8. Não será realizado qualquer tipo de pagamento através de boleto bancário ou por outro meio diferente do previsto no Contrato.

8.0.9. A Administração CONTRATANTE, no momento do pagamento, providenciará as devidas retenções tributárias, nos termos da legislação vigente, exceto nos casos em que a empresa contratada comprovar, na forma prevista em lei, não lhe serem aplicáveis tais retenções.

8.0.10. Caso a empresa contratada seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das ME e EPP – SIMPLES, desde que não haja vedação legal para tal opção em razão do objeto executado, deverá apresentar, juntamente com o documento fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

9. CLÁUSULA NONA - REAJUSTE

9.0.1. Os preços relativos aos serviços contratados serão fixos e irreajustáveis, durante o período de 12 (doze) meses, contado da data de assinatura do Contrato ou do último reajuste.

9.0.2. Após esse período, os preços poderão ser reajustados, mediante a aplicação do **ICTI (Índice de Custo da Tecnologia da Informação)**, calculado pelo Instituto de Pesquisas Econômicas Aplicadas – IPEA, ocorrido no período, ou por outro índice que o venha a substituí-lo.

9.0.3. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

10. CLÁUSULA DÉCIMA - EQUILÍBRIO ECONÔMICO-FINANCEIRO

10.1. Com vistas à manutenção do equilíbrio econômico financeiro do Contrato, poderá ser promovida revisão contratual, desde que eventuais solicitações nesse sentido estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, configurando álea econômica extraordinária e extracontratual, bem como de demonstração analítica de seu impacto nos custos do Contrato, nos termos da Lei nº 14.133/21.

11. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

11.0.1. Exigir o cumprimento integral das obrigações assumidas pela CONTRATADA.

11.0.2. Conferir e validar os relatórios gerenciais dos serviços executados, apresentados pela CONTRATADA.

11.0.3. Orientar e supervisionar a observância, pela CONTRATADA, dos regulamentos administrativos e dos procedimentos de segurança da SEFAZ/AC.

11.0.4. Encaminhar formalmente as demandas à CONTRATADA, por meio de Ordem de Serviço, ou por sistema de chamados, de acordo com os critérios dispostos neste Termo de Referência.

11.0.5. Exercer o acompanhamento e a fiscalização do contrato, por intermédio de servidores especialmente designados, conforme art. 140 da Lei nº 14.133/2021.

11.0.6. Notificar a CONTRATADA por escrito sobre toda e qualquer ocorrência relevante à prestação dos serviços, fixando prazo para correção e certificando-se da adequação das soluções.

11.0.7. Realizar avaliações periódicas da qualidade dos serviços após o seu recebimento, promovendo os registros necessários.

11.0.8. Aplicar à CONTRATADA as sanções administrativas e contratuais cabíveis, nos termos da legislação.

11.0.9. Emitir, por meio do Departamento de Tecnologia da Informação, pareceres sobre atos relativos à execução do contrato, especialmente quanto à exigência de condições estabelecidas no processo licitatório.

11.0.10. Liquidar o empenho e efetuar o pagamento à CONTRATADA dentro dos prazos preestabelecidos.

11.0.11. Comunicar formalmente à CONTRATADA todas as ocorrências relacionadas à execução dos serviços, inclusive quanto à necessidade de providências corretivas.

- 11.0.12. Prestar informações necessárias à execução do objeto, em tempo hábil, sempre que solicitado pela CONTRATADA.
- 11.0.13. Permitir o acesso do pessoal técnico e dos equipamentos da CONTRATADA necessários à execução dos serviços, obedecidas as normas de segurança e sigilo institucionais.
- 11.0.14. Encaminhar as faturas dos serviços prestados para o ateste dos gestores competentes.
- 11.0.15. Não responder por compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por danos a terceiros decorrentes de atos da CONTRATADA ou de seus prepostos e empregados.

