Principal Instituição Financeira de fomento do Governo Federal na Região Amazônica, tem como missão promover o desenvolvimento sustentável da Amazônia, por meio da execução de políticas públicas e oferta de produtos e serviços financeiros.

O Banco da Amazônia S.A. reconhece seu papel no resgate da importância da Região para o desenvolvimento de sua gente e contribuição para um país melhor, mais justo e equânime.

Na qualidade de Agente Financeiro para a implementação das políticas creditícias para a Região, o que norteia nossos relacionamentos é a busca do bem-estar de todos que compõem a comunidade em que atuamos.

Apresentarmo-nos a essa comunidade implica estabelecer e divulgar padrões que orientam nossas ações, ora expressas em nosso Código de Ética.

MISSÃO

Desenvolver uma Amazônia Sustentável com crédito e soluções eficazes.

VISÃO

Ser o principal Banco de desenvolvimento da Amazônia, inovador com colaboradores engajados e resultados sólidos.

VALORES

- Transparência;
- Meritocracia;
- Ética;
- Valorização do cliente;
- Responsabilidade;
- Inovação;
- Diversidade.
- Sustentabilidade

CÓDIGO DE ÉTICA

O Código de Ética do Banco da Amazônia contém padrões baseados nos princípios da legalidade, probidade, impessoalidade e transparência, bem como, pelo respeito ao ser humano, presentes na Constituição Federal, no Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal e o Código de Conduta da Alta Administração Federal.

RELAÇÃO COM SEUS FORNECEDORES, PRESTADORES DE SERVIÇOS E OUTROS PARCEIROS

O Banco da Amazônia pauta seus relacionamentos com os fornecedores e prestadores de serviços orientado pelo compartilhamento dos padrões morais e éticos e com base na valorização de iniciativas sociais e ambientalmente responsáveis.

A seleção de fornecedores e prestadores de serviços é realizada com imparcialidade, transparência e preservação da qualidade e viabilidade econômica dos serviços prestados e dos produtos fornecidos, observados os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência dos atos administrativos.

O Banco da Amazônia, quando da contratação das empresas e seus empregados, respeita os princípios e os valores éticos fundamentais, a exemplo da honestidade, da cooperação, da disciplina, do compromisso, da confiança, da transparência, da igualdade e do respeito mútuo nas relações de trabalho.

ATENDIMENTO À LEGISLAÇÃO E ÀS NORMAS

O Banco da Amazônia exige e cumpre, em seu processo de contratação de bens e serviços, incluindo obras e serviços de engenharia, o atendimento à legislação vigente no País, em especial a Lei nº. Lei nº 13.303/2016 - Lei de Responsabilidade das Estatais, Decreto Federal nº 8.945/2016, Lei Complementar nº. 123/2006 - Estatuto da ME e EPP, subsidiariamente a Lei nº 14.133/2021 - Lei de Licitações e Contratos Administrativos, IN SEGES 73/2022, Decreto nº 11.462, de 31 de março de 2023 e do Regulamento de Licitações e Contratos do Banco da Amazônia (adiante denominado simplesmente “Regulamento”), de 28 de fevereiro de 2018, instituído pela Resolução nº 1/CA, de 26 de janeiro de 2018, atualizado pela Proposição CA Nº 2022/039 de 24.05.2022, dentre outras.

PACTO PELA ERRADICAÇÃO DO TRABALHO ESCRAVO

Em cumprimento do disposto legal, veda-se nos processos licitatórios a participação de empresas que mantenham em seus quadros trabalhadores em condições análogas à de escravo.

Ademais, o Banco explicita em cláusula específica, nos contratos com fornecedores, Termo de Parceria, Acordos, Convênios e demais instrumentos contratuais, o combate ao trabalho em condições análogas à de escravo.

Assim, não é permitida a contratação ou manutenção de contratos com fornecedores que tenham sido autuados por manterem trabalhadores em condições análogas à de escravidão.

PACTO PELA ERRADICAÇÃO DO TRABALHO INFANTIL

O Banco da Amazônia observa os direitos fundamentais no trabalho definidos pelas convenções e declarações da Organização Internacional do Trabalho (OIT) sobre os Princípios e Direitos Fundamentais no Trabalho, Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e outras leis, normas e resoluções contra o trabalho infantil.

COMBATE À CORRUPÇÃO EM TODAS AS SUAS FORMAS

Na realização de seus negócios, o Banco da Amazônia observa os princípios éticos organizacionais consubstanciados em seu Código de Conduta Ética, Estatuto Social, normas e regulamentos internos da área de Gestão de Pessoas e legislação aplicável.

PLANOS DE APLICAÇÃO DE RECURSO

Os Planos de Aplicação de Recursos elaborados pelo Banco da Amazônia representam importantes ferramentas estratégicas na condução da política de crédito da Instituição e são concebidos em alinhamento com as políticas e programas do Governo Federal para a Amazônia e prioridade nos nove Estados da Região Amazônica.

A finalidade precípua dos Planos de Aplicação é a de orientar a atuação do Banco da Amazônia na Região, visando o alcance da máxima eficiência na alocação dos recursos sob sua gestão e, assim, cumprir com o nobre papel institucional de promover o desenvolvimento regional em bases sustentáveis, contribuindo para a inclusão social, a redução da pobreza, a melhoria da qualidade de vida das populações locais e a minimização das desigualdades inter e intrarregionais.

ADOÇÃO DE CRITÉRIOS DE SUSTENTABILIDADE NAS COMPRAS E CONTRATAÇÕES DO BANCO DA AMAZÔNIA

Nos editais e minutas de contratos em geral, o Banco da Amazônia preza pelo atendimento da legislação que recomenda a adoção de critérios de sustentabilidade nas especificações dos bens a serem fornecidos e a exigência de práticas sustentáveis por parte das empresas na execução dos serviços, mormente o Decreto nº 7.746/2012 e a Instrução Normativa SLTI nº 1/2010, e demais dispositivos legais pertinentes à matéria. Destarte, desde que justificável e preservado o caráter competitivo do certame, as licitações promovidas pelo Banco seguem as diretrizes de sustentabilidade expressas no art. 4º daquele Decreto, a saber:

- menor impacto sobre recursos naturais como flora, fauna, ar, solo e água;
- preferências para materiais, tecnologias e matérias-primas de origem local;
- maior eficiência na utilização de recursos naturais como água e energia;
- maior geração de empregos, preferencialmente com mão de obra local;
- maior vida útil e menor custo de manutenção do bem e da obra;
- uso de inovações que reduzam a pressão sobre recursos naturais; e
- origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

Como consequência, nos instrumentos convocatórios que tenham por objeto o fornecimento de bens, por exemplo, constatada a presença dos requisitos referentes à justificativa e à competitividade referidos no parágrafo anterior, são incluídos critérios de sustentabilidade, os quais passam a integrar as especificações técnicas dos bens.

No que se refere aos contratos, dentre as obrigações gerais do contrato consta exigência da adoção de práticas de sustentabilidade na execução dos serviços, de modo a prevenir ações danosas ao meio ambiente, em observância à legislação vigente, principalmente no que se refere aos crimes ambientais, contribuindo para a manutenção de um meio ambiente ecologicamente equilibrado. Adicionalmente, também é obrigação do contratado orientar e capacitar os prestadores de serviços, fornecendo informações necessárias para a perfeita execução dos serviços, incluindo noções de responsabilidade socioambiental.

Além da adoção dos critérios e práticas de sustentabilidade já mencionados, outros podem ser adotados conforme a natureza do objeto. Neste caso, as exigências e/ou obrigações referentes aos critérios e práticas de sustentabilidade são amoldadas às peculiaridades de cada objeto.

Diretoria Corporativa – DICOP

Gerência de Contratações e Gestão de Administração de Contratos - GECOG

Coordenadoria de Processos Licitatórios – COPOL

BANCO DA AMAZÔNIA S.A.

(SIASG: 179007)

Diretoria Corporativa

Gerente Executiva de Contratações e Gestão de Administração de Contratos

Coordenadoria de Processos Licitatórios

PREGÃO ELETRÔNICO N. 90029/2026

1. DISPOSIÇÕES PRELIMINARES

1.1. O BANCO DA AMAZÔNIA S.A., através de Pregoeiro designado pela **OS 2026/025,** torna público que realizará, nos termos em especial a Lei nº. Lei nº 13.303/2016 - Lei de Responsabilidade das Estatais, Decreto Federal nº 8.945/2016, Lei Complementar nº. 123/2006 - Estatuto da ME e EPP, se aplicando para a fase externa a Lei nº 14.133/2021 e Instrução Normativa nº 73 de 30 de setembro de 2022, no que couber, e do Regulamento de Licitações e Contratos do Banco da Amazônia (adiante denominado simplesmente "Regulamento"), de 28 de fevereiro de 2018, instituído pela Resolução nº 1/CA, de 26 de janeiro de 2018, atualizado pela Proposição CA Nº 2022/039 de 24.05.2022, dentre outras, licitação na modalidade Pregão Eletrônico, critério de julgamento **menor preço global**, em único lote, para Contratação de empresa especializada para prestação de Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center (CFC), compreendendo a disponibilização, implementação, integração, operação, sustentação e evolução contínua de solução integrada que contemple, de forma indissociável, as capacidades de Monitoramento e Resposta a Incidentes e Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), em regime de alta disponibilidade 24x7x365, incluindo Serviços Técnicos Especializados e capacitação técnica sob demanda, pelo período de 60 (sessenta) meses, **conforme especificações do termo de referência** e condições estabelecidas neste Edital.

Data da sessão pública de abertura: 17/11/2026.
Horário: 10h (horário de Brasília-DF).
Local: www.gov.br/compras.
Modo de disputa: Aberto.
Critério de julgamento: Menor preço Global em Lote único.
Forma de adjudicação: Global.
Regime de execução: Fornecimento contínuo.
Garantia contratual: 5% (cinco por cento) do preço global contratado.
Participação exclusiva de ME/EPP: Não.
Participação de consórcio: Sim.
Numero da contrataçao SIASG: 15/2026

1.2. O pregão eletrônico será realizado em sessão pública, no sistema de licitações COMPRASNET do Portal de Compras do Governo Federal (https://www.gov.br/compras) por meio da internet, mediante condições de segurança - criptografia e autenticação em todas as suas fases.

1.3. As datas e horários das etapas da licitação estão definidos na respectiva página da licitação (https://www.gov.br/compras) e no site do Banco da Amazônia (www.bancoamazonia.com.br). As datas e horários poderão sofrer alterações de acordo com os aditamentos feitos ao Edital. Cabe à proponente o acompanhamento permanente das possíveis alterações.

1.4. Os trabalhos serão conduzidos por empregado do Banco da Amazônia, denominado Pregoeiro, devidamente designado conforme documentos constantes do processo.

2. OBJETO

2.1. Constitui objeto da presente licitação a Contratação de empresa prestação de Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center (CFC), compreendendo a disponibilização, implementação, integração, operação, sustentação e evolução contínua de solução integrada que contemple, de forma indissociável, as capacidades de Monitoramento e Resposta a Incidentes e Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), em regime de alta disponibilidade 24x7x365, incluindo Serviços Técnicos Especializados e capacitação técnica sob demanda, pelo período de 60 (sessenta) meses.

2.2. Como parte integrante do escopo técnico dos Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, a solução deverá contemplar, de forma obrigatória, a implementação, o licenciamento, a operação contínua e a integração nativa de todos os itens descritos na tabela abaixo, devendo operar de forma unificada, coordenada e indissociável, sob responsabilidade integral da CONTRATADA, sendo vedada a prestação isolada de quaisquer componentes que façam parte dos itens ou a dependência de integrações externas que comprometam a efetividade da solução como um todo.

2.3. Esta Licitação será realizada em lote único, porém em sua proposta, a licitante deverá detalhar os preços unitários de cada item, conforme abaixo, em conformidade com as especificações contidas no Termo de Referência e anexos deste Edital:

	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	Mês	60
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	Mês	60
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	Mês	60
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	Serviço	1
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	UST	5.000
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	Turma	3 (com 15 participantes cada)
Obs.:	**** Regime contínuo de 24x7x365.***		
	***** Sob demanda, a critério do Banco, mediante Ordem de Serviço.***		

3. RECURSOS ORÇAMENTÁRIOS

3.1. Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto desta licitação estão previstos no orçamento de investimento do Banco da Amazônia:

ITEM	DESCRIÇÃO	RUBRICA
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	82.559-0
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	82.543-3
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	82.559-0
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	82.548-4
Obs.:	** Regime contínuo de 24x7x365.*	
	*** Sob demanda, a critério do Banco, mediante Ordem de Serviço.*	

4. REFERÊNCIA DE TEMPO

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

5. CONDIÇÕES PARA PARTICIPAÇÃO

5.1. Poderão participar da presente licitação interessados:

5.1.1. qualquer pessoa física ou jurídica legalmente estabelecida no País, cujo ramo de atividade seja compatível com o objeto da licitação e que atenda às exigências deste Edital e seus anexos.

5.1.2. Que estejam previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores – Sicaf e no Portal de Compras do Governo Federal (www.gov.br/compras);

5.2. Não poderão participar da presente licitação as pessoas, físicas ou jurídicas, que, direta ou indiretamente, enquadrem-se nas seguintes hipóteses de vedação:

5.2.1. referidas nos artigos 38 e 44 da Lei n. 13.303/2016; que estejam cumprindo penalidade que as impeça de licitar e contratar com o Banco da Amazônia, nomeadamente:

a) suspensão temporária de participação em licitação e impedimento, nos termos do inciso III do artigo 83 da Lei n. 13.303/2016, aplicada pelo Banco da Amazônia;

b) impedimento de licitar e contratar, previsto no inciso III do art. 83 da lei 13.303/2016;

declaração de inidoneidade, prevista na Lei e no Regulamento do Banco, aplicada por qualquer órgão ou entidade integrante da Administração Pública nacional, ou a prevista no artigo 46 da Lei n. 8.443/1992, aplicada pelo Tribunal de Contas da União;

c) proibição de contratar com o Poder Público prevista nos incisos do artigo 12 da Lei n. 8.429/1992;

5.2.2. Para fins das vedações explicitadas neste subitem, considera-se participação indireta a existência de vínculos de natureza técnica, comercial, econômica, financeira ou trabalhista entre o autor do Termo de Referência, pessoa física ou jurídica, e o proponente ou responsável pelos fornecimentos de bens, prestação de serviços ou execução de obras, incluindo-se os fornecimentos de bens e serviços a estes necessários.

5.2.3. A vedação deste item aplica-se a empregados incumbidos de levar a efeito atos e procedimentos realizados pelo Banco da Amazônia no curso da licitação.

5.2.4. 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;

5.2.5. 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;

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

5.3. Para os fins desta licitação, os impedimentos referidos neste Edital serão verificados perante o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP) e outros sistemas cadastrais pertinentes que sejam desenvolvidos e estejam à disposição para consulta, conforme o caso.

5.4. Será admitida a participação de empresas reunidas em consórcio, observadasas condiçoes estabelecidas no Edital, na lei 13.303/2016 e no Regulamento de Licitações e Contratos do Banco da Amazônia.

5.5. O proponente poderá participar do procedimento licitatório por intermédio de sua matriz ou filial, desde que cumpra as condições exigidas para habilitação e credenciamento, em relação ao estabelecimento com o qual pretenda participar do certame.