12. CLÁUSULA DÉCIMA SEGUNDA – OBRIGAÇÕES DA CONTRATADA

- 12.0.1. Indicar formalmente, em até 5 dias úteis após a assinatura do contrato, preposto responsável pela execução do objeto e interlocução com a CONTRATANTE.
- 12.0.2. Atender prontamente todas as orientações, exigências e determinações da fiscalização do contrato, inerentes à execução do objeto.
- 12.0.3. Reparar, corrigir, remover, reconstruir ou substituir, integralmente e às suas expensas, quaisquer danos, vícios, defeitos ou incorreções resultantes da execução do contrato, dos serviços ou dos materiais empregados, responsabilizando-se inclusive pelo ressarcimento imediato de prejuízos causados à CONTRATANTE ou a terceiros.
- 12.0.4. Manter, durante toda a execução do contrato, todas as condições referentes à habilitação jurídica, fiscal, trabalhista, previdenciária, técnica e financeira exigidas à época da contratação.
- 12.0.5. Manter sua equipe de profissionais continuamente capacitada, treinada e certificada, conforme requisitos técnicos do Termo de Referência e suas atualizações.
- 12.0.6. Executar todos os serviços contratados em estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), normas correlatas e exigências da CONTRATANTE.
- 12.0.7. Não divulgar, publicar ou utilizar, sem autorização prévia e expressa da CONTRATANTE, qualquer informação ou publicidade relativa à execução dos serviços objeto do contrato.
- 12.0.8. Utilizar as informações e dados da CONTRATANTE exclusivamente para execução do objeto contratual, vedada sua utilização, reprodução ou divulgação para quaisquer outros fins.
- 12.0.9. Garantir que todos profissionais envolvidos possuam perfil técnico adequado e estejam atualizados conforme exigências das soluções contratadas e fabricantes.
- 12.0.10. Responder integralmente por todas as obrigações trabalhistas, fiscais, previdenciárias e tributárias pertinentes, eximindo a Administração de qualquer responsabilidade solidária ou subsidiária em caso de inadimplência.
- 12.0.11. Realizar os serviços conforme especificações técnicas estabelecidas, mantendo a produtividade, qualidade e recursos necessários ao perfeito cumprimento contratual.
- 12.0.12. Realizar a correção, substituição ou reparo de qualquer serviço ou material que apresente inadequação, vício ou defeito, conforme determinação da CONTRATANTE.
- 12.0.13. Aceitar acréscimos e supressões no objeto contratual conforme previsto pela Lei nº 14.133/2021, até o limite de 25% do valor inicial, sem questionar ou impedir a execução do ajuste.
- 12.0.14. Comunicar de imediato à CONTRATANTE qualquer anomalia, acidente, irregularidade ou fato relevante que possa comprometer a boa execução dos serviços.
- 12.0.15. Garantir o acesso irrestrito à fiscalização da CONTRATANTE, disponibilizando documentos, informações e recursos solicitados sempre que necessário.
- 12.0.16. Ressarcir a CONTRATANTE por danos causados por suas ações ou omissões, seja por agentes, prepostos ou empregados, autorizando desconto em garantia ou pagamentos devidos.
- 12.0.17. Arcar com despesas de qualquer infração cometida por empregados/prepostos, inclusive indenizações e penalidades legais.
- 12.0.18. Assegurar que todos profissionais alocados estejam devidamente habilitados e conhecedores dos serviços, cumprindo padrões técnicos e legais em vigor.
- 12.0.19. Manter contato permanente do preposto com a fiscalização da CONTRATANTE, adotando providências e coordenando toda a execução dos serviços contratados.
- 12.0.20. Relatar formalmente à CONTRATANTE qualquer irregularidade constatada durante a prestação dos serviços.
- 12.0.21. Manter sigilo absoluto sobre todas as informações, dados, documentos e procedimentos obtidos em razão da execução do contrato.
- 12.0.22. Notificar ao fiscal do contrato, em até 24 horas, qualquer ocorrência anormal ou acidente verificado nos serviços.
- 12.0.23. Prestar todos os esclarecimentos, apresentar documentos e garantir acesso ao local dos trabalhos aos representantes da CONTRATANTE, sempre que solicitado.
- 12.0.24. Paralisar, imediatamente e por determinação da CONTRATANTE, qualquer atividade que esteja sendo executada em desacordo com a técnica, normas de segurança ou que exponha risco a pessoas, bens ou dados.

12.0.25. Planejar, executar, monitorar e manter os serviços contratados conforme níveis de serviço acordados e exigidos pela CONTRATANTE.

12.0.26. Submeter previamente à CONTRATANTE, por escrito, qualquer alteração de método, processo ou tecnologia que fuja das especificações do Termo de Referência, aguardando aprovação formal para implementação.

12.0.27. Cumprir integralmente todas as normas de segurança institucional determinadas pela CONTRATANTE.

12.0.28. Realizar os serviços dentro de rotinas e parâmetros técnicos aceitáveis, observando sempre as boas práticas, normas regulamentares e legislação vigente.

12.0.29. Participar das reuniões de alinhamento de expectativas estabelecidas pela CONTRATANTE, bem como das demais convocações necessárias ao acompanhamento contratual.

12.0.30. Promover a transferência de conhecimento e técnicas de execução na transição contratual, capacitando técnicos da CONTRATANTE, quando solicitado, sem prejuízo das informações.