5.5.1. O CNPJ do estabelecimento que participar do certame, matriz ou filial, deverá ser o mesmo a constar no contrato com o Banco da Amazônia e nas Notas Fiscais/Faturas emitidas, quando do fornecimento ou execução dos serviços contratados. Dessa forma, não será admitida a emissão de Notas Fiscais/Faturas por CNPJ de estabelecimento diverso daquele participante da Licitação.

5.6. Esta licitação é de âmbito nacional.

6. CADASTRO, ACESSO E UTILIZAÇÃO DO SISTEMA DE LICITAÇÕES

6.1. Os interessados em participar da licitação deverão possuir cadastro no COMPRASNET do Portal de Compras do Governo Federal (https://www.gov.br/compras), dispondo de chave de identificação e senha de acesso ao sistema.

6.1.1. A chave de identificação e a senha são pessoais e intransferíveis, terão validade de 1 (um) ano e poderão ser utilizadas em qualquer licitação eletrônica, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco da Amazônia, devidamente justificada.

6.1.2. A perda da senha ou a quebra de sigilo deverão ser comunicadas ao provedor do sistema para imediato bloqueio de acesso.

6.1.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais 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

6.2. A cadastrado será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, declarando e assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao Banco da Amazônia responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

6.2.1. O cadastro da proponente e de seu representante legal junto ao sistema eletrônico implica responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes à licitação eletrônica.

6.3. O acesso ao sistema se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecido.

6.4. Caberá à proponente acompanhar as operações no sistema, antes, durante e após a sessão pública de lances, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.5. A proponente deverá comunicar imediatamente qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso.

7. PROCEDIMENTO DA LICITAÇÃO

7.1. A presente licitação será conduzida pelo Pregoeiro, que pode ser auxiliado por equipe de apoio ou por técnicos especializados, de acordo com as seguintes fases e procedimento:

a) publicação do Edital;

b) credenciamento no sistema de licitações;

c) eventual pedido de esclarecimento ou impugnação;

d) resposta motivada sobre o eventual pedido de esclarecimento ou impugnação;

e) cadastramento da proposta no sistema de licitações;

f) apresentação de propostas e lances;

g) verificação de efetividade dos lances ou propostas;

h) negociação;

i) Prova de Conceito;

j) julgamento;

k) habilitação;

l) declaração de vencedor;

m) interposição de recurso;

n) adjudicação e homologação.

8. CONSULTAS, ESCLARECIMENTOS E IMPUGNAÇÃO

8.1. Cidadãos e agentes econômicos poderão pedir esclarecimentos e impugnar o Edital, no prazo de até 3 (três) dias úteis antes da data fixada para a ocorrência do certame, em requerimento escrito que deve ser formulado e encaminhado para o e-mail de licitacoes@basa.com.br.

8.1.1. O documento deve estar, obrigatoriamente, em formato passível de cópia (Pdf editável, Word, Libreoffice, etc), permitindo a transferência/colagem de seu conteúdo para o sistema eletrônico da licitação.

8.1.2. Não serão conhecidos os pedidos de esclarecimentos e impugnações apresentados intempestivamente e/ou subscritos por representante não habilitado legalmente ou não identificado no processo para responder pela impugnante.

8.1.3. Ao receber pedido de esclarecimentos ou impugnação, o Pregoeiro deverá remetê-lo imediatamente à unidade instrutora, para que ofereça resposta motivada.

8.2. Os esclarecimentos e impugnações serão decididos e respondidos pelo Pregoeiro no prazo de 03 (três) dias úteis e devidamente publicados no sítio eletrônico oficial, **(https://www.gov.br/compras/pt-br),** limitado ao último dia útil anterior à data da abertura do certame, para ciência de todas as proponentes.

8.2.1. Acaso os pedidos de impugnação e esclarecimentos não sejam respondidos até o dia útil anterior à data da sessão pública, a abertura da licitação deverá ser adiada, de modo que seja respeitado o prazo de intervalo entre a data da resposta ao pedido de impugnação e esclarecimentos e a abertura da licitação.

8.2.2. A decisão de adiamento da abertura da licitação prevista no subitem anterior e a remarcação de sua abertura é de competência do Pregoeiro e deverá ser publicada no **sistema de licitações COMPRASNET do Portal de Compras**

do Governo Federal (https://www.gov.br/compras/pt-br).

8.3. Somente terão validade, esclarecimentos prestados por intermédio do Pregoeiro, disponibilizados na forma deste subitem.

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

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

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

8.7. O proponente, através de consulta permanente, deverá manter-se atualizado quanto a quaisquer alterações e esclarecimentos sobre o Edital, não cabendo ao Banco da Amazônia a responsabilidade por desconhecimento de tais informações, em face de inobservância do proponente quanto ao procedimento apontado neste subitem.

9. APRESENTAÇÃO DA PROPOSTA NO SISTEMA DE LICITAÇÕES

9.1. O proponente encaminhará, exclusivamente por meio do sistema, sua proposta comercial, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio de proposta.

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

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

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

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

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

9.2.5. A declaração falsa sujeitará a proponente às sanções previstas neste Edital e na legislação.

9.3. O proponente deverá encaminhar sua proposta preenchendo o campo específico no sistema de licitações.

9.3.1. O preenchimento da proposta, bem como a inclusão de seus anexos, no sistema de licitações é de exclusiva responsabilidade do proponente, não cabendo ao Banco da Amazônia qualquer responsabilidade.

9.3.2. Até a data e hora definidas para abertura das propostas, o proponente poderá retirar ou substituir a proposta anteriormente apresentada.

9.3.3. No sistema, deverá ser cotado preço unitário, contendo no máximo 02 (duas) casas decimais, sem arredondamentos. No preço cotado, deverão incluir todos os custos e despesas, tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucro, uniformes, alimentação, transporte, plano de assistência médico-hospitalar e odontológica e outros necessários ao cumprimento integral do objeto.

9.3.4. Apesar de no item anterior informar da forma de cadastramento do preço da proposta no sistema, quando do envio da proposta formal solicitada pelo Pregoeiro, o licitante deverá informar o preço global de acordo com o modelo do ANEXO II (CARTA PROPOSTA)

9.3.5. O proponente microempresa ou empresa de pequeno porte optante do Simples Nacional deve indicar a alíquota de imposto incidente com base no faturamento acumulado dos últimos 12 meses anteriores.

9.3.6. Quando o objeto licitado estiver enquadrado em algumas das vedações previstas no artigo 17 da Lei Complementar n. 123/2016, os proponentes microempresas ou empresas de pequeno porte que forem optantes do Simples Nacional deverão formular suas propostas desconsiderando os benefícios tributários do regime a quem fazem jus.

9.3.7. O prazo de validade das propostas será de 60 (sessenta) dias, contados da data da sessão pública e apresentação das propostas, podendo vir a ser prorrogado mediante solicitação do Banco da Amazônia e aceitação do proponente.

10. PROCEDIMENTO DA ETAPA COMPETITIVA, MODO DE DISPUTA E CRITÉRIO DE JULGAMENTO

10.1. A presente licitação ocorrerá em sessão pública, por meio de sistema eletrônico e será conduzida pelo Pregoeiro, iniciado na data e hora designados neste Edital e, em caso de suspensão, sua continuidade se dará nos termos indicados em comunicado formal subsequente.

10.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

10.2.1. Também será desclassificada a proposta que identifique o proponente.

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

10.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

10.3. Aberta a sessão pública, os proponentes que atenderem às condições do presente Edital poderão participar da etapa competitiva.

10.3.1. O sistema ordenará automaticamente as propostas classificadas, permitindo que os proponentes encaminhem seus lances exclusivamente por meio do sistema eletrônico.

10.3.2. Será permitida a apresentação de lances intermediários, assim considerados iguais ou superiores ao menor lance ofertado, mas inferior ao último lance dado pelo próprio proponente.

10.3.3. O lance deverá ser ofertado pelo **valor global para 60 meses**.

10.3.4. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser **R$ 5.000,00 (cinco mil reais).**

10.3.5. Durante o transcurso da sessão pública, os proponentes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do proponente.

10.3.6. Durante a sessão, quando necessário, o Pregoeiro disponibilizará campo próprio para troca de mensagens com os proponentes, vedada qualquer interação entre estes diretamente.

10.3.7. Se por algum motivo a sessão de disputa não puder ser realizada na data e horário previstos, os participantes deverão ficar atentos à nova data e horário que serão disponibilizados no sistema eletrônico em que se realizará a sessão pública e no sítio eletrônico do Banco da Amazônia.

10.3.8. No caso de desconexão do Pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível às proponentes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

10.3.9. Quando a desconexão do Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão da licitação eletrônica será suspensa e reiniciada somente após comunicação aos participantes.

10.4. Na etapa competitiva, o procedimento seguirá de acordo com o modo de disputa adotado.

10.5. A etapa competitiva será realizada pelo modo de disputa aberta, que apresentarão lances sucessivos e públicos, com prorrogações:

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

10.5.2. prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver

lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

10.5.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

10.5.4. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

10.5.5. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia.

10.5.6. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

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

10.5.8. Durante o transcurso da Sessão Pública, os LICITANTEs serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais LICITANTEs, vedada a identificação do detentor do lance.

10.6. A presente licitação será julgada pelo critério do Menor preço Global, considerando o valor global estimado, nos termos do item 1 do artigo 65 do Regulamento.

11. DIREITO DE PREFERÊNCIA PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

11.1. Para esta licitação, **não haverá a aplicação do tratamento diferenciado** previsto na Lei Complementar nº 123/2006, tendo em vista que o valor estimado do lote supera o limite legal de faturamento bruto anual das Empresas de Pequeno Porte (EPP), fixado no artigo 3º, inciso II, da referida lei.

12. DESEMPATE

12.1. Nas licitações em que, após o exercício de preferência, esteja configurado empate em primeiro lugar, deverá ser realizada disputa final entre os proponentes empatados, que poderão apresentar nova proposta fechada, em prazo definido pelo Pregoeiro.

12.2. Persistindo o empate, deverá ser dada preferência, sucessivamente, às propostas que tenha por objeto bens e serviços:

a) produzidos ou prestados por empresas brasileiras;

b) produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País; e,

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

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

12.3. Persistindo o empate, deverá ser realizado sorteio.

13. VERIFICAÇÃO DA EFETIVIDADE DA PROPOSTA E DO JULGAMENTO

13.1. O proponente autor da melhor proposta deverá apresentar, no prazo de 2(duas) horas, podendo ser prorrogado a critério do Pregoeiro, sua proposta final devidamente preenchida na forma do Anexo II – Modelo de Proposta de Preços, em arquivo único com o valor equalizado ao seu último lance ofertado, por meio da opção "Enviar Anexo" no sistema **www.gov.br/compras,** em que deve constar, conforme o caso:

a) indicação dos quantitativos e dos custos unitários;

b) composição dos custos unitários; e

c) detalhamento das Bonificações e Despesas Indiretas (BDI) e dos encargos sociais.

d) acaso o proponente seja microempresa ou empresa de pequeno porte optante do Simples Nacional, deverá indicar a alíquota de imposto incidente com base no faturamento acumulado dos últimos 12 meses anteriores.

13.2. Juntamente com a proposta, deverão ser encaminhados as seguintes declarações:

13.2.1. Declaração de que tem conhecimento do teor do Decreto nº 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da administração pública federal;

13.2.2. Declaração de que atende o art. 38 da Lei nº 13.303/2016;

13.2.3. Declaração de conhecimento do teor da Lei de Improbidade Administrativa (Lei nº 8.429/1992) e a Lei nº 12.846/13 e seus regulamentos (em conjunto, "Leis Anticorrupção");

13.3. O Pregoeiro deverá avaliar se a proposta melhor classificada atende às especificações técnicas, demais documentos e formalidades exigidas neste Edital, ocasião em que será subsidiado pela unidade especificadora no que se referir ao atendimento das questões técnicas relacionadas ao objeto da licitação ou de documentos com informações de ordem técnica que podem impactar a sua execução.

13.4. O Pregoeiro deverá desclassificar as propostas que apresentem preços manifestamente inexequíveis, assim considerados aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida.

13.4.1. A inexequibilidade dos valores referentes a itens isolados da planilha de custos, desde que não contrariem instrumentos legais, não caracterizarão motivo suficiente para a desclassificação da proposta.

13.4.2. A análise de exequibilidade da proposta não deverá considerar materiais e instalações a serem fornecidos pelo proponente em relação aos quais ele renuncie

à parcela ou à totalidade da remuneração, desde que a renúncia esteja expressa na proposta.

13.4.3. O Pregoeiro poderá realizar diligências para aferir a exequibilidade ou qualquer outro aspecto da proposta.

13.4.4. O Pregoeiro poderá exigir do proponente, sob pena de desclassificação, documentos que contenham indicação dos preços de insumos (tais como composições de custos ou propostas de terceiros), dos salários e remunerações (tais como acordos, convenções e sentença coletivas, tabelas de honorários profissionais ou contratos de prestação de serviços) e outras informações pertinentes (tais como notas fiscais de insumos ou outros contratos de serviços similares), que sejam capazes de demonstrar a exequibilidade da sua proposta.

13.4.5. Qualquer proponente poderá requerer motivadamente que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

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

13.5. O Pregoeiro deverá desclassificar, em decisão motivada, apenas as propostas que contenham vícios insanáveis, observando-se o seguinte:

13.5.1. São vícios sanáveis, entre outros, os defeitos materiais atinentes à descrição do objeto da proposta e suas especificações técnicas, incluindo aspectos relacionados à execução do objeto, às formalidades, aos requisitos de representação, às planilhas de composição de preços, e, de modo geral, aos documentos de conteúdo declaratório sobre situações pré-existentes, desde que não alterem a substância da proposta.

13.5.2. O Pregoeiro não deverá permitir o saneamento de defeitos em propostas apresentadas com má-fé ou intenção desonesta, como aqueles contaminados por falsidade material ou intelectual ou que tentem induzir o Pregoeiro a erro.

13.5.3. O Pregoeiro deverá conceder prazo adequado, para que o proponente corrija os defeitos de sua proposta.

13.5.4. O Pregoeiro deverá indicar expressamente quais aspectos da proposta ou documentos apresentados junto à proposta devem ser corrigidos.

13.5.5. A correção dos defeitos sanáveis não poderá importar alteração do valor final da proposta, exceto para oferecer preço mais vantajoso para o Banco da Amazônia.

13.5.6. Se a proposta não for corrigida de modo adequado, o Pregoeiro poderá conceder novo prazo para novas correções.

13.6. O Pregoeiro poderá negociar com o proponente autor da melhor proposta condições mais vantajosas, que poderão abranger os diversos aspectos da proposta, desde preço, prazos de pagamento e de entrega, sem que lhe caiba, a pretexto da

negociação, relativizar ou atenuar as exigências e condições estabelecidas no Edital e nos seus documentos anexos.

13.6.1 O Pregoeiro poderá, de acordo com sua análise de conveniência e oportunidade, divulgar o orçamento do Banco da Amazônia para efeito de negociação.

13.6.2 O valor global da proposta, após a negociação, não poderá superar o orçamento estimado pelo Banco da Amazônia, sob pena de desclassificação do proponente.

14 HABILITAÇÃO

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

14.2 O proponente autor da melhor proposta, aceita pelo Pregoeiro, deve apresentar os documentos de habilitação exigidos neste item do Edital em formato digital, no prazo de até
2 (duas) horas prorrogável por decisão do Pregoeiro, por meio do SICAF ou por funcionalidade disponível no próprio sistema da licitação enviados por meio da opção "Enviar Anexo" do sistema www.gov.br/compras.

14.2.1 A prorrogação de prazo de envio da documentação somente poderá ocorrer por solicitação da licitante, mediante justificativa aceita pelo Pregoeiro; ou de ofício, a critério do Pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no Edital para a verificação de conformidade.

14.3 Por ocasião do início da fase de habilitação, o pregoeiro realizará as consultas relacionadas a seguir, a fim de comprovar a inexistência de registros impeditivos da contratação do licitante ou de sua participação neste certame:

14.3.1 Consulta ao SICAF, com vistas a verificação da composição societária do licitante, de modo a verificar a existência de ocorrências impeditivas diretas ou indiretas relativas ao licitante, além de confirmar a existência de licitantes integrantes de um mesmo grupo econômico;

14.3.2 portal eletrônico do Tribunal de Contas da União (TCU), disponível no endereço https://certidoes-apf.apps.tcu.gov.br/, o qual consolida as pesquisas relativas aos seguintes cadastros:

14.3.2.1 Lista de inidôneos do TCU;

14.3.2.2 CNIA – Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade, mantido pelo Conselho Nacional de Justiça (CNJ);

14.3.2.3 CEIS – Cadastro Nacional de Empresas Inidôneas e Suspensas e CNEP – Cadastro Nacional de Empresas Punidas, mantidos pelo Portal da Transparência.

14.4 A Licitante deverá apresentar declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nasconvenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes

na data de entrega das propostas.

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

14.6 Caso os resultados das consultas previstas no item 14.3 evidenciem a existência de registros impeditivos à contratação do licitante, este será inabilitado, ou, inexistindo impedimentos à contratação, o pregoeiro passará a analisar a habilitação do proponente a partir dos seguintes parâmetros:

14.6.1 habilitação jurídica;

14.6.2 qualificação técnica;

14.6.3 capacidade econômica e financeira;

14.6.4 regularidade fiscal e trabalhista;

14.7 A verificação do atendimento pelo licitante dos parâmetros habilitatórios dar-se-á em conformidade com as seguintes fases:

14.7.1 habilitação parcial pelo SICAF;

14.7.2 análise da documentação complementar de habilitação, a qual deverá ser enviada após solicitação do pregoeiro, na forma deste edital.

14.8 A Habilitação parcial pelo sistema SICAF será verificada relativamente aos documentos abrangidos por aquele sistema.

14.9 a hipótese de falha no SICAF ou nos sítios oficiais, que impossibilite a confirmação da habilitação mencionada no item anterior, o(a) Pregoeiro(a) poderá por outros meios solicitar ao Licitante que envie a documentação necessária.

14.10 Os documentos exigidos para habilitação que não estejam contemplados no **SICAF** serão enviados por meio do sistema, em formato digital, no prazo estipulado pelo pregoeiro na forma do item 14.2.

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

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

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

HABILITAÇÃO JURÍDICA

14.14 A comprovação do atendimento ao parâmetro habilitação jurídica, caso o licitante não se encontre com o cadastramento atualizado no SICAF ou não tenha, pelo menos, registro regular nível “Habilitação Jurídica” do SICAF, consistirá na seguinte

documentação complementar conforme o caso:

14.14.1 Inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, no caso de empresário individual;

14.14.2 Certificado da Condição de Microempreendedor Individual – CCMEI, no caso de microempreendedor individual, cuja aceitação ficará condicionada à verificação de sua autenticidade no sítio www.portaldoempreendedor.gov.br;

14.14.3 Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores, no caso de sociedade empresária;

14.14.4 Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de o licitante ser sucursal, filial ou agência;

14.14.5 Inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores, no caso de sociedades simples;

14.14.6 Decreto de autorização, em se tratando de sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento expedido pelo órgão competente.

REGULARIDADE FISCAL E TRABALHISTA

14.15 A comprovação do atendimento ao parâmetro regularidade fiscal e trabalhista, caso o licitante não se encontre com o cadastramento atualizado no SICAF, consistirá na seguinte documentação complementar:

14.15.1 Prova de regularidade para com a Fazenda Federal, mediante apresentação de certidão expedida pela Secretaria da Receita Federal do Brasil – RFB ou Certidão Negativa ou Positiva com efeito de Negativa de Regularidade e pela Procuradoria-Geral da Fazenda Nacional – PGFN, referente a todos os tributos federais e à Dívida Ativa da União – DAU por elas administrados, incluindo as contribuições sociais e previdenciárias;

14.15.2 Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS;

14.15.3 Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com Efeito de Negativa.

14.15.3.1. Será considerada a CNDT ou Certidão Positiva de Débitos Trabalhistas com Efeito de Negativa mais atualizada, conforme entendimento do Tribunal Superior do Trabalho – TST.

14.15.4 Prova de regularidade para com a Fazenda Estadual e/ou Municipal mediante apresentação de certidão negativa de débitos fiscais ou Certidão Positiva de débitos fiscais com Efeito de Negativa, respectivamente.

QUALIFICAÇÃO TÉCNICA

14.16 A habilitação técnica consistirá na apresentação de, no mínimo, 01 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em

documento timbrado, e que comprove a aptidão da licitante para o desempenho de atividade pertinente e compatível em características e quantidade equivalentes com o objeto da presente licitação, equivalentes com o objeto da presente licitação, além dos documentos descritos no item 31 – DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA" do Termo de Referência, Anexo I desse Edital.

14.16.1 Serão aceitos quantos atestados forem necessários para a comprovação dos quantitativos através de sua soma.

14.16.2 Os atestados referir-se-ão a contratos já concluídos ou já decorrido no mínimo 01 (um) ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior, apenas aceito mediante a apresentação do contrato.

14.16.3 As licitantes disponibilizarão todas as informações necessárias à comprovação da legitimidade dos atestados apresentados.

14.16.4 Para a referida comprovação serão aceitos quantos atestados forem necessários para a comprovação dos quantitativos através de sua soma.

14.16.5 Somente será aceito o somatório de atestados de períodos concomitantes para comprovar a capacidade técnica;

14.16.6 O atestado de capacidade deverá se referir a serviços prestados no âmbito de sua atividade econômica principal ou secundária no contrato social vigente, devidamente registrado na junta comercial competente, bem como no cadastro de Pessoas Jurídicas da Receita Federal do Brasil;

14.16.7 Será admitida a utilização de atestados emitidos em nome de empresas incorporadas, desde que se comprove que houve transferência parcial de patrimônio e profissionais decorrente de reestruturação societária e que implique a transferência efetiva de qualificação técnica e operacional entre elas, atinentes ao acerto técnico transferido.

14.16.8 Os documentos de habilitação relativos ao parâmetro qualificação técnica serão encaminhados pelo pregoeiro à área técnica do Banco da Amazônia, com vistas à emissão de parecer acerca do atendimento dos requisitos exigidos;

14.16.9 Para fins de verificação da qualificação técnica, o licitante deverá disponibilizar, quando solicitadas pelo pregoeiro, todas as informações necessárias à comprovação do(s) atestado(s) de capacidade técnica apresentado(s), podendo, para tanto, o pregoeiro solicitar cópia do instrumento que deu suporte à contratação, informações sobre o endereço atual do contratante e local onde foram prestados os serviços, dentre outras informações que julgar necessárias.

CAPACIDADE ECONÔMICA E FINANCEIRA

14.17 O proponente deverá apresentar os seguintes documentos relativos à capacidade econômico-financeira:

14.17.1 balanço patrimonial e demonstrações contábeis referentes ao último exercício social, exigíveis na forma da lei, que comprove a boa situação financeira

por meio da satisfação de índices de liquidez geral (LG), liquidez corrente (LC), e solvência geral (SG) superiores a 1 (um), com indicação dos seus cálculos, que deverão ser realizados de acordo com as seguintes fórmulas:

$$LG = \frac{\text{ativo circulante + realizável a longo prazo}}{\text{passivo circulante + passivo não circulante}}$$

$$LC = \frac{\text{ativo circulante}}{\text{passivo circulante}}$$

$$SG = \frac{\text{ativo total}}{\text{passivo circulante + passivo não circulante}}$$

14.17.2 certidão negativa de feitos sobre falência da sede do interessado.

14.18 O proponente deverá comprovar que possui patrimônio líquido ou capital social equivalente a 10% (dez por cento) do valor total estimado da contratação.

14.19 As empresas constituídas no exercício em curso ou com menos de um ano deverão apresentar balanço de abertura e, no caso de empresas com movimentações, balanço intermediário, com a assinatura do administrador e do responsável por sua contabilidade, devidamente registrado e autenticado pelo órgão competente.

14.20 As empresas inativas no exercício anterior deverão apresentar as demonstrações contábeis do último exercício em que a empresa esteve ativa, certidão de inatividade correspondente ao período em que não realizou atividades e balanço de reabertura.

14.21 Serão considerados na forma da lei o balanço patrimonial e as demonstrações contábeis apresentados em uma das formas a seguir:

14.21.1 Disponibilizados via Escrituração Contábil Digital – ECD, desde que comprovada a transmissão desta à Receita Federal do Brasil, por meio da apresentação do Termo de Autenticação (recibo gerado pelo Sistema Público de Escrituração Digital – SPED);

14.21.2 Exemplar registrado ou autenticado pela Junta Comercial da sede do licitante, quando se tratar de empresa comercial, ou autenticado em Cartório de Registro Civil das Pessoas Jurídicas, se sociedade simples;

14.21.3 Transcrição do livro Diário, em que se comprove o registro pela Junta Comercial da sede do licitante, quando se tratar de empresa comercial, ou a autenticação em Cartório de Registro Civil das Pessoas Jurídicas, se sociedade simples, acompanhada, obrigatoriamente, de cópia autenticada dos Termos de Abertura e de Encerramento do respectivo livro;

14.21.4 Publicação em jornal de grande circulação ou em Diário Oficial.

14.22 O licitante que se encontrar em recuperação judicial ou extrajudicial deverá atender a todos os requisitos para comprovação da capacidade econômica e financeira, como os demais licitantes, e ainda apresentar:

14.22.1 Certidão emitida pela instância judicial competente, que ateste que o licitante está apto econômica e financeiramente a participar de procedimento licitatório nos termos da Lei nº 13.303/2016;

14.22.2 Comprovação do acolhimento judicial do plano de recuperação judicial ou da homologação judicial do plano de recuperação, no caso de recuperação extrajudicial.

BENEFÍCIOS ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

14.23 Microempresas e empresas de pequeno porte deverão atender a todas as exigências de habilitação previstas neste Edital.

14.24 As microempresas e empresas de pequeno porte, assim declaradas, na forma da lei, gozarão do tratamento diferenciado descrito a seguir:

14.24.1 As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação da regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição;

14.24.2 Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, o pregoeiro concederá o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogável por igual período, a critério do Banco, mediante apresentação de justificativa por parte do licitante, para regularidade da documentação, para pagamento ou parcelamento do débito e para emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

14.25 A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sendo facultado ao Banco convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

14.26 O Pregoeiro somente deverá inabilitar o proponente autor da melhor proposta em razão de defeitos em seus documentos de habilitação que sejam insanáveis, aplicando-se os mesmos procedimentos e critérios prescritos neste Edital para o saneamento de propostas, observando-se o seguinte:

14.26.1 consideram-se sanáveis defeitos relacionados a documentos que declaram situações pré-existentes ou concernentes aos seus prazos de validade;

14.26.2 o Pregoeiro poderá realizar diligência para esclarecer o teor ou sanar defeitos constatados nos documentos de habilitação;

14.26.3 o Pregoeiro, se for o caso de diligência, poderá conceder prazo de 2 (dois) dias úteis, prorrogável por igual período, para que o proponente corrija os defeitos constatados nos seus documentos de habilitação, apresentando, se for o caso, nova documentação;

14.26.4 o Pregoeiro, se for o caso de diligência, deverá indicar expressamente quais documentos devem ser reapresentados ou quais informações devem ser corrigidas;

14.26.5 se os defeitos não forem corrigidos de modo adequado, o Pregoeiro poderá conceder novo prazo para novas correções.

14.27 Constatado o atendimento às exigências de habilitação estabelecidas neste edital, o licitante será habilitado e, consequentemente, declarado vencedor.

14.28 Se o proponente desatender às exigências habilitatórias, o Pregoeiro examinará a documentação do proponente subsequente, e assim, sucessivamente, até a apuração de documentação que atenda os termos do Edital, cujo proponente será declarado vencedor.Se todos os proponentes forem desclassificados ou inabilitados, dada a constatação de defeitos insanáveis em todas as propostas apresentadas, o Pregoeiro deverá declarar a licitação fracassada.

15 RECURSOS

15.1 O processo licitatório, de que trata o presente edital, terá fase recursal única, a qual transcorrerá com o encerramento da fase de habilitação, atendidas as demais condições definidas neste item.

15.2 Declarado o vencedor, qualquer licitante poderá, durante o prazo concedido na sessão pública, no prazo de 30 minutos, de forma imediata após o julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema eletrônico, manifestar a sua intenção de recorrer.

15.2.1 A falta de manifestação imediata do proponente importará a decadência do direito de recurso, possibilitando a adjudicação do objeto da licitação ao licitante declarado vencedor.

15.2.2 As razões do recurso poderão trazer outros motivos não indicados expressamente na sessão pública.

15.2.3 As razões e contrarrazões de recursos, quando feitas, deverão ser enviadas em formato digital por meio eletrônico, preferencialmente por funcionalidade disponível no próprio sistema da licitação ou, na impossibilidade deste meio, por e- mail para licitacoes@basa.com.br.

15.2.4 O licitante recorrente enviará no prazo de 3 (três) dias úteis, contados a partir da data de intimação, para apresentar as razões do recurso, em campo próprio do sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, também via sistema eletrônico, contado da data final do prazo do recorrente.

15.3 O Pregoeiro poderá não conhecer o recurso já nesta fase em situação excepcional e restrita, acaso a manifestação referida no subitem precedente seja apresentada fora do prazo ou por pessoa que não represente o proponente ou se o motivo apontado não guardar relação de pertinência com a licitação. Será vedado ao Pregoeiro rejeitar o recurso de plano em razão de discordância de mérito com os motivos apresentados pelo proponente.

15.4 Apresentadas as razões e contrarrazões, o Pregoeiro disporá de 03 (três) dias úteis, para reavaliar sua decisão e dar os seguintes encaminhamentos, conforme o caso:

a) se acolher as razões recursais, deverá retomar a sessão pública para dar prosseguimento à licitação, garantindo, depois de nova declaração de vencedor, o direito à interposição de recurso, inclusive por parte de proponente que tenha sido impedido de participar da licitação, que teve sua proposta desclassificada ou que foi inabilitado;

b) se não acolher as razões recursais, deverá produzir relatório e encaminhar o recurso para a autoridade competente, para decisão definitiva, que deve ser produzida no prazo máximo de 10 (dez) dias úteis, contado do recebimento dos autos. Nesta última hipótese, a autoridade competente deverá tomar a decisão definitiva sobre o recurso.

15.4.1 A decisão definitiva sobre o recurso deverá ser publicada no sítio eletrônico oficial www.compras.gov.br/compras

15.4.2 Na hipótese da alínea "a" deste subitem, após a publicação da decisão de acolhimento no sítio eletrônico do item anterior, será observado o prazo de, no mínimo, 2 (dois) dias úteis para a retomada da sessão pública.