13. CLÁUSULA DÉCIMA TERCEIRA – GARANTIA DE EXECUÇÃO

13.0.1. No ato da assinatura do Contrato, o fornecedor deve apresentar comprovante de garantia para sua execução, com validade durante todo período de vigência contratual, correspondente a 5% (cinco por cento) de seu valor global, em uma das modalidades de garantia previstas no art. 96 da Lei 14.133/21:

- I - Caução em dinheiro ou em títulos da dívida pública;
- II - Seguro garantia;
- III - Fiança bancária.
- IV - Título de Capitalização.

13.0.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- a) Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- b) Prejuízos causados à Administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
- c) Multas moratórias e punitivas aplicadas pela Administração ao contratado; e
- d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pelo contratado.

13.0.3. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento).

13.0.4. O garantidor não é parte interessada para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao contratado.

13.0.5. A garantia será considerada extinta com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

13.0.6. A garantia prestada deverá vigorar por mais 90 (noventa) dias após o término da vigência contratual e será liberada ou restituída a CONTRATADA findo este prazo, desde que integralmente cumpridas todas as obrigações assumidas, inclusive as trabalhistas. Caso o pagamento das verbas rescisórias trabalhistas não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas diretamente pela Contratante;

13.0.7. A Contratante não executará a garantia nas seguintes hipóteses:

- a) Caso fortuito ou força maior;
- b) Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;
- c) Descumprimento das obrigações pelo contratado decorrente de atos ou fatos da Administração;
- d) Prática de atos ilícitos dolosos por servidores da Administração;

13.0.8. Não serão admitidas outras hipóteses de não execução da garantia, que não as previstas no item anterior;

13.0.9. Cabe à própria administração apurar a isenção da responsabilidade prevista nos incisos III e IV acima, não sendo a entidade garantidora parte no processo instaurado pela CONTRATANTE;

13.0.10. A CONTRATADA se compromete a repor ou a completar a garantia na hipótese de utilização parcial ou total, inclusive na hipótese de utilização para indenização a terceiros, e, ainda, na alteração do valor contratado, para manter o percentual inicial, no prazo de 48 (quarenta e oito) horas, a partir da data em que for notificada pela Contratante, mediante correspondência entregue contra recibo.

14. CLÁUSULA DÉCIMA QUARTA – DA MATRIZ DE RISCO

14.1. Na hipótese de ocorrência de um dos eventos listados na matriz de risco anexa deste Contrato, a CONTRATADA deverá informar a CONTRATANTE sobre o ocorrido, contendo as seguintes informações mínimas:

14.1.1. Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada;

14.1.2. As medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;

- 14.1.3. As medidas que irá tomar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;
- 14.1.4. As obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e,
- 14.1.5. Outras informações relevantes.
- 14.2. Após a notificação, a CONTRATANTE decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais a CONTRATADA. Em sua decisão a CONTRATANTE poderá isentar temporariamente a CONTRATADA do cumprimento das obrigações contratuais afetadas pelo Evento.
- 14.3. A concessão de qualquer isenção não exclui a possibilidade de aplicação das sanções previstas na Cláusula contratual respectiva.
- 14.4. O reconhecimento pela CONTRATANTE dos eventos descritos na matriz de risco anexo deste Contrato que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente a CONTRATADA, não dará ensejo a recomposição do equilíbrio econômico financeiro do Contrato, devendo o risco ser suportado exclusivamente pela CONTRATADA.
- 14.5. As partes deverão acordar a forma e o prazo para resolução do ocorrido.
- 14.6. As partes não serão consideradas inadimplentes em razão do descumprimento contratual decorrente de caso fortuito, fato do príncipe ou força maior.
- 14.7. Avaliada a gravidade do evento, as partes, mediante acordo, decidirão quanto a recomposição do equilíbrio econômico financeiro do Contrato, salvo se as consequências do evento sejam cobertas por Seguro, se houver.
- 14.8. O Contrato poderá ser rescindido, quando demonstrado que todas as medidas para sanar os efeitos foram tomadas e mesmo assim a manutenção do contrato se tornar impossível ou inviável nas condições existentes ou é excessivamente onerosa.
- 14.9. As partes se comprometem a empregar todas as medidas e ações necessárias a fim de minimizar os efeitos advindos dos eventos de caso fortuito, fato do príncipe ou força maior.
- 14.10. Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos na matriz de risco, serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico financeiro do contrato.

15. CLÁUSULA DÉCIMA QUINTA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

- 15.1. Será considerada infratora a licitante ou contratada que incorrer em qualquer um dos incisos do Art. 155 da Lei 14.133/2021.
- 15.2. Serão aplicadas a infratora ou licitante as sanções previstas no Art. 156 da Lei 14.133.