15.5 O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

16 DA REABERTURA DA SESSÃO PÚBLICA

16.1 O pregoeiro poderá determinar o retorno à fase de sessão pública, consistente na sua reabertura, quando:

16.1.1 houver a anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que deles dependam;

16.1.2 ocorrer erro na aceitação do preço mais bem classificado ou quando o licitante declarado vencedor não assinar o contrato ou não comprovar a regularidade fiscal e trabalhista, nos termos do art. 43, §1º, da Lei Complementar nº 123/2006, sendo adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

16.2 Havendo a necessidade de reabertura da sessão pública do pregão, o pregoeiro convocará, por meio do sistema eletrônico, via chat, os licitantes remanescentes para acompanhá-la, de acordo com a fase da licitação.

16.3 Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o subitem 14.26, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema eletrônico com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

17 ADJUDICAÇÃO E HOMOLOGAÇÃO

17.1 Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá:

a) determinar o retorno dos autos para saneamento de irregularidades;

b) revogar a licitação por motivo de conveniência e oportunidade;

c) proceder à anulação da licitação, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável;

d) adjudicar o objeto e homologar a licitação.

17.1.1 O vício de legalidade será convalidado se o ato por ele contaminado puder ser repetido sem o referido vício, o que ocorre, dentre outros casos, com vícios de competência e tocantes às formalidades.

17.1.2 Nos casos de anulação e revogação, deverá ser assegurada a prévia manifestação dos interessados.

17.1.3 O motivo determinante para a revogação do processo licitatório deverá ser resultante de fato superveniente que constitua óbice manifesto e incontornável.

18 DA CONTRATAÇÃO

18.1 No prazo de até 15 (quinze) dias úteis após a homologação, ao Banco da Amazônia convocará o proponente adjudicado para assinar o contrato, conforme minuta que integra o presente Edital (ANEXO VI) e seus adendos decorrentes do Código de Conduta e Integridade da Banco da Amazônia (consultar no site www.bancoamazonia.com.br).

18.2 O representante legal do proponente adjudicado deverá comparecer ao Banco da Amazônia no prazo de 5 (cinco) dias úteis, a contar da convocação, para assinatura do respectivo instrumento de contrato.

18.3 O Banco realizará consultas à lista restritivas de Prevenção e Lavagem de Dinheiro (PLD), sendo que caso a CONTRATADA apresente restrições nas referidas listas, tal restrição será encaminhada ao Comitê Antifraude e Anticorrupção (CAFRA) para deliberação sobre a contratação;

18.4 Consulta ao CADIN (Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Federais) sendo que o proponente adjudicante não deve ter existência de registro nesse Cadastro, sob pena de não ser contratado, considerando que é fator impeditivo para contratação, observada a Lei nº 10.522 de 2002, alterada pela Lei nº 14.973 de 2024

18.4.1 Para efetivação do respectivo instrumento de contrato, a assinatura poderá ser eletrônica, conforme decisão do gestor do contrato.

18.5 Como condição da assinatura do instrumento contratual:

18.5.1 o licitante vencedor deverá manter todas as condições de habilitação exigidas nesta licitação;

18.5.2 será exigido do proponente adjudicado a indicação da modalidade de garantia de execução, do contrato que será prestado;

18.6 A recusa injustificada do proponente vencedor em assinar o instrumento contratual, dentro do prazo e condições estabelecidos, caracterizará o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas.

18.6.1 Ocorrendo o previsto neste subitem, O Banco da Amazônia poderá revogar a licitação ou convocar os proponentes remanescentes, atendida a ordem de classificação, para negociação e possível adjudicação do objeto da licitação e homologação pela autoridade superior.

18.7 O contrato a ser celebrado entre o Banco da Amazônia e o licitante vencedor regular- se-á pelas suas cláusulas, pelo disposto na Lei nº 13.303/2016, pelo Regulamento de Licitações e Contrato do Banco da Amazônia e pelos preceitos do direito privado.

19 SANÇÕES ADMINISTRATIVAS

19.1. O proponente estará sujeito à multa, garantido o contraditório e a ampla defesa, nas seguintes hipóteses e nos seguintes percentuais:

19.1.1. não assinar o contrato, quando convocada dentro do prazo de validade de sua proposta, ou não mantiver a proposta: multa de 2% (dois por cento) sobre o valor da sua proposta;

19.1.2. deixar de entregar documentação exigida neste Edital: multa de 2% (dois por cento) sobre o valor da sua proposta;

19.1.3. apresentar documentação falsa: multa de 5% (cinco por cento) sobre o valor da sua proposta;

19.1.4. comportar-se de modo inidôneo: multa de 5% (cinco por cento) sobre o valor da sua proposta;

19.1.5. fizer declaração falsa: multa de 5% (cinco por cento) sobre o valor da sua proposta;

19.1.6. cometer fraude fiscal: multa de 5% (cinco por cento) sobre o valor da sua proposta.

19.2. Ocorrendo mais de uma infração, as multas serão cumulativas até o limite de 5% (cinco por cento) do valor de sua proposta.

19.3. O proponente que se comportar com má-fé estará sujeito, garantido o contraditório e a ampla defesa, à penalidade de suspensão temporária de participação em licitação e impedimento de contratar com o Banco da Amazônia, por prazo não superior a 2 (dois) anos, de acordo com os critérios do artigo 109 do Regulamento de Licitações e Contratos do Banco da Amazônia.

19.4. As penalidades referentes à inexecução do Contrato estão estabelecidas na Minuta de Contrato, **ANEXO VI** deste Edital e no Termo de Referência – **ANEXO I** deste Edital.

20 RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANCO DA AMAZÔNIA

20.1 Com fundamento no artigo 5º da Lei n. 12.846/2013, constituem atos lesivos ao Banco da Amazônia as seguintes práticas:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo do procedimento licitatório;

b) impedir, perturbar ou fraudar a realização de qualquer ato do procedimento

licitatório;

c) afastar ou procurar afastar proponente, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar a licitação ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação ou celebrar contrato administrativo;

f) obter vantagem ou benefício indevido, por meio fraudulento, de modificações no ato convocatório da licitação;

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados.

20.2 A prática, pelo proponente, de atos lesivos ao Banco da Amazônia, o sujeitará, garantida a ampla defesa e o contraditório, às seguintes sanções administrativas:

a) multa, no valor de 0,1% (um décimo por cento) a 20% (vinte por cento) do faturamento bruto do último exercício anterior ao da instauração do processo administrativo, excluídos os tributos, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação;

b) publicação extraordinária da decisão condenatória.

20.3 Na hipótese da aplicação da multa prevista na alínea "a" deste subitem, caso não seja possível utilizar o critério do valor do faturamento bruto da pessoa jurídica, a multa será de R$ 6.000,00 (seis mil reais) a R$ 60.000.000,00 (sessenta milhões de reais).

20.3.1 As sanções descritas neste subitem serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e natureza das infrações.

20.3.2 A publicação extraordinária será feita às expensas da empresa sancionada e será veiculada na forma de extrato de sentença nos seguintes meios:

20.3.2.1 em jornal de grande circulação na área da prática da infração e de atuação do proponente ou, na sua falta, em publicação de circulação nacional;

20.3.2.2 em Edital afixado no estabelecimento ou no local de exercício da atividade do proponente, em localidade que permita a visibilidade pelo público, pelo prazo mínimo de 30 (trinta) dias; e

20.3.2.3 no sítio eletrônico do proponente, pelo prazo de 30 (trinta) dias e em destaque na página principal do referido sítio.

20.3.3 A aplicação das sanções previstas neste subitem não exclui, em qualquer hipótese, a obrigação da reparação integral do dano causado.

20.4 A prática de atos lesivos ao Banco da Amazônia será apurada em Processo Administrativo de Responsabilização (PAR), instaurado pelo gestor da unidade de contratação e conduzido por comissão composta por 2 (dois) servidores designados.

20.4.1 Na apuração do ato lesivo e na dosimetria da sanção eventualmente aplicada, o Banco da Amazônia deve levar em consideração os critérios estabelecidos no artigo 7º e seus incisos da Lei n. 12.846/2013.

20.4.2 Caso os atos lesivos apurados envolvam infrações administrativas à Lei n. 13.303/16, ou a outras normas de licitações e contratos da administração pública, e tenha ocorrido a apuração conjunta, o proponente também estará sujeito a sanções administrativas que tenham como efeito restrição ao direito de participar em licitações ou de celebrar contratos com a administração pública, a serem aplicadas no PAR.

20.4.3 A decisão administrativa proferida pela autoridade julgadora ao final do PAR será publicada no Diário Oficial da União.

20.4.4 O processamento do PAR não interferirá na instauração e seguimento de processo administrativo específicos para apuração da ocorrência de danos e prejuízos ao Banco da Amazônia resultantes de ato lesivo cometido pelo proponente, com ou sem a participação de agente público.

20.4.5 O PAR e o sancionamento administrativo obedecerão às regras e parâmetros dispostos em legislação específica, notadamente, na Lei n. 12.846/2013 e Decreto n. 11.129/2022, inclusive suas eventuais alterações.

20.5 A responsabilidade da pessoa jurídica na esfera administrativa não afasta ou prejudica a possibilidade de sua responsabilização na esfera judicial.

20.6 As disposições deste item se aplicam quando o proponente se enquadrar na definição legal do parágrafo único do artigo 1º da Lei n. 12.846/2013.

21 DISPOSIÇÕES FINAIS

21.1 A presente licitação não importa necessariamente em contratação, podendo o BANCO revogá-la, no todo ou em parte, por razões de interesse público, derivadas de fato superveniente que constitua óbice manifesto e incontornável comprovado ou anulá-la por ilegalidade, de ofício ou por provocação, mediante ato escrito e fundamentado, disponibilizado no sistema para conhecimento dos INTERESSADOS.

21.2 Os proponentes serão responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados, em qualquer época.

21.3 As normas que disciplinam esta licitação serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse do Banco da Amazônia, a finalidade e a segurança da contratação.

21.4 Os atos, comunicados, decisões e quaisquer documentos referentes a este processo licitatório serão sempre publicados no sítio eletrônico do Banco da Amazônia e, adicionalmente, poderão ser veiculados por e-mail aos proponentes e/ou mediante publicação no Portal de Compras do Governo Federal (https://www.gov.br/compras/pt-br).

21.5 No intuito de dar celeridade ao Processo Licitatório, o Banco da Amazônia recomenda às interessadas em participar deste procedimento de licitação que providenciem a sua inclusão/atualização no SICAF.

21.6 O processo de licitação, bem como todos os documentos a ele pertinentes, estão disponíveis para a realização de vistas. Para tanto, é necessário prévio agendamento junto ao agente da licitação, por solicitação pelo e-mail **licitacoes@basa.com.br.**

21.7 Fazem parte integrante deste Edital os seguintes Anexos:

ANEXO I – TERMO DE REFERÊNCIA
ANEXO I-A – Especificações Técnicas da Solução Completa
ANEXO I-B – Níveis Mínimos de Serviço (NMS)
ANEXO I-C – Prova de Conceito (POC)
ANEXO I-D – REQUISITOS MÍNIMOS PARA SISTEMAS ADIQUIRIDOS
ANEXO II – MODELO PARA A PROPOSTA
ANEXO III, ANEXO IV, ANEXO V – MODELOS DE DECLARAÇÕES
ANEXO VI – MINUTA DE CONTRATO
ANEXO VII – TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO
ANEXO - VIII – TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES
ANEXO IX – TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE DO EMPREGADO TERCEIRIZADO
ANEXO X – MATRIZ DE RISCO

21.8 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será o local da realização do certame, considerado aquele a que está vinculado o agente da licitação.

Belém, PA, 26 de outubro de 2026.

Bruna Eline da Silva Cavalcante
Gerente Executiva de Contratações e Gestão
de Administração de Contratos - GECOG

PREGÃO ELETRÔNICO N. 90029/2026
TERMO DE REFERÊNCIA
ANEXO I

Abertura de Processo Licitatório para contratação de empresa especializada no fornecimento de solução e serviços gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center (CFC), em lote único, compreendendo a disponibilização, implementação, integração e operação contínua de solução integrada que contemple, de forma indissociável, as capacidades de Monitoramento e Resposta a Incidentes e Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), com alta disponibilidade (24x7x365), incluindo capacitação técnica e prestação de serviços especializados sob demanda, pelo período de 60 (sessenta) meses.

1 DEFINIÇÃO DO OBJETO

1.1 Contratação de empresa especializada, mediante Pregão Eletrônico, em lote único, para prestação de Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center (CFC), compreendendo a disponibilização, implementação, integração, operação, sustentação e evolução contínua de solução integrada que contemple, de forma indissociável, as capacidades de Monitoramento e Resposta a Incidentes e Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), em regime de alta disponibilidade 24x7x365, incluindo Serviços Técnicos Especializados e capacitação técnica sob demanda, pelo período de 60 (sessenta) meses, nos termos da Lei nº 13.303/2016 e em conformidade com este Termo de Referência e seus anexos.

1.2 Como parte integrante do escopo técnico dos Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, a solução deverá contemplar, de forma obrigatória, a implementação, o licenciamento, a operação contínua e a integração nativa de todos os itens descritos na tabela abaixo, devendo operar de forma unificada, coordenada e indissociável, sob responsabilidade integral da CONTRATADA, sendo vedada a prestação isolada de quaisquer componentes que façam parte dos itens ou a dependência de integrações externas que comprometam a efetividade da solução como um todo:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	Mês	60
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	Mês	60
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	Mês	60
4	Serviço de implantação, integração, migração,	Serviço	1

	homologação e transição operacional do Cyber Fusion Center		
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	UST	5.000
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	Turma	3 (com 15 participantes cada)
Obs.:	**** Regime contínuo de 24x7x365.***		
	***** Sob demanda, a critério do Banco, mediante Ordem de Serviço.***		

2 FORMA DE FORNECIMENTO E MODO DE DISPUTA

2.1 A execução do objeto observará as seguintes formas de fornecimento:

a) os Itens 1, 2 e 3 – referentes aos Serviços Gerenciados de Segurança Operacional Cibernética – XDR baseado em SIEM, GVUL e SRIS –, serão prestados de forma contínua e ininterrupta, em regime 24x7x365, durante a vigência contratual;

b) o item 4 – compreende o serviço de implantação, integração, migração, homologação e transição operacional para o novo SOC no modelo de Cyber Fusion Center, e serão prestados imediatamente após o kick-off e mobilização inicial.

c) o Item 5 – Serviços Técnicos Especializados, mensurado em UST, será executado sob demanda, mediante prévia autorização e emissão de Ordem de Serviço pelo Banco da Amazônia, sem obrigação de consumo integral do quantitativo estimado; e

d) o Item 6 – Capacitação Técnica e Treinamentos será executado sob demanda, mediante solicitação formal do Banco da Amazônia, sem obrigação de utilização integral das turmas previstas.

2.1.1 Para os serviços de natureza continuada, a execução será aferida em ciclos mensais, mediante apresentação, pela CONTRATADA, do respectivo Relatório de Serviços Prestados – RSP, contendo as evidências, os indicadores, os resultados e as demais informações necessárias à comprovação da execução dos serviços e ao atendimento dos Níveis Mínimos de Serviço.

2.1.2 A avaliação e a validação do RSP corresponderão ao procedimento de recebimento da respectiva parcela mensal dos serviços e observarão os prazos estabelecidos no art. 100, item 2, do Regulamento de Licitações e Contratos do Banco da Amazônia.

2.1.3 O ciclo de medição, recebimento e pagamento observará a seguinte sequência:

a) apresentação do RSP pela CONTRATADA;

b) avaliação e validação do RSP pelo Banco, nos prazos regulamentares aplicáveis ao recebimento;

c) autorização do Banco para emissão da Nota Fiscal ou documento fiscal equivalente;

d) emissão e apresentação da Nota Fiscal pela CONTRATADA; e

e) pagamento no prazo máximo estabelecido neste Termo de Referência, observado o disposto no art. 101, item 2, do Regulamento de Licitações e Contratos do Banco da Amazônia.

2.1.4 A apresentação da Nota Fiscal deverá ocorrer somente após a conclusão da avaliação e validação do respectivo RSP e a correspondente autorização do Banco, não se confundindo a data de apresentação do relatório com a data de início do prazo de pagamento.

2.1.5 As regras detalhadas de medição, recebimento, aplicação dos Níveis Mínimos de Serviço, ajustes de pagamento, glosas, aceite e faturamento serão estabelecidas no capítulo específico deste Termo de Referência, devendo ser interpretadas em conformidade com o ciclo previsto nos subitens 2.1.2 a 2.1.4.

2.2 O modo de disputa será aberto, considerando-se, para fins de julgamento, o menor preço global do lote único, sem prejuízo da verificação da aceitabilidade dos preços individuais de cada item, nos termos deste Termo de Referência.

3 FORMA DE SELEÇÃO DO FORNECEDOR E CRITÉRIO DE JULGAMENTO DE PROPOSTA

3.1 O fornecedor será selecionado por meio da realização de procedimento de Licitação na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço global.

3.2 A licitação será realizada em lote único considerando que o levantamento de mercado apontou que as soluções avaliadas, verifica-se que a divisão do objeto em itens/lotes, implicaria aumento significativo da complexidade operacional, elevação dos riscos de descontinuidade no fluxo de tratamento de incidentes, dependência de integrações entre múltiplos fornecedores e potencial comprometimento da efetividade do modelo de defesa cibernética adotado.

3.3 Sob a perspectiva técnica, a atuação integrada entre detecção, análise, resposta e mitigação de riscos exige fluxo contínuo, automatizado e orquestrado, com compartilhamento em tempo real de eventos, alertas, indicadores de risco, contexto de negócio e evidências, o que é mais adequadamente assegurado quando a responsabilidade pela solução é atribuída a um único fornecedor, com visão ponta a ponta da operação.

3.4 Nesse sentido, a adoção de lote único permite:

3.5 Responsabilidade integral (end-to-end) sobre a operação, desempenho e qualidade dos serviços, eliminando lacunas de responsabilidade entre fornecedores;

3.6 Redução de riscos operacionais, especialmente aqueles relacionados a falhas de integração, atrasos de escalonamento e conflitos de atribuição;

3.7 Maior eficiência na resposta a incidentes, com eliminação de dependência de acionamentos cruzados entre múltiplos prestadores;

3.8 Simplificação da governança contratual, com centralização da gestão, fiscalização e acompanhamento dos níveis de serviço;

3.9 Maior coerência técnica da arquitetura, assegurando integração nativa entre SIEM, XDR baseado em SIEM, GVUL e SRIS;

3.10 Padronização de processos, playbooks e fluxos operacionais, evitando desalinhamentos metodológicos;

3.11 Melhor rastreabilidade e auditabilidade, com consolidação de evidências, logs e registros sob responsabilidade única;

3.12 Otimização do tempo de detecção (MTTD) e resposta (MTTR), decorrente da eliminação de barreiras operacionais entre domínios.

3.13 Do ponto de vista econômico, embora a divisão em lotes possa, em determinados cenários, ampliar a competitividade, no contexto específico desta contratação tal abordagem tende a gerar custos indiretos adicionais, decorrentes de esforços de integração, sobreposição de ferramentas, aumento da complexidade de governança e maior necessidade de coordenação operacional entre fornecedores distintos.

3.14 Adicionalmente, a responsabilidade distribuída pode dificultar a identificação de falhas, a aplicação de penalidades e a mensuração objetiva de desempenho, impactando negativamente a eficiência da gestão contratual.

3.15 A adoção de lote único, por sua vez, favorece a obtenção de propostas mais consistentes do ponto de vista técnico-operacional, uma vez que exige dos licitantes a apresentação de soluções completas, integradas e plenamente aderentes ao modelo de Cyber Fusion Center, com capacidade comprovada de entrega fim-a-fim.

3.16 Complementarmente, como mecanismo de mitigação de riscos e garantia de aderência técnica, a solução ofertada será obrigatoriamente submetida à Prova de Conceito (POC), conforme estabelecido pelo Banco da Amazônia, permitindo validar, em ambiente controlado, a capacidade real de integração, operação, desempenho e atendimento aos requisitos definidos.

3.17 Esse mecanismo reforça a segurança da contratação, assegurando que a escolha da proposta mais vantajosa não se baseie exclusivamente em critérios econômicos, mas também na comprovação prática da capacidade técnica da solução ofertada.

3.18 Importa destacar que a opção pelo lote único não restringe a competitividade do certame, uma vez que o mercado dispõe de fornecedores e integradores com capacidade de ofertar soluções completas e integradas, seja por meio de plataformas próprias, parcerias tecnológicas ou modelos consolidados de prestação de serviços gerenciados (MSSP).

3.19 Adicionalmente, a modelagem adotada não direciona a contratação a fabricante ou tecnologia específica, estabelecendo apenas requisitos mínimos obrigatórios e resultados esperados, em conformidade com os princípios da isonomia, competitividade e seleção da proposta mais vantajosa, nos termos da Lei nº 13.303/2016.

3.20 Dessa forma, a não divisão do objeto em lotes mostra-se tecnicamente necessária, operacionalmente adequada permitindo ao Banco da Amazônia estruturar uma solução de segurança cibernética integrada, resiliente, eficiente e orientada a resultados, em plena aderência ao modelo de Cyber Fusion Center, às exigências regulatórias e às melhores práticas de governança e gestão de riscos cibernéticos.

3.21 Nesse contexto, recomenda-se a não divisão do objeto em lotes, adotando-se modelo de contratação em lote único, fundamenta-se em critérios técnicos, operacionais, de governança e de gestão de riscos, visando assegurar a entrega de uma solução de segurança cibernética integrada, contínua e orientada a resultados, em conformidade com o modelo de Cyber Fusion Center (CFC) definido pelo Banco da Amazônia.

3.22 Para fins de qualificação técnico-operacional, a licitante deverá apresentar certificado válido da norma ISO/IEC 27001:2022, emitido por organismo credenciado pelo INMETRO ou membro do IAF,cujo escopo contemple a prestação de serviços de Centro de Operações de Segurança (SOC), Cyber Fusion Center (CFC) ou Serviços Gerenciados de Segurança, nos termos do Art. 39, do Regulamento Interno de

Licitações e Contratos do Banco da Amazônia e subsidiariamente Art. 17, § 6º, inciso III, c/c art. 67, inciso III, da Lei nº 14.133/2021.

3.23 Embora a solução proposta seja composta por diferentes capacidades funcionais – Monitoramento e Resposta a Incidentes (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes na Primeira Linha de Defesa (SRIS) –, tais componentes não operam de forma isolada, sendo intrinsecamente interdependentes e demandando integração nativa, correlação multidimensional de eventos e atuação coordenada em tempo real.

3.24 Para efeito de julgamento, os lances ofertados deverão obedecer à composição de preços constantes no Mapa de Composição de Preços.

4 PRAZO DE EXECUÇÃO DO OBJETO DA CONTRATAÇÃO

4.1 A vigência contratual será de 60 (sessenta) meses, contados da data estabelecida no instrumento contratual.

4.2 Os Serviços de Implantação e Transição Operacional do Cyber Fusion Center deverão ser concluídos no prazo máximo de 90 (noventa) dias corridos, contados do início da vigência contratual ou da emissão da Ordem de Serviço específica de implantação, conforme definido pelo Banco da Amazônia.

4.3 O prazo máximo para a implantação inicial e ativação plena dos serviços e soluções objeto deste contrato (SOC, GVUL e XDR baseado em SIEM) será de até 90 (noventa) dias corridos, contados a partir da assinatura do contrato – este prazo é baseado em requisitos internos de transição e continuidade, de modo que o cronograma dependerá da validação contínua das equipes do Banco.

4.4 A implantação deverá observar, no mínimo, as seguintes etapas e respectivos prazos máximos acumulados:

ETAPA	PRAZO MÁXIMO
Kick-off e mobilização inicial	Até 5 dias úteis
Planejamento, diagnóstico, levantamento de fontes, ativos e arquitetura detalhada	Até 15 dias corridos
Implementação, configuração, parametrização e integrações das soluções XDR baseado em SIEM, GVUL e SRIS	Até 45 dias corridos
Migração ou adequação de casos de uso, regras, integrações e fluxos operacionais prioritários	Até 55 dias corridos
Testes técnicos, testes unitários e testes de integração	Até 60 dias corridos
Homologação pelo Banco e realização de UAT	Até 70 dias corridos
Correção das inconsistências identificadas na homologação	Até 75 dias corridos
Go-Live da solução integrada	Até 75 dias corridos
Operação assistida e estabilização	Do Go-Live até o 90º dia
Entrega da documentação final, transferência de conhecimento e aceite da implantação	Até 90 dias corridos

4.5 Os prazos estabelecidos no item 4.3 são cumulativos e representam limites máximos, podendo as etapas ser antecipadas ou executadas parcialmente em paralelo, desde que não haja comprometimento da segurança, da qualidade, da rastreabilidade, da disponibilidade ou da continuidade dos serviços.

4.6 O prazo de até 5 (cinco) dias úteis previsto para o kick-off e a mobilização inicial não se confunde com o prazo de implantação da solução. Esse período destina-se ao início formal dos trabalhos, à apresentação das equipes, à definição dos responsáveis, à validação do cronograma e à organização das atividades iniciais.

4.7 A fase de Planejamento e Diagnóstico deverá contemplar, no mínimo:

a) realização da reunião de kick-off;
b) elaboração e apresentação do Plano de Implantação;
c) levantamento e validação das fontes de dados;
d) levantamento dos ativos e endpoints;
e) definição da arquitetura detalhada da solução;
f) inventário das integrações necessárias;
g) elaboração do Plano de Migração e Transição;
h) priorização dos casos de uso, regras e integrações; e
i) definição dos critérios de testes, homologação e aceite.

4.8 A fase de Implementação deverá contemplar, no mínimo:

a) configuração e parametrização das soluções;
b) integração entre SIEM, XDR baseado em SIEM, GVUL e SRIS;
c) integração das fontes de logs e eventos;
d) integração com ServiceNow e demais sistemas corporativos previstos;
e) configuração e ativação da Gestão de Vulnerabilidades;
f) configuração dos fluxos operacionais do SRIS;
g) desenvolvimento, migração ou adequação de casos de uso;
h) criação ou ajuste de regras de detecção;
i) parametrização de playbooks;
j) ajustes de desempenho e tuning; e
k) demais atividades necessárias à preparação do ambiente para testes e homologação.

4.9 A fase de Testes e Homologação deverá compreender, conforme aplicável:

a) testes técnicos dos componentes;
b) testes unitários;
c) testes de integração;
d) testes de ingestão, processamento e correlação;
e) testes das integrações corporativas;
f) testes dos casos de uso e regras de detecção;
g) testes dos fluxos de resposta;
h) testes de capacidade, desempenho, disponibilidade e resiliência;
i) Testes de Aceitação pelo Usuário – UAT;
j) registro das respectivas evidências; e
k) correção e reteste das inconsistências identificadas.

4.10 A conclusão dos testes técnicos pela CONTRATADA não implicará automaticamente a aceitação da implantação, que dependerá da homologação pelo Banco da Amazônia e da comprovação do atendimento aos requisitos e critérios estabelecidos neste Termo de Referência e em seus anexos.

4.11 O Go-Live somente poderá ocorrer após:

a) conclusão satisfatória dos testes técnicos;
b) aprovação dos testes de integração;
c) conclusão da UAT;
d) correção das não conformidades impeditivas;
e) validação das integrações essenciais;
f) validação dos casos de uso considerados prioritários para entrada em produção;
g) aprovação dos procedimentos de contingência e reversão; e
h) autorização formal do Banco da Amazônia.

4.12 A partir do Go-Live, iniciar-se-á a operação produtiva do Cyber Fusion Center, passando a ser aplicáveis integralmente os Níveis Mínimos de Serviço previstos para os serviços continuados de XDR baseado em SIEM, GVUL e SRIS.

4.13 Após o Go-Live, a CONTRATADA deverá executar período de operação assistida e estabilização, até o limite máximo do 90º (nonagésimo) dia da implantação, destinado:

a) ao acompanhamento intensivo da operação;
b) à correção de falhas e inconsistências;
c) ao ajuste fino das regras, correlações e playbooks;
d) à estabilização das integrações;
e) à validação dos indicadores e fluxos operacionais;
f) à transferência de conhecimento; e
g) à consolidação da documentação técnica.

4.14 A conclusão da operação assistida deverá ser formalizada mediante aceite da implantação pelo Banco da Amazônia, condicionado, no mínimo, à:

a) inexistência de pendências críticas;
b) comprovação do funcionamento integrado dos componentes;
c) atendimento aos critérios de disponibilidade, desempenho e capacidade;
d) conclusão das integrações previstas para a entrada em produção;
e) entrega da documentação as-built;
f) entrega dos procedimentos operacionais;
g) entrega dos planos de continuidade, recuperação e contingência;
h) realização da transferência de conhecimento prevista para a fase; e
i) correção das não conformidades consideradas impeditivas para o aceite.

4.15 Pendências classificadas pelo Banco como não impeditivas poderão ser tratadas mediante plano de ação formalmente aprovado, desde que não comprometam a segurança, a disponibilidade, a integridade, a rastreabilidade, o desempenho ou a efetividade da solução.

4.16 O prazo máximo de 90 (noventa) dias para implantação não poderá ser utilizado como justificativa para postergação injustificada das atividades, devendo a CONTRATADA adotar planejamento que possibilite a entrada em produção no menor prazo tecnicamente viável.

4.17 A Prova de Conceito – POC não integra o prazo de implantação previsto neste item, por constituir etapa anterior à contratação, destinada à validação da aderência técnica, funcional e operacional da solução ofertada. A homologação da implantação terá finalidade distinta e será realizada sobre o ambiente efetivamente configurado e integrado ao ecossistema tecnológico do Banco da Amazônia.

4.18 O processo de implantação deverá observar, de forma sequencial e inequívoca, os seguintes marcos:

4.19 Conclusão da Implementação → Testes Unitários e de Integração → UAT → Correções → Go-Live → Operação Assistida e Estabilização → Aceite da Implantação.

4.20 A conclusão da implantação e o respectivo aceite não encerram as obrigações da CONTRATADA relativas à sustentação, operação, suporte, evolução tecnológica, manutenção das integrações e atendimento aos Níveis Mínimos de Serviço, que permanecerão exigíveis durante toda a vigência contratual.

5 JUSTIFICATIVA DA CONTRATAÇÃO

5.1 Em 26 de abril de 2018, foi editada a Resolução CMN nº 4.658, que estabeleceu requisitos relativos à política de segurança cibernética e à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Posteriormente, essa norma foi revogada e substituída pela Resolução CMN nº 4.893, de 26 de fevereiro de 2021, atualmente aplicável à matéria, que passou a disciplinar esses requisitos, incluindo diretrizes relacionadas à segurança cibernética, à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem e à continuidade dos serviços, observadas suas alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025.

5.2 Essa normativa reforçou a necessidade de adoção de controles técnicos e administrativos robustos, capazes de prevenir, detectar e responder a incidentes de segurança cibernética, assegurando a resiliência operacional das instituições integrantes do Sistema Financeiro Nacional.