16. CLAÚSULA DÉCIMA SEXTA – DA EXTINÇÃO CONTRATUAL

- 16.1. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:
- a) Não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;
 - b) Desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
 - c) Alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
 - d) Decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
 - e) Caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
 - f) Razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade contratante;
- 16.2. O CONTRATADO terá direito à extinção do contrato nas seguintes hipóteses:
- a) Supressão, por parte da Administração, de obras, serviços ou compras que acarrete modificação do valor inicial do contrato além do limite permitido no art. 125 da Lei 14.133/2021;
 - b) Suspensão de execução do contrato, por ordem escrita da Administração, por prazo superior a 3 (três) meses;
 - c) Repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;
 - d) Atraso superior a 2 (dois) meses, contado da emissão da nota fiscal, dos pagamentos ou de parcelas de pagamentos devidos pela Administração por despesas de obras, serviços ou fornecimentos;
 - e) Não liberação pela Administração, nos prazos contratuais, de área, local ou objeto, para execução de obra, serviço ou fornecimento, e de fontes de materiais naturais especificadas no projeto, inclusive devido a atraso ou descumprimento das obrigações atribuídas pelo contrato à Administração relacionadas a desapropriação, a desocupação de áreas públicas ou a licenciamento ambiental.
- 16.3. As hipóteses de extinção a que se referem os incisos II, III e IV observarão as seguintes disposições:
- 16.3.1. Não serão admitidas em caso de calamidade pública, de grave perturbação da ordem interna ou de guerra, bem como quando decorrerem de ato ou fato que o contratado tenha praticado, do qual tenha participado ou para o qual tenha contribuído;

16.3.2. Assegurarão ao contratado o direito de optar pela suspensão do cumprimento das obrigações assumidas até a normalização da situação, admitido o restabelecimento do equilíbrio econômico-financeiro do contrato, na forma da alínea “d” do Inciso II do caput do art. 124 desta Lei.

16.4. Os emitentes das garantias previstas no art. 96 da Lei 14.133/2021 deverão ser notificados pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

16.5. A extinção do contrato poderá ser:

- a) Determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;
- b) Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;
- c) Determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

16.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.

16.7. Quando a extinção decorrer de culpa exclusiva da Administração, o contratado será ressarcido pelos prejuízos regularmente comprovados que houver sofrido e terá direito a:

- a) Devolução da Garantia;
- b) Pagamentos devidos pela execução do contrato até a data de extinção;
- c) Pagamento do custo da desmobilização.

16.8. A extinção determinada por ato unilateral da Administração poderá acarretar, sem prejuízo das sanções previstas na Lei 14.133/2021, as seguintes consequências:

- a) Assunção imediata do objeto do contrato, no estado e local em que se encontrar, por ato próprio da Administração;
- b) Ocupação e utilização do local, das instalações, dos equipamentos, do material e do pessoal empregados na execução do contrato e necessários à sua continuidade;
- c) Execução da garantia contratual para:
 - I - Ressarcimento da Administração Pública por prejuízos decorrentes da não execução;
 - II - Pagamento de verbas trabalhistas, fundiárias e previdenciárias, quando cabível;
 - III - Pagamento das multas devidas à Administração Pública;
 - IV - Exigência da assunção da execução e da conclusão do objeto do contrato pela seguradora, quando cabível;
 - V - Retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à Administração Pública e das multas aplicadas.

17. CLÁUSULA DÉCIMA SÉTIMA – DOTAÇÃO ORÇAMENTÁRIA

17.1. As despesas decorrentes da contratação correrão à conta os recursos consignados abaixo:

- Cód. Órgão / Unidade Executora:
- Programa de Trabalho:
- Elemento de Despesa:
- Fonte de Recurso:

18. CLÁUSULA DÉCIMA OITAVA – DOS CASOS OMISSOS

18.1. 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.

19. CLÁUSULA DÉCIMA NONA - ALTERAÇÕES

19.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 124 e seguintes da Lei nº 14.133, de 2021.

19.2. 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. 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 (art. 132 da Lei nº 14.133, de 2021).

19.3. 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.

20. CLÁUSULA VIGÉSIMA - PUBLICAÇÃO

20.1. 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.

21. CLÁUSULA VIGÉSIMA PRIMEIRA - ANTICORRUPÇÃO

21.1. **Compromisso com a Integridade:** A Contratada declara expressamente que não oferecerá, dará, prometerá, solicitará ou aceitará, direta ou indiretamente, qualquer vantagem indevida, suborno, propina, comissão ou qualquer outra forma de benefício ilícito a agentes públicos ou terceiros em razão deste contrato.