5.3 Em atendimento a essas diretrizes e considerando o cenário de crescente sofisticação das ameaças digitais, o Banco da Amazônia estruturou sua estratégia de segurança da informação com base em serviços gerenciados especializados, voltados ao fortalecimento contínuo das capacidades de prevenção, detecção e resposta a incidentes.

5.4 Nesse contexto, a instituição passou a operar um Centro de Operações de Segurança (SOC), responsável pelo monitoramento contínuo de eventos, identificação de vulnerabilidades, tratamento de incidentes e mitigação de riscos, em regime ininterrupto (24x7x365), com atuação integrada entre as diversas capacidades de segurança cibernética.

5.5 O ambiente de negócios do Banco da Amazônia exige elevados níveis de disponibilidade e continuidade operacional, de modo que interrupções decorrentes de ataques cibernéticos, falhas de segurança ou exploração de vulnerabilidades representam riscos financeiros, reputacionais e regulatórios relevantes.

5.6 Nesse cenário, o SOC atua de forma proativa e reativa, identificando, analisando e contendo incidentes de segurança, reduzindo impactos e assegurando a integridade

das operações e dos dados institucionais, por meio de um modelo operacional integrado que envolve capacidades de monitoramento, detecção, gestão de vulnerabilidades e resposta a incidentes, de forma coordenada e contínua.

5.7 A presente contratação tem por finalidade garantir a continuidade, a resiliência e a modernização dos serviços de segurança cibernética do Banco da Amazônia, por meio da substituição da solução atualmente vigente, cujo contrato se encerra em setembro de 2026, assegurando aderência aos requisitos de continuidade operacional, às diretrizes estabelecidas pela Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, bem como às políticas internas de governança e gestão de riscos.

5.8 Em abril de 2026, o Banco da Amazônia concluiu avaliação formal de maturidade cibernética, com base no NIST Cybersecurity Framework (CSF) 2.0, obtendo nota global de 3,9, em escala de 5,0, classificada, conforme a metodologia adotada pelo Banco, como “Intermediário Superior”. A avaliação estabeleceu como objetivo institucional a evolução para o nível “Referência” (≥ 4,5) até junho de 2028. O scorecard por função evidenciou os seguintes gaps prioritário:

Função CSF 2.0	Gap prioritário identificado	Urgência	Contribuição da presente contratação
Respond (3,3)	Fluxo de comunicação regulatória de incidentes de segurança sem aprovação formal e sem automação suficiente	Crítico	Direta — item 4 do Anexo I-B (SRIS)
Detect (4,0)	Integração DRP ↔ SOC ↔ CSIRT não automatizada	Alto	Direta — correlação multidomínio e indicador FIC (Anexo I-B)
Recover (3,4)	Relatórios de execução de testes DR/BCP ausentes	Médio	Complementar — RCA e lições aprendidas do SRIS podem subsidiar o tratamento do gap, sem suprir a necessidade de relatórios formais de DR/BCP.
Govern (3,9)	Painel de KPI único ausente; métricas de conscientização ausentes	Alto	Parcial — RSP e Nota de Desempenho cobrem o painel de KPI de operações de segurança; métricas de conscientização permanecem fora do escopo
Identify (3,7)	Pentest e plano de ação 2026 pendentes	Crítico	Fora do escopo direto — disponível apenas via Item 5 (UST sob demanda), a critério do Banco

Função CSF 2.0	Gap prioritário identificado	Urgência	Contribuição da presente contratação
Protect (4,3)	MFA/isolamento lógico PIX-STR-RSFN pendentes	Crítico	Fora do escopo — arquitetura de identidade e segmentação de rede não integra XDR, GVUL ou SRIS

5.9 Os resultados da avaliação de maturidade demonstram que, embora o Banco da Amazônia apresente nível global de maturidade cibernética de 3,9, permanecem gaps prioritários, especialmente nas funções Respond e Detect, diretamente relacionados à capacidade operacional de detecção, análise, correlação e resposta a incidentes. Nesse contexto, a presente contratação foi estruturada para contribuir diretamente para o tratamento desses gaps, por meio da capacidade de resposta a incidentes na primeira linha de defesa (SRIS) e da correlação multidomínio proporcionada pela solução de XDR baseado em SIEM. Os gaps remanescentes nas funções Identify, Protect, Govern e Recover demandarão iniciativas complementares sob responsabilidade do Banco da Amazônia, não constituindo, integralmente, objeto da presente contratação.

5.10 A adoção do modelo de Cyber Fusion Center, em arquitetura cloud-native e no formato Software como Serviço (SaaS), visa modernizar o ambiente de monitoramento e resposta, ampliando a cobertura tecnológica, a eficiência operacional e a soberania dos dados institucionais, reduzindo a dependência de infraestrutura local e elevando a capacidade analítica por meio de inteligência artificial, análise comportamental (UEBA) e automação de resposta (SOAR), no contexto de uma solução integrada e unificada.

5.11 A solução deverá contemplar capacidades de detecção e resposta baseadas em identidade, de forma integrada e contextualizada. Nesse contexto, a correlação realizada por meio de mecanismos de SIEM e análise comportamental (UEBA) será complementar, mas não substitutiva.

5.12 O modelo de Cyber Fusion Center representa a evolução do Centro de Operações de Segurança tradicional, promovendo a integração nativa entre as capacidades de monitoramento, resposta a incidentes, gestão de vulnerabilidades, inteligência de ameaças e governança de riscos, consolidando um ecossistema de defesa cibernética orientado a dados, automação e análise de risco, com atuação contínua, coordenada e sob responsabilidade integral da CONTRATADA.

5.13 Seu propósito é romper barreiras entre áreas técnicas e de negócio, criando um ecossistema colaborativo de defesa cibernética capaz de correlacionar, em tempo real, eventos tecnológicos, comportamentais e operacionais, com visão unificada do risco institucional.

5.14 No contexto do Banco da Amazônia, essa abordagem ampliará a maturidade cibernética institucional, permitindo uma visão preditiva, contextualizada e orientada a risco das ameaças, baseada em análise multidomínio, automação de resposta (SOAR), aprendizado de máquina e análise comportamental (UEBA), com atuação integrada, contínua e sob responsabilidade única da CONTRATADA.

5.15 O SOC, no modelo de Cyber Fusion Center, atuará como núcleo estratégico de inteligência e resiliência digital do Banco da Amazônia, alinhado às diretrizes do Banco Central do Brasil e às melhores práticas internacionais de segurança cibernética,

promovendo a convergência nativa entre monitoramento, gestão de vulnerabilidades e resposta a incidentes, sem fragmentação operacional.

5.16 A capacidade integrada de resposta a incidentes, em regime contínuo (24x7x365), constitui elemento essencial da solução, garantindo atuação imediata, coordenada e eficaz diante de eventos de segurança que possam comprometer a disponibilidade, integridade e confidencialidade das informações corporativas, operando de forma plenamente integrada às capacidades de monitoramento, detecção e gestão de vulnerabilidades.

5.17 O aumento da complexidade dos ataques, aliado à criticidade dos serviços bancários digitais e à necessidade de conformidade com normas como a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, a Lei nº 13.709/2018 (LGPD) e a ISO/IEC 27035:2023, exige uma capacidade operacional contínua, especializada, altamente integrada e orientada a inteligência.

5.18 A solução assegurará a contenção rápida de ameaças, a redução dos tempos médios de resposta (MTTR) e o apoio técnico à mitigação de impactos, promovendo maior eficiência na gestão de incidentes, minimizando riscos financeiros, reputacionais e regulatórios, no contexto de uma operação centralizada e integrada de segurança cibernética.

5.19 A disponibilização de equipe técnica dedicada, especializada e certificada garante o tratamento adequado de eventos críticos, contribuindo diretamente para a resiliência cibernética e a continuidade dos serviços essenciais do Banco da Amazônia.

5.20 O objetivo da contratação é assegurar uma transição planejada para uma arquitetura tecnológica de segurança mais moderna, escalável e aderente às melhores práticas regulatórias e de mercado, preservando a integridade das operações críticas e ampliando a capacidade institucional de prevenção, detecção e resposta a incidentes cibernéticos, por meio de uma solução integrada, coordenada e operada de forma contínua.

5.21 A expansão dos serviços digitais – como abertura de contas online, novos canais transacionais, superaplicativo e ampliação de produtos financeiros – tende a aumentar significativamente o volume, a complexidade e a criticidade dos eventos operacionais e transacionais, demandando soluções avançadas de monitoramento, gestão de vulnerabilidades e resposta a incidentes, com uso intensivo de inteligência artificial, correlação automatizada de eventos e detecção comportamental (UEBA).

5.22 A nova arquitetura proposta contempla uma solução integrada de Segurança Gerenciada (MSSP), estruturada no modelo de Cyber Fusion Center, reunindo, de forma unificada, as capacidades de monitoramento e resposta a incidentes, gestão de vulnerabilidades e detecção e resposta estendidas (XDR baseado em SIEM), operando em regime contínuo (24x7x365) e assegurando atuação coordenada, integrada e contínua em todo o ciclo de segurança cibernética, sob responsabilidade integral da CONTRATADA.

5.23 O ambiente deverá utilizar infraestrutura em nuvem, no modelo cloud-native e SaaS, com capacidade mínima de ingestão de 600 GB/dia, retenção de logs por, no mínimo, 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), assegurando a integridade, rastreabilidade e disponibilidade das informações para fins

de auditoria, investigação forense e conformidade regulatória. Adicionalmente, a solução deverá suportar a correlação entre eventos de segurança, registros operacionais e dados transacionais, viabilizando mecanismos avançados de detecção baseados em comportamento (UEBA) e ampliando a visibilidade sobre todo o ecossistema tecnológico do Banco da Amazônia, de forma integrada e sob gestão unificada.

5.24 A retenção de 48 (quarenta e oito) meses possui finalidade regulatória, forense e de auditoria. Os dados mantidos além dos 12 (doze) meses em camada “quente” não necessitam permanecer integralmente normalizados no SIEM, podendo ser consultados a partir de dados brutos indexados ou em formatos definidos na fase de implantação, desde que preservadas a integridade, a rastreabilidade e a auditabilidade das informações.

5.25 A retenção complementar poderá ser atendida mediante exportação automática, segura e íntegra dos logs para ambiente sob custódia direta do Banco da Amazônia, permanecendo sob responsabilidade da CONTRATADA a garantia da integridade, periodicidade, completude e segurança desse processo, bem como sua rastreabilidade para fins de auditoria.

5.26 O período de 12 (doze) meses de logs “quentes” fundamenta-se em requisitos regulatórios, necessidades de auditoria, investigações e governança interna. Eventuais ajustes poderão ser realizados mediante validação prévia do Banco da Amazônia, desde que mantida a retenção total mínima de 60 (sessenta) meses.

5.27 A arquitetura proposta deverá assegurar elasticidade, escalabilidade automática e alta disponibilidade, superando as limitações do modelo atual e viabilizando análises históricas, correlação multidimensional e investigações forenses com maior profundidade, eficiência e agilidade, sem impacto na continuidade operacional dos serviços.

5.28 Além do monitoramento centralizado, a solução deverá contemplar capacidades contínuas de gestão de vulnerabilidades, incluindo identificação, análise, priorização automatizada de riscos e acompanhamento da remediação, operando de forma nativamente integrada às capacidades de detecção e resposta a incidentes, de modo a permitir atuação preventiva e orientada a risco.

5.29 De forma complementar, a solução deverá incorporar capacidades de Detecção e Resposta Estendida (XDR baseado em SIEM), responsáveis pela correlação avançada de eventos provenientes de endpoints, redes, aplicações, identidades e ambientes em nuvem, ampliando a visibilidade, reduzindo o tempo de detecção e permitindo resposta mais rápida, coordenada e eficaz a incidentes de segurança.

5.30 A contratação deverá contemplar, ainda, a disponibilização de serviços técnicos especializados sob demanda, destinados ao atendimento de necessidades específicas do Banco da Amazônia, tais como auditorias, análises forenses, testes de invasão, consultorias e outras atividades técnicas correlatas, bem como a capacitação das equipes internas, visando à transferência de conhecimento e ao fortalecimento das competências institucionais.

5.31 A necessidade dessa evolução tecnológica é reforçada pela Orientação Técnica nº 01/2025 do Banco Central do Brasil, que recomenda a implementação de controles aprimorados de detecção de fraudes, monitoramento de transações e análise

comportamental, com vistas ao fortalecimento da resiliência operacional e à proteção do Sistema de Pagamentos Brasileiro (SPB).

5.32 Adicionalmente, o Banco da Amazônia enfrenta desafios relacionados à proteção de dados não estruturados e à governança de acessos privilegiados, ampliando a exposição a riscos de acesso indevido, vazamento de informações sensíveis e manipulação de dados críticos, o que reforça a necessidade de uma solução integrada, com capacidades avançadas de monitoramento, correlação, detecção e resposta.

5.33 Nesse contexto, a contratação deverá abranger mecanismos avançados de auditoria de acessos, controle de credenciais privilegiadas (PAM) e análise comportamental de usuários, indispensáveis ao fortalecimento da governança, da rastreabilidade, da detecção de anomalias e da conformidade institucional.

5.34 A contratação proposta revela-se, portanto, necessária, proporcional e tecnicamente adequada, destinando-se a assegurar a continuidade e o fortalecimento dos serviços de segurança cibernética, a resiliência operacional e a proteção do patrimônio informacional e tecnológico do Banco da Amazônia, por meio de uma solução integrada e operada de forma contínua.

5.35 Diante do exposto, a iniciativa assegura conformidade com a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e com a Orientação Técnica nº 01/2025 do Banco Central do Brasil, além de alinhar-se ao Planejamento Estratégico Institucional 2024–2030 e ao Plano Diretor de Tecnologia da Informação (PDTI), contribuindo para a consolidação da maturidade cibernética da instituição e para a preservação dos pilares fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade.

5.36 A arquitetura de Cyber Fusion Center proposta neste Termo de Referência representa a consolidação de um modelo de segurança cibernética unificado, colaborativo e orientado a inteligência, com integração nativa entre capacidades de monitoramento, detecção, resposta e gestão de riscos.

5.37 A integração entre as capacidades de monitoramento e resposta estendida (XDR baseado em SIEM), gestão de vulnerabilidades e resposta a incidentes, combinada à automação de resposta (SOAR) e à análise comportamental (UEBA), proporcionará ao Banco da Amazônia uma visão única, contextualizada e preditiva das ameaças, fortalecendo sua resiliência operacional e alinhando suas práticas às exigências regulatórias e aos padrões internacionais de segurança da informação.

5.38 A implementação do SOC, no modelo de Cyber Fusion Center, consolida uma estratégia de defesa cibernética integrada, colaborativa e orientada a inteligência, permitindo a convergência operacional entre monitoramento, gestão de vulnerabilidades, resposta a incidentes e análise de riscos, com uso intensivo de automação, análise comportamental e inteligência artificial, promovendo atuação preditiva, contínua e baseada em evidências frente a ameaças emergentes.

5.39 Essa abordagem estabelece um novo patamar de maturidade e governança cibernética no âmbito do Sistema Financeiro Nacional, reforçando o compromisso do Banco da Amazônia com a resiliência e a segurança digital institucional, em conformidade com a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, a Lei nº 13.709/2018 (LGPD) e a Lei nº 13.303/2016 (Lei das Estatais).

5.40 Por fim, todo o tratamento de dados institucionais do Banco da Amazônia deverá observar rigorosamente os princípios e requisitos da Lei nº 13.709/2018 (LGPD), as disposições da Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e demais normativos aplicáveis, assegurando a proteção de dados, a rastreabilidade das informações e a segurança jurídica da instituição.

6 DESCRIÇÃO DOS SERVIÇOS E ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

6.1 Das Disposições Gerais

6.2 O conjunto de serviços compreende a implementação, disponibilização, integração, operação e sustentação das capacidades de XDR baseado em SIEM, GVUL e SRIS, bem como as atividades correlatas de monitoramento, detecção, análise, resposta a incidentes, gestão de vulnerabilidades, *threat hunting*, análise comportamental (UEBA), automação e orquestração de respostas e demais capacidades previstas neste Termo de Referência, devendo operar de forma unificada, coordenada e integrada, sob responsabilidade integral da CONTRATADA.

6.3 Para fins deste Termo de Referência, a expressão “XDR baseado em SIEM” refere-se às capacidades de Detecção e Resposta Estendidas implementadas a partir do SIEM e de seus mecanismos de correlação, análise, automação e integração com múltiplas fontes de telemetria e controles de segurança. O XDR baseado em SIEM objeto desta contratação não se confunde com solução de XDR de endpoint, não abrangendo a substituição da plataforma de proteção de endpoints já existente no Banco da Amazônia.

6.4 O XDR baseado em SIEM deverá integrar e correlacionar informações provenientes, conforme aplicável, de endpoints, identidades, redes, aplicações, ambientes em nuvem, Gestão de Vulnerabilidades, Threat Intelligence e demais fontes de segurança, inclusive mediante interoperabilidade com a solução de XDR de endpoint já utilizada pelo Banco, sem exigir sua substituição.

6.5 A solução deverá integrar-se, de forma nativa e bidirecional, à plataforma de Digital Risk Protection (DRP) já contratada pelo Banco da Amazônia, aproveitando as fontes de inteligência de ameaças voltadas à cibersegurança ali disponíveis, inclusive, quando pertinente ao contexto de risco cibernético, os indicadores relacionados a fraude, observadas as vedações institucionais de sobreposição com as áreas de prevenção a fraudes já previstas neste Termo de Referência. A solução deverá, ainda, integrar-se à plataforma corporativa de Governança, Risco e Compliance (GRC) do Banco da Amazônia, incluindo os indicadores de risco operacional nela mantidos, atualmente em consolidação por meio do módulo de Gestão Integrada de Riscos (IRM) em implantação sobre a plataforma ServiceNow , sem prejuízo de fontes complementares que o Banco venha a definir.

6.6 Os serviços continuados deverão ser prestados em regime gerenciado 24x7x365, assegurando alta disponibilidade, resiliência operacional e atendimento aos Níveis Mínimos de Serviço (NMS) definidos no Anexo I-B, devendo a CONTRATADA assegurar o funcionamento contínuo e integrado do ciclo de detecção, análise, resposta e mitigação de incidentes.

6.7 A solução deverá ser fornecida em modelo *cloud-native* e Software como Serviço (SaaS), cabendo à CONTRATADA disponibilizar todas as licenças, subscrições,

direitos de uso, infraestrutura, armazenamento, processamento, integrações, automações, mecanismos de correlação e demais componentes tecnológicos necessários à execução dos serviços.

6.8 As licenças, subscrições, softwares e demais componentes tecnológicos constituem recursos integrantes da prestação dos serviços e serão disponibilizados para utilização durante a vigência contratual, não caracterizando aquisição definitiva, licenciamento patrimonial autônomo ou cessão permanente de direitos de uso ao Banco da Amazônia, nem resultando em incorporação de ativos ao seu patrimônio.

6.9 A solução deverá assegurar integração nativa e operacional entre os domínios de monitoramento, Gestão de Vulnerabilidades e resposta a incidentes, com compartilhamento contínuo de informações, preservação de contexto e correlação automatizada entre vulnerabilidades, alertas e incidentes, reduzindo latências e assegurando fluxo contínuo e auditável entre detecção, análise e resposta.

6.10 Como etapa obrigatória do procedimento de seleção, a solução ofertada será submetida à Prova de Conceito (POC), conforme os critérios estabelecidos no Anexo I-C, destinada a comprovar, previamente à contratação, a aderência técnica, funcional, de integração e de desempenho da solução ofertada, sendo sua aprovação condição para aceitação da proposta.

6.10.1 Sem prejuízo da tabela de itens constante no item 1.2 deste Termo de Referência, a solução deverá observar, de forma obrigatória, os seguintes parâmetros técnicos mínimos e condições associadas a cada item, devendo operar de forma unificada, coordenada e indissociável, sob responsabilidade integral da CONTRATADA, sendo vedada a prestação isolada de quaisquer componentes ou a dependência de integrações externas que comprometam a efetividade da solução como um todo:

6.10.2 O Item 1 (Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM — XDR baseado em SIEM) compreenderá todos os licenciamentos, subscrições, infraestrutura e componentes necessários à sua operação, incluindo capacidade mínima de ingestão de 600 GB/dia, cobertura mínima de 5.000 endpoints protegidos por mês, UEBA, SOAR ou capacidades equivalentes, inteligência de ameaças e demais funcionalidades estabelecidas neste Termo de Referência e no Anexo I-A.

6.10.3 O Item 2 (Serviço e Solução Integrada de Gestão de Vulnerabilidades — GVUL) compreenderá todos os licenciamentos, subscrições, scanners, agentes, componentes e demais recursos necessários à Gestão de Vulnerabilidades de, no mínimo, 5.000 ativos monitorados por mês, conforme as especificações estabelecidas no Anexo I-A.

6.10.4 O Item 3 (Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa — SRIS) compreenderá os recursos tecnológicos e operacionais necessários à sua prestação contínua, não constituindo licenciamento autônomo vinculado a quantitativo de endpoints.

6.10.5 O Item 4 (Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center) será prestado sob a unidade "Serviço", quantidade estimada 1, devendo ser concluído em até 90 (noventa) dias corridos após o kick-off, conforme detalhado no item 4.3 deste Termo de Referência.

6.10.6 O Item 5 (Serviços Técnicos Especializados sob demanda) compreende consultorias, revisões, integrações e customizações de segurança, a serem realizados/consumidos a critério do Banco, mensurados em Unidades de Serviço Técnico (UST), em até 5.000 USTs durante a vigência do contrato, sem obrigação de utilização integral do quantitativo previsto.

6.10.7 O Item 6 (Capacitação técnica e treinamentos) compreende até 3 (três) turmas, sob demanda, com carga horária mínima de 40 (quarenta) horas cada e até 15 (quinze) participantes por turma, a critério do Banco, sem obrigação de utilização integral do quantitativo previsto.

6.10.8 Os licenciamentos, subscrições e componentes tecnológicos necessários à execução dos Itens 1, 2 e 3 deverão estar integralmente incluídos nos respectivos preços, não constituindo itens autônomos de contratação ou faturamento.

6.10.9 Os parâmetros técnicos de 600 GB/dia de ingestão, 5.000 ativos monitorados por mês e 5.000 endpoints protegidos por mês constituem capacidades mínimas associadas aos respectivos serviços, e não itens contratuais.

6.10.10 Os Serviços Gerenciados de Segurança Operacional Cibernética (SOC), contemplando Monitoramento e Resposta a Incidentes, capacidades de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes na Primeira Linha de Defesa (SRIS), deverão ser prestados de forma integrada e indissociável, em regime contínuo (24x7x365), pelo período de 60 (sessenta) meses, assegurando alta disponibilidade, monitoramento proativo, correlação avançada de alertas, emissão de relatórios técnicos, execução coordenada de respostas e mitigação tempestiva de incidentes, sob responsabilidade integral da CONTRATADA.

6.10.11 Os Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, deverão operar como um ecossistema único e integrado, responsável por monitorar continuamente o ambiente tecnológico do Banco da Amazônia, detectar ameaças, correlacionar eventos, apoiar a resposta a incidentes e subsidiar as ações de mitigação de riscos cibernéticos, assegurando fluxo contínuo e automatizado entre detecção, análise e resposta, sem dependência de integrações externas ou atuação de múltiplos fornecedores.

6.10.12 O SOC, no modelo de Cyber Fusion Center, deverá operar orientado por um modelo formal de Gestão de Risco Cibernético, baseado em referenciais reconhecidos internacionalmente (tais como NIST Cybersecurity Framework – CSF, ISO/IEC 27005 e CIS Controls), integrado de forma nativa aos processos, tecnologias e fluxos operacionais definidos neste Termo de Referência, assegurando a atuação coordenada, automatizada e contínua entre as capacidades de monitoramento (XDR baseado em SIEM), gestão de vulnerabilidades (GVUL) e resposta a incidentes (SRIS), como componentes de uma única solução.

6.10.13 A gestão de risco cibernético deverá ser contínua, orientada por dados e baseada em evidências, sendo operacionalizada por meio da correlação integrada entre eventos de segurança, vulnerabilidades, exposições, ativos críticos, indicadores operacionais e contexto de negócio do Banco da Amazônia, não se restringindo a avaliações pontuais ou exclusivamente reativas, devendo refletir a operação unificada da solução e garantir visão consolidada, preditiva e contextualizada do risco cibernético institucional.

6.10.14 O modelo de operação do SOC, no formato de Cyber Fusion Center, deverá permitir, de forma integrada, contínua e centralizada:

a) Associação de eventos, alertas, incidentes e vulnerabilidades aos ativos críticos do Banco da Amazônia, com manutenção de contexto e rastreabilidade completa;

b) Priorização inteligente de alertas, vulnerabilidades e incidentes com base em critérios de impacto, exposição, criticidade dos ativos e probabilidade de exploração, utilizando mecanismos de correlação avançada e análise contextual;

c) Correlação multidimensional entre risco técnico, risco operacional, risco regulatório e risco reputacional, permitindo visão consolidada e orientada a risco do ambiente cibernético institucional;

d) Acompanhamento contínuo da evolução do risco cibernético ao longo do tempo, com geração de indicadores, métricas e tendências, suportando a tomada de decisão estratégica e o aprimoramento contínuo dos controles de segurança.

6.10.15 A CONTRATADA deverá apresentar, na fase de implantação, documento descritivo do modelo de gestão de risco cibernético adotado, detalhando a metodologia, critérios de priorização, mecanismos de correlação e sua integração nativa com as capacidades de monitoramento, detecção e resposta a incidentes (XDR baseado em SIEM) e com os processos de resposta a incidentes (SRIS), sem prejuízo da autonomia do Banco da Amazônia sobre suas estruturas corporativas de GRC.

6.10.16 A solução de SIEM (Security Information and Event Management) deverá ser responsável pelo gerenciamento centralizado de informações e eventos de segurança, incluindo ingestão, normalização, correlação e análise de logs em tempo real, permitindo a detecção precoce de ameaças, geração de alertas priorizados e suporte efetivo à resposta a incidentes, como parte integrante da solução unificada de SOC.

6.10.17 A solução de SIEM deverá operar de forma nativamente integrada ao SOC, às capacidades de detecção e resposta estendida (XDR baseado em SIEM) e aos processos de resposta a incidentes (SRIS), incorporando mecanismos de análise comportamental (UEBA), correlação entre múltiplas fontes de dados e geração automatizada de alertas priorizados por severidade, assegurando fluxo contínuo, automatizado e coordenado entre detecção, análise e resposta.

6.10.18 A capacidade de XDR baseado em SIEM deverá prover detecção e resposta baseadas em identidade, de forma integrada e contextualizada ao ambiente do Banco da Amazônia. Nesse contexto, a correlação realizada por meio do SIEM e dos mecanismos de análise comportamental (UEBA) será complementar, mas não substitutiva.

6.10.19 O licenciamento da solução de SIEM deverá contemplar o processamento mínimo de 600 GB/dia de logs e eventos de segurança, abrangendo todas as fontes de dados corporativos – infraestrutura, servidores, aplicações, endpoints, dispositivos de segurança, serviços em nuvem e sistemas de negócio críticos – assegurando armazenamento por período mínimo de 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), garantindo integridade, rastreabilidade e disponibilidade das informações para fins de auditoria, investigação forense e conformidade regulatória.

6.10.20 A retenção de 48 (quarenta e oito) meses destina-se a finalidades regulatórias, forenses e de auditoria. Os dados além dos 12 (doze) meses em camada quente não necessitam permanecer pesquisáveis em estrutura normalizada do SIEM, podendo as consultas ser realizadas a partir de dados brutos indexados ou em formatos alternativos, conforme definido na fase de implantação.

6.10.21 O período de 12 (doze) meses de retenção em camada de consulta imediata está fundamentado em requisitos regulatórios, auditoria, investigações e governança interna. Eventuais adequações poderão ser realizadas, desde que previamente avaliadas e formalmente aprovadas pelo Banco da Amazônia, mantendo-se obrigatoriamente a retenção total mínima de 60 (sessenta) meses.

6.10.22 A retenção dos 48 (quarenta e oito) meses adicionais poderá ser atendida mediante exportação automática, segura e íntegra dos logs para ambiente de armazenamento sob custódia direta do Banco da Amazônia, sendo de responsabilidade da CONTRATADA garantir a integridade, periodicidade, disponibilidade e segurança desse processo de exportação.

6.10.23 A solução de Gestão de Vulnerabilidades (GVUL) deverá ser destinada à detecção, análise, priorização e tratamento contínuo de vulnerabilidades, por meio de mecanismos automatizados de varredura, análise de risco, classificação de criticidade e emissão de relatórios técnicos consolidados, como parte integrante da solução unificada de segurança cibernética.

6.10.24 O serviço de GVUL deverá contemplar o ciclo completo de gestão de vulnerabilidades, incluindo identificação, análise, priorização e acompanhamento das ações corretivas até sua efetiva resolução, devendo operar de forma nativamente integrada, coordenada e interoperável com as capacidades de monitoramento, detecção e resposta (XDR baseado em SIEM) e com os processos de resposta a incidentes (SRIS), assegurando fluxo contínuo entre prevenção, detecção e mitigação de riscos.

6.10.25 A CONTRATADA deverá disponibilizar plataforma dedicada, com acesso seguro via web, que permita a visualização dos resultados, priorização de riscos, acompanhamento das ações corretivas e geração de painéis técnicos e executivos, garantindo visibilidade consolidada da postura de vulnerabilidades do Banco da Amazônia.

6.10.26 Os perfis de acesso deverão observar o princípio do menor privilégio, contemplando níveis distintos para operação, auditoria e leitura, sendo sua definição detalhada realizada em conjunto com o Banco da Amazônia durante a fase de implantação.

6.10.27 O licenciamento da solução de GVUL deverá abranger, no mínimo, 5.000 (cinco mil) ativos monitorados por mês, incluindo servidores físicos e virtuais, estações de trabalho, dispositivos de rede, appliances de segurança e ativos em ambiente de nuvem sob responsabilidade do Banco da Amazônia.

6.10.28 O quantitativo de 5.000 (cinco mil) ativos monitorados por mês foi definido com base na estimativa atual e projetada do parque tecnológico do Banco da Amazônia, considerando aproximadamente 2.000 (dois mil) servidores físicos e virtuais e 3.000 (três mil) estações de trabalho corporativas, além de dispositivos de rede, equipamentos de segurança, infraestrutura e recursos em nuvem.

6.10.29 A adoção desse volume visa garantir cobertura integral da superfície de ataque da instituição, assegurando que todos os ativos críticos, endpoints e componentes de rede estejam contemplados nas rotinas automatizadas de varredura, análise e tratamento de vulnerabilidades, em conformidade com as melhores práticas de segurança cibernética e gestão de riscos tecnológicos.