21.2. **Conformidade com a Legislação:** A Contratada se compromete a cumprir todas as disposições da Lei Federal n.º 12.846/2013 (Lei Anticorrupção), da Lei Estadual n.º 3.747/2021 (Programa de Integridade e Compliance do Estado do Acre) e demais normas aplicáveis.

21.3. **Canal de Denúncias:** A Contratada se compromete a divulgar, no âmbito de sua organização, o canal de denúncias da (SECRETARIA), assegurando que qualquer colaborador possa relatar irregularidades relacionadas à execução deste contrato. Para tanto, deverão ser informados os seguintes meios de contato:

- E-mail: ouvid.sefaz@ac.gov.br
- Telefone: (68) 3212-7608
- WhatsApp: (68) 3212-7608
- Endereço: Rua 24 de Janeiro, n.º 53, Bairro Seis de Agosto. CEP 69.905-596 - Rio Branco/AC.

22. CLÁUSULA VIGÉSIMA SEGUNDA - FORO

22.1. Fica eleito o foro da Justiça Comum da Comarca de Rio Branco, Acre, como competente para dirimir quaisquer questões oriundas do presente contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

Representante Legal
Contratante

Representante Legal
Contratada



Documento assinado eletronicamente por **ZANIR NILSON DO NASCIMENTO DUARTE, Chefe de Divisão**, em 12/01/2026, às 08:56, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0018980681** e o código CRC **B572022F**.

ANEXO IV DO EDITAL - PROPOSTA DE PREÇOS (MODELO)

Referente: Edital Pregão Eletrônico SRP N.º ____/____.

Apresentamos a V.S., nossa Proposta de fornecimento de serviços especializados _____, nos termos do Edital e seus Anexos.

NOME COMPLETO DO LICITANTE: _____

CNPJ: _____

ENDEREÇO: _____

EMAIL: _____

TELEFONE: _____

CONFORME TABELA CONSTANTE NO ITEM 1. DO TERMO DE REFERÊNCIA

Item	Especificação	Unid.	Qtd Registro	Qtd Consumo	Valor Unitário	Valor Total
01	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Und.	xx	xx	XXXXXXXX	XXXX

O prazo de validade de nossa proposta de preços é de xx (xxxxxxx) dias, contados da data da abertura da licitação.

Prazo de entrega conforme especificações do Anexo I.

Declaramos que 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.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência.

Local e data

Assinatura do representante legal da empresa

Notas:

1. Em caso de discordância existente entre as especificações deste objeto descritas no COMPRASGOV e as especificações constantes do Anexo I – Termo de Referência deste Edital prevalecerão às últimas.
2. O prazo mínimo de validade da proposta será de 60 (sessenta) dias a contar da sessão pública.
3. Vide outras determinações no Anexo I – Termo de Referência, deste Edital.
- 4.

ANÁLISE DE RISCO Nº 22/2025/SEFAZ - DIPROJ

Processo nº 0715.007435.00055/2025-41

1. INTRODUÇÃO

- 1.1. O presente Mapa de Gerenciamento de Riscos tem como objetivo identificar e mitigar os principais riscos associados a **prestação de serviços gerenciados de segurança cibernética, na modalidade SaaS (Software as a Service), com o fornecimento das respectivas soluções de software e serviços técnicos especializados, visando atender às demandas da Secretaria de Estado da Fazenda do Acre (SEFAZ/AC)**, de acordo com as especificações técnicas e quantitativos previstos no Termo de Referência.
- 1.2. Este documento foi elaborado com base no Manual de Gestão de Riscos do TCU e o Código das Melhores Práticas de Governança Corporativa, e segue a metodologia de análise qualitativa e quantitativa de riscos, considerando os impactos e probabilidades conforme os padrões definidos na ISO 31000:2009.
- 1.3. O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.
- 1.4. O Mapa de Gerenciamento de Riscos deve conter a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.
- 1.5. Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impacto caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos).
- 1.6. A figura a seguir apresenta a **Matriz Probabilidade x Impacto**, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco:

PROBABILIDADE (P)			
Muito Provável 3	3 Médio	6 Alto	9 Alto
Provável 2	2 Baixo	4 Médio	6 Alto
Pouco Provável 1	1 Baixo	2 Baixo	3 Médio
	Baixo 1	Médio 2	Alto 3
	IMPACTO (I)		

- 1.7. Parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão as ações relacionadas aos riscos durante as fases de contratação (planejamento, seleção de fornecedor e gestão do contrato).
- 1.8. **Classificação de Níveis de Risco:**
- Verde = Baixo risco (1,2)
 - Amarelo = Médio risco (3,4)
 - Vermelho = Alto risco (6,9)
- 1.9. A matriz permite avaliar o nível de risco combinando a probabilidade de ocorrência do evento e seu impacto, servindo como base para definir as ações mitigadoras.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