6.10.30 O quantitativo proposto contempla margem de crescimento orgânico ao longo da vigência contratual de 60 (sessenta) meses, de modo a evitar a necessidade de ajustes contratuais decorrentes da expansão do parque tecnológico.

6.10.31 O dimensionamento de 5.000 (cinco mil) ativos monitorados por mês representa projeção técnica compatível com o porte e a criticidade da infraestrutura do Banco da Amazônia, alinhada às melhores práticas de gestão de vulnerabilidades em ambientes corporativos de missão crítica.

6.10.32 O quantitativo inicial de ativos monitorados será definido no início da fase de implantação, com base em inventário validado pelo Banco da Amazônia, preservando a previsibilidade contratual, a adequada precificação das propostas e a aderência às necessidades operacionais.

6.10.33 A capacidade de XDR baseado em SIEM deverá constituir componente tecnológico integrante da solução unificada de segurança cibernética, associada às capacidades de monitoramento e resposta a incidentes, voltada à correlação avançada de eventos e à execução automatizada de respostas, correlacionando informações provenientes de múltiplas camadas do ambiente tecnológico, incluindo endpoints, redes, aplicações, identidades e ambientes em nuvem.

6.10.34 A solução de XDR baseado em SIEM deverá operar de forma nativamente integrada ao SIEM e aos processos de resposta a incidentes, possibilitando correlação inteligente de eventos, priorização automatizada de alertas e execução orquestrada de ações de resposta, com o objetivo de reduzir o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR), assegurando fluxo contínuo, automatizado e coordenado entre detecção, análise e resposta.

6.10.35 A solução de XDR baseado em SIEM deverá prover capacidade de detecção e resposta baseada em identidade, de forma integrada e contextualizada ao ambiente do Banco da Amazônia. Nesse contexto, a correlação realizada por meio do SIEM e dos mecanismos de análise comportamental (UEBA) será complementar, mas não substitutiva.

6.10.36 A console da solução de XDR baseado em SIEM poderá estar em língua inglesa, bem como os manuais globais do fabricante. Entretanto, toda a documentação técnica, relatórios, entregáveis, evidências e materiais produzidos pela CONTRATADA deverão ser obrigatoriamente disponibilizados em língua portuguesa. A utilização de documentação em inglês não poderá comprometer a operação, a conformidade ou a auditabilidade da solução, devendo ser complementada, sempre que necessário, por documentação adequada em português.

6.10.37 Além dos indicadores tradicionais de desempenho, como o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR), o SOC, no modelo de Cyber Fusion Center, deverá adotar métricas complementares que reflitam a eficiência operacional, analítica e integrada das suas atividades, incluindo:

a) FCR – First Contact Resolution: percentual de incidentes resolvidos no primeiro atendimento, sem necessidade de escalonamento para níveis superiores;

b) MRR – Mean Remediation Rate: média de tempo decorrido entre a identificação de uma vulnerabilidade ou incidente e a aplicação efetiva da correção ou mitigação;

c) FIC – Fusion Intelligence Coverage Rate: percentual de incidentes tratados com base em correlação multidomínio, envolvendo dados de diferentes fontes (SIEM, GVUL, XDR baseado em SIEM, Threat Intelligence e indicadores de risco operacional).

6.10.38 O SOC deverá disponibilizar indicadores consolidados de risco cibernético, construídos a partir da correlação entre severidade de incidentes, criticidade dos ativos impactados, vulnerabilidades identificadas, exposições existentes e inteligência de ameaças relevante ao setor financeiro, refletindo a operação integrada da solução.

6.10.39 Esses indicadores deverão permitir:

a) Visualização do nível de exposição cibernética do Banco da Amazônia;

b) Acompanhamento da tendência e evolução do risco ao longo do tempo;

c) Apoio à tomada de decisão executiva e à governança de segurança da informação.

6.10.40 Os indicadores de risco deverão ser apresentados por meio de painéis gerenciais e relatórios executivos, observando as diretrizes de governança, rastreabilidade, auditabilidade e transparência estabelecidas neste Termo de Referência.

6.10.41 As métricas e indicadores deverão ser acompanhados de forma contínua e apresentados mensalmente em relatórios gerenciais, permitindo a avaliação sistemática da maturidade, integração e efetividade das operações do SOC, no modelo de Cyber Fusion Center.

6.10.42 O licenciamento das capacidades de XDR baseado em SIEM deverá abranger, no mínimo, 5.000 (cinco mil) endpoints protegidos por mês, sob responsabilidade do Banco da Amazônia, contemplando cobertura adequada da superfície de ataque e suporte às capacidades de detecção, correlação e resposta a incidentes.

6.10.43 O quantitativo de 5.000 (cinco mil) endpoints protegidos por mês foi estabelecido com base na estimativa do parque computacional do Banco da Amazônia, abrangendo aproximadamente 3.000 (três mil) estações de trabalho e notebooks, bem como 2.000 (dois mil) servidores físicos e virtuais distribuídos entre a matriz e as unidades regionais.

6.10.44 A definição desse volume tem como objetivo assegurar a cobertura integral dos ativos computacionais conectados ao ambiente corporativo, incluindo dispositivos móveis e ambientes híbridos ou em nuvem, garantindo visibilidade contínua, correlação avançada e resposta automatizada a incidentes em todas as camadas do ambiente tecnológico.

6.10.45 O dimensionamento proposto considera a operação integrada das capacidades de monitoramento, detecção e resposta, permitindo que todos os endpoints licenciados sejam continuamente monitorados e participem dos fluxos de análise comportamental, contenção, isolamento e remediação automatizada de ameaças, assegurando fluxo contínuo e coordenado entre detecção, análise e resposta.

6.10.46 O quantitativo de 5.000 (cinco mil) endpoints contempla margem de crescimento ao longo dos 60 (sessenta) meses de vigência contratual, considerando expansão do parque tecnológico, substituições de ativos e evolução dos serviços digitais do Banco da Amazônia.

6.10.47 O dimensionamento estabelecido configura-se como adequado, proporcional e preventivo, assegurando cobertura integral do ambiente computacional e efetividade das capacidades de detecção, correlação e resposta a incidentes cibernéticos.

6.10.48 Os Serviços Técnicos Especializados sob Demanda compreendem atividades especializadas de consultoria, auditoria e auditoria de segurança, testes de invasão, análises forenses, revisões técnicas e de configuração, integrações técnicas, hardening, customizações específicas e apoio avançado à resposta a incidentes, executadas mediante solicitação formal do Banco da Amazônia, conforme necessidades pontuais no contexto da solução contratada, e mensuradas em Unidades de Serviço Técnico – UST.

6.10.49 Tais serviços deverão ser executados mediante autorização formal do Banco da Amazônia, com acompanhamento técnico da área responsável, sendo mensurados em Unidades de Serviço Técnico (UST), totalizando 5.000 (cinco mil) UST ao longo da vigência contratual.

6.10.50 A definição da UST, os critérios de mensuração, os perfis profissionais, os níveis de complexidade, os entregáveis, os quantitativos de UST aplicáveis a cada atividade e os procedimentos de solicitação, autorização, execução e aceite serão estabelecidos pelo Banco da Amazônia.

6.10.51 Nenhuma atividade será executada ou faturada em UST sem prévia Ordem de Serviço emitida ou autorizada pelo Banco, contendo o escopo, o nível de complexidade, o quantitativo máximo de UST autorizado, os entregáveis e os critérios de aceite.

6.10.52 O quantitativo de 5.000 UST constitui limite máximo estimado para a vigência contratual, não implicando obrigação de consumo mínimo ou integral pelo Banco.

6.10.53 A capacidade de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) deverá contemplar atuação imediata e operacional na identificação, análise, contenção, erradicação e recuperação de incidentes de segurança cibernética, assegurando a continuidade operacional e a mitigação tempestiva de impactos, como parte integrante da solução unificada de segurança.

6.10.54 O serviço deverá incluir a triagem e validação de alertas, execução de ações corretivas emergenciais, registro e escalonamento de ocorrências, apoio à coleta e preservação de evidências, bem como integração com os processos de monitoramento e análise, garantindo rastreabilidade, consistência e continuidade operacional.

6.10.55 O serviço será prestado por equipe técnica especializada, em regime contínuo (24x7x365), em atuação coordenada com as equipes internas do Banco da Amazônia, conforme procedimentos e playbooks previamente definidos e aprovados, assegurando integração nativa, resposta estruturada e alinhamento aos processos institucionais de gestão de incidentes.

6.10.56 A capacitação técnica e os treinamentos sob demanda têm por finalidade assegurar a transferência de conhecimento e o fortalecimento das competências internas das equipes do Banco da Amazônia, promovendo autonomia na operação, interpretação e acompanhamento das soluções e serviços contratados, no contexto da solução integrada de segurança cibernética.

6.10.57 A CONTRATADA deverá ofertar, sob demanda, 3 (três) turmas de capacitação, com carga horária mínima de 40 (quarenta) horas cada e até 15 (quinze) participantes por turma, abrangendo os produtos, plataformas, metodologias, processos operacionais e fluxos integrados utilizados na execução dos serviços objeto da contratação.

6.10.58 Os treinamentos serão realizados sob demanda e a critério do Banco da Amazônia, podendo ocorrer de forma presencial ou remota, devendo ser ministrados por instrutores qualificados e certificados, com fornecimento de material didático atualizado, em língua portuguesa, e emissão de certificados individuais de conclusão aos participantes.

6.10.59 O público-alvo e a profundidade dos treinamentos serão definidos pelo Banco da Amazônia, de modo a assegurar que as equipes técnicas e operacionais de Segurança Cibernética e Infraestrutura estejam plenamente capacitadas para operar, administrar, interpretar e acompanhar a solução de forma integrada, garantindo sua adequada utilização, governança e evolução contínua no contexto do modelo de Cyber Fusion Center.

6.11 Todas as especificações técnicas da solução encontram-se descritas no Anexo I-A – Especificações Técnicas da Solução Completa, integrante deste Termo de Referência.

6.12 As soluções deverão observar as diretrizes técnicas, padrões de interoperabilidade e tecnologias estabelecidas pelo Banco da Amazônia, assegurando plena compatibilidade com o ecossistema tecnológico institucional, que contempla arquitetura baseada em microsserviços, containers e APIs REST em ambiente Red Hat OpenShift Container Platform, devendo operar de forma integrada, coordenada e interoperável no contexto da solução unificada de segurança cibernética.

6.13 A arquitetura do SOC deverá permitir, ao longo da vigência contratual, a integração de novos sensores e controles de segurança, tais como NDR, DLP, controles de acesso externo, segurança de e-mail, monitoramento de aplicações SaaS e controles relacionados ao uso de Inteligência Artificial, sempre que demandado pelo Banco da Amazônia, preservando a integração nativa, a interoperabilidade e a consistência da solução.

6.14 As integrações deverão ocorrer sem impacto na operação contínua, sem degradação de desempenho, preservando a coerência dos indicadores de risco e sem exigência de substituição dos componentes já implantados.

6.15 As soluções hospedadas em nuvem deverão integrar-se às ferramentas corporativas de observabilidade, métricas e logs (tais como Prometheus, Grafana, Elasticsearch e

equivalentes), garantindo interoperabilidade com o ambiente tecnológico do Banco da Amazônia, sendo obrigatória a compatibilidade com o ambiente Red Hat OpenShift Container Platform, incluindo suporte a agentes, APIs nativas ou mecanismos equivalentes para coleta, correlação e exportação de dados em clusters.

6.16 As diretrizes arquiteturais do Banco da Amazônia estabelecem padrões e versões suportadas, considerando a evolução contínua do ambiente tecnológico. As versões atualmente em uso serão disponibilizadas na fase de Due Diligence Técnica, previamente ao início da implantação, garantindo plena compatibilidade e integração das soluções.

6.17 Será admitida a participação de empresas reunidas em consórcio, observadas as condições estabelecidas no Edital, na Lei nº 13.303/2016 e no Regulamento de Licitações e Contratos do Banco da Amazônia.

6.17.1 A participação em consórcio não afastará a exigência de execução integrada da solução nem permitirá fragmentação de responsabilidades perante o Banco, devendo ser definida empresa líder e assegurada a responsabilidade pelo cumprimento integral das obrigações assumidas, na forma estabelecida no Edital e no instrumento contratual.

6.17.2 A composição do consórcio deverá preservar a capacidade de entrega fim a fim do Cyber Fusion Center, inclusive quanto à integração entre XDR baseado em SIEM, GVUL e SRIS, ao atendimento dos NMS e à continuidade da operação 24x7x365.

6.17.3 Será admitida a subcontratação parcial, mediante prévia e expressa autorização do Banco da Amazônia, exclusivamente para atividades específicas, acessórias ou de elevada especialização que não integrem o núcleo operacional contínuo do Cyber Fusion Center.

6.17.4 Poderão ser objeto de subcontratação, conforme necessidade e autorização do Banco:

a) análises forenses especializadas;
b) testes de invasão ou avaliações técnicas de alta complexidade;
c) serviços especializados de fabricantes necessários a atividades específicas;
d) capacitação ministrada por fabricantes, parceiros oficiais ou instrutores especializados; e
e) outras atividades acessórias ou especializadas expressamente autorizadas pelo Banco que não impliquem transferência da responsabilidade pelos serviços essenciais.

6.17.5 Não poderão ser subcontratados, total ou parcialmente, os serviços que compõem o núcleo operacional permanente do Cyber Fusion Center, especialmente:

a) gestão e coordenação operacional do CFC;
b) monitoramento contínuo e operação do XDR baseado em SIEM;
c) triagem, análise e tratamento contínuo de eventos e alertas;
d) operação continuada da Gestão de Vulnerabilidades;
e) operação do SRIS;
f) execução dos fluxos permanentes de detecção, escalonamento e resposta;
g) gestão dos Níveis Mínimos de Serviço e dos indicadores contratuais; e
h) responsabilidade pela integração e funcionamento fim a fim da solução.

6.17.6 A subcontratação autorizada não transferirá à subcontratada qualquer vínculo contratual com o Banco nem afastará ou reduzirá a responsabilidade integral da CONTRATADA pela qualidade, segurança, confidencialidade, cumprimento dos prazos, NMS, resultados e demais obrigações relacionadas aos serviços executados.

6.17.7 A CONTRATADA deverá assegurar que a subcontratada atenda aos requisitos técnicos, de qualificação, segurança da informação, confidencialidade, proteção de dados e compliance aplicáveis à atividade, podendo o Banco exigir a documentação comprobatória correspondente.

6.17.8 A contratação, pela CONTRATADA, de licenças, subscrições, plataformas ou suporte de fabricantes terceiros necessários à composição da solução não caracteriza, por si só, subcontratação da operação dos serviços, permanecendo a CONTRATADA integralmente responsável pelo funcionamento, integração, suporte e atendimento dos requisitos do objeto.

6.18 O critério de julgamento será o menor preço global do lote único, observadas as exigências técnicas, os Níveis Mínimos de Serviço e os critérios de aceitabilidade estabelecidos neste Termo de Referência.

6.18.1 A proposta comercial deverá apresentar, de forma individualizada, o preço unitário e o preço total de cada um dos itens, além do valor global do lote.

6.18.2 Sem prejuízo do julgamento pelo menor preço global, a aceitabilidade da proposta será verificada individualmente para cada item, com base nos respectivos valores máximos unitários e totais estimados pelo Banco.

6.18.3 Não será aceita proposta que apresente preço unitário ou total de qualquer item superior ao respectivo valor máximo admitido pelo Banco, ainda que o valor global do lote esteja abaixo do orçamento