- 2.1. Definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

2.2. A tabela síntese dos riscos identificados e classificados neste documento.

ID	Risco Identificado	Fase	Probabilidade (P) ¹	Impacto (I) ²	Nível de Risco NR= (PxI) ³
R01	Definição incompleta ou inadequada dos requisitos técnicos e de negócio, afetando especificações do edital	Planejamento da Contratação	2 (Provável)	3 (Alto)	6 (Alto)
R02	Estimativas incorretas dos quantitativos e do orçamento para contratação	Planejamento da Contratação	2 (Provável)	3 (Alto)	6 (Alto)
R03	Subdimensionamento dos riscos cibernéticos (ameaças emergentes, IA, ransomware, DDoS)	Planejamento da Contratação	2 (Provável)	3 (Alto)	6 (Alto)
R04	Falta de alinhamento com os normativos legais e regulatórios aplicáveis, como LGPD e legislação específica	Planejamento da Contratação	1 (Pouco Provável)	3 (Alto)	3 (Médio)
R05	Insuficiência no Estudo Técnico Preliminar	Planejamento da Contratação	1 (Pouco Provável)	3 (Alto)	3 (Médio)
R06	Seleção de fornecedor com capacidade técnica insuficiente (certificações, equipe qualificada e ferramentas)	Seleção do Fornecedor	2 (Provável)	3 (Alto)	6 (Alto)
R07	Critérios de julgamento inadequados (propostas fora do escopo, preço baixo sem aderência)	Seleção do Fornecedor	2 (Provável)	2 (Médio)	4 (Médio)
R08	Fraudes e irregularidades no processo licitatório	Seleção do Fornecedor	1 (Pouco Provável)	3 (Alto)	3 (Médio)
R09	Falhas de publicidade e transparência	Seleção do Fornecedor	1 (Pouco Provável)	2 (Médio)	2 (Baixo)
R10	Falhas na análise da qualificação técnica dos licitantes	Seleção do Fornecedor	2 (Provável)	3 (Alto)	6 (Alto)
R11	Ausência de monitoramento contínuo e efetivo dos serviços contratados	Gestão do Contrato	2 (Provável)	3 (Alto)	6 (Alto)

R12	Inadimplência contratual com relação a requisitos técnicos e de segurança da informação	Gestão do Contrato	1 (Pouco Provável)	3 (Alto)	3 (Médio)
R13	Comunicação falha entre gestor, fiscal e fornecedor	Gestão do Contrato	2 (Provável)	2 (Médio)	4 (Médio)
R14	Defasagem tecnológica durante a vigência do contrato	Gestão do Contrato	2 (Provável)	3 (Alto)	6 (Alto)
R15	Falta de capacitação contínua da equipe operacional	Gestão do Contrato	2 (Provável)	2 (Médio)	4 (Médio)
R16	Riscos de incidentes de exfiltração de dados/transgressão à LGPD	Gestão do Contrato	2 (Provável)	3 (Alto)	6 (Alto)
R17	Riscos de integração/API entre sistemas SaaS/SOC	Gestão do Contrato	2 (Provável)	2 (Médio)	4 (Médio)

Legenda: P – Probabilidade; I – Impacto.
1 Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita uti lizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
2 Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
3 Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

2.3. Tabela analítica dos critérios de Probabilidade e Impacto para cada risco apresentado

ID	Risco Identificado	Critérios para Probabilidade	Critérios para Impacto
R01	Definição incompleta ou inadequada dos requisitos técnicos e de negócio, afetando especificações do edital	2 (Provável) Falhas recorrentes em processos de contratação TIC/SaaS e constante inovação tecnológica	3 (Alto) Possível incompatibilidade de solução, prejuízos e paralisação contratual
R02	Estimativas incorretas dos quantitativos e do orçamento para contratação	2 (Provável) Erros no dimensionamento inicial	3 (Alto) Gera sobrepreço, aditivos, insuficiência operacional
R03	Subdimensionamento dos riscos cibernéticos (ameaças emergentes, IA, ransomware, DDoS)	2 (Provável) Cenário dinâmico, ameaças emergentes e evolução de técnicas	3 (Alto) Falhas de proteção, vazamentos ou ataques, prejuízo funcional
R04	Falta de alinhamento com os normativos legais e regulatórios aplicáveis, como LGPD e legislação específica	1 (Pouco provável) Monitoramento é estruturado e legislação é conhecida	3 (Alto) Risco de sanções legais, descumprimento normativo, reputação

R05	Insuficiência no Estudo Técnico Preliminar	1 (Pouco provável) Revisão intersetorial e práticas de elaboração presentes	3 (Alto) Falhas graves no planejamento, processos e contratação
R06	Seleção de fornecedor com capacidade técnica insuficiente (certificações, equipe qualificada e ferramentas)	2 (Provável) Ofertas no mercado sem consistência técnica são comuns	3 (Alto) Prejuízos na execução, interrupção contratual, baixa qualidade
R07	Critérios de julgamento inadequados (propostas fora do escopo, preço baixo sem aderência)	2 (Provável) Editais podem conter equívocos; histórico de impugnações	2 (Médio) Contratação fora do escopo, impacto moderado na execução
R08	Fraudes e irregularidades no processo licitatório	1 (Pouco provável) Estrutura de controle, auditoria e transparência presentes	3 (Alto) Prejuízo financeiro, questionamento legal, paralisação
R09	Falhas de publicidade e transparência	1 (Pouco provável) Ações de publicidade exigidas; sistema eletrônico	2 (Médio) Menor número de participantes, questionamentos administrativos
R10	Falhas na análise da qualificação técnica dos licitantes	2 (Provável) Processos de habilitação complexos e passíveis de erro	3 (Alto) Contratação inadequada, impacto na qualidade dos serviços
R11	Ausência de monitoramento contínuo e efetivo dos serviços contratados	2 (Provável) Dificuldade de fiscalização técnica em SaaS/SOC	3 (Alto) Vulnerabilidades não detectadas, falhas de controle
R12	Inadimplência contratual com relação a requisitos técnicos e de segurança da informação	1 (Pouco provável) Cláusulas contratuais e penalidades bem estabelecidas	3 (Alto) Paralisação ou redução de eficiência operacional
R13	Comunicação falha entre gestor, fiscal e fornecedor	2 (Provável) Gestão complexa, múltiplos atores	2 (Médio) Ruídos, atrasos ou desentendimentos na execução
R14	Defasagem tecnológica durante a vigência do contrato	2 (Provável) Evolução rápida das tecnologias SaaS/SOC	3 (Alto) Solução torna-se obsoleta, demanda aditivos ou troca
R15	Falta de capacitação contínua da equipe operacional	2 (Provável) Rotatividade e desatualização	2 (Médio) Redução de eficiência e

		recorrente na área técnica	controle dos serviços
R16	Riscos de incidentes de exfiltração de dados/transgressão à LGPD	2 (Provável) Incidentes de segurança e privacidade ocorrem no setor	3 (Alto) Sanções, prejuízo grave ao usuário/instituição
R17	Riscos de integração/API entre sistemas SaaS/SOC	2 (Provável) Complexidade técnica, múltiplos ambientes interoperáveis	2 (Médio) Interrupção parcial de serviços, afetando processos

3.

MEDIDAS MITIGATÓRIAS

3.1.

A tabela a seguir detalha as medidas mitigatórias para os principais riscos identificados:

ID	Risco Identificado	Medidas Mitigatórias
R01	Definição incompleta ou inadequada dos requisitos técnicos e de negócio, afetando especificações do edital	Elaboração detalhada dos requisitos técnicos e validação intersetorial; exigência de integração e certificações SaaS/SOC.
R02	Estimativas incorretas dos quantitativos e do orçamento para contratação	Realizar levantamento orçamentário criterioso e reserva técnica para ajuste de valores
R03	Subdimensionamento dos riscos cibernéticos (ameaças emergentes, IA, ransomware, DDoS)	Atualização frequente do mapeamento de ameaças (inteligência, ransomware, novas técnicas – IA).
R04	Falta de alinhamento com os normativos legais e regulatórios aplicáveis, como LGPD e legislação específica	Monitoramento legal permanente; consulta à LGPD e demais normas federais/estaduais; exigência de compliance contratual.
R05	Insuficiência no Estudo Técnico Preliminar	Desenvolver Estudo Técnico Preliminar robusto e revisar periodicamente antes da publicação do edital
R06	Seleção de fornecedor com capacidade técnica insuficiente (certificações, equipe qualificada e ferramentas)	Exigência de certificações internacionais (ISO 27001, 27701, 20000, 9001), comprovação de experiência e habilitação técnica.
R07	Critérios de julgamento inadequados	Critérios claros e alinhados ao Termo de Referência;

	(propostas fora do escopo, preço baixo sem aderência)	julgamento objetivo/tecnicamente motivado.
R08	Fraudes e irregularidades no processo licitatório	Adoção de mecanismos de transparência (publicidade em canais oficiais, auditoria periódica).
R09	Falhas de publicidade e transparência	Adoção de mecanismos de transparência (publicidade em canais oficiais, auditoria periódica).
R10	Falhas na análise da qualificação técnica dos licitantes	Análise rigorosa da documentação; entrevistas técnicas se aplicável; exigência de atestados.
R11	Ausência de monitoramento contínuo e efetivo dos serviços contratados	Implantar monitoramento ininterrupto, com indicadores e alertas para detecção precoce dos incidentes
R12	Inadimplência contratual com relação a requisitos técnicos e de segurança da informação	Penalidades contratuais em caso de inadimplemento; auditoria periódica contratual
R13	Comunicação falha entre gestor, fiscal e fornecedor	Estabelecer canais formais de comunicação entre as partes e realizar reuniões periódicas de alinhamento
R14	Defasagem tecnológica durante a vigência do contrato	Prever atualizações tecnológicas contratuais e cláusulas de renegociação para inovação
R15	Falta de capacitação contínua da equipe operacional	Programas de treinamento e capacitação regular para todos envolvidos.
R16	Riscos de incidentes de exfiltração de dados/transgressão à LGPD	Geração de relatórios mensais de incidentes, medidas de prevenção contra exfiltração, validação de conformidade LGPD, uso de frameworks MITRE ATT&CK, NIST e SANS.
R17	Riscos de integração/API entre sistemas SaaS/SOC	Testes regulares de integração, manutenção de

	documentação técnica e registro de problemas/incidentes em plataforma ITSM integrada.
--	---

4. ACOMPANHAMENTO DAS AÇÕES DE TRATAMENTO DE RISCOS

4.1. O acompanhamento será realizado por revisões periódicas e auditorias internas pelo Departamento de TI, com relatórios de conformidade, indicadores específicos e reuniões de monitoramento com os responsáveis das áreas afetadas.

4.2. Caso detectado desvio, serão recomendadas ações corretivas alinhadas às melhores práticas de governança, jurisprudência TCU e políticas de segurança institucional..

5. NORMATIVOS

- Lei 14.133/2021 e Decreto Estadual nº 11.363/2023;
- Manual de Gestão de Riscos do TCU (2ª ed., 2020);
- Código das Melhores Práticas do IBGC (2023);
- ISO 31000/2009 – Gestão de Riscos;
- Frameworks: NIST, MITRE ATT&CK, SANS, LGPD.

Elaborado por:
DIVISÃO DE PROJETOS - DIPROJ

Requisitante:
ISRAEL JORDÃO SANTOS DE MELO
Chefe do Departamento de Tecnologia da Informação
Portaria nº 13/2023

Aprovado por:
JOSÉ AMARÍSIO FREITAS DE SOUZA
Secretário de Estado da Fazenda

REFERÊNCIAS:

1. **BRASIL**. Tribunal de Contas da União. *Manual de gestão de riscos do TCU: um passo para a eficiência*. 2. ed. Brasília, DF: TCU, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/outros-documentos-externos/tcu_manual_gestao_riscos.pdf/view.
2. **BRASIL**. Lei nº 14.133, de 1º de abril de 2021. Institui a nova Lei de Licitações e Contratos Administrativos. Diário Oficial da União: seção 1, Brasília, DF, 1 abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14133.htm.
3. **BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
4. **INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA – IBGC**. *Código das Melhores Práticas de Governança Corporativa*. 6. ed. São Paulo: IBGC, 2023. 80 p. ISBN 978-65-5515-787-1. Disponível em: <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640>
5. **INTERNATIONAL ORGANIZATION FOR STANDARDIZATION**. ISO 31000:2009 – *Risk management: principles and guidelines*. Geneva: ISO, 2009.
6. **INTERNATIONAL ORGANIZATION FOR STANDARDIZATION**. ISO 31000:2009 - *Risk management: Principles and guidelines*. Geneva: ISO, 2009.
7. **MITRE CORPORATION**. ATT&CK® Framework. Bedford, MA: MITRE, 2023. Disponível em: <https://attack.mitre.org/>.
8. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD: NIST, 2018. Disponível em: <https://www.nist.gov/>.



Documento assinado eletronicamente por **ZANIR NILSON DO NASCIMENTO DUARTE, Chefe de Divisão**, em 14/11/2025, às 00:20, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **ISRAEL JORDAO SANTOS DE MELO, Chefe(a) de Departamento**, em 14/11/2025, às 09:43, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0018199899** e o código CRC **31689C6D**.

Referência: Processo nº 0715.007435.00055/2025-41

SEI nº 0018199899

Referência: Processo nº 0715.007435.00055/2025-41

SEI nº 0019007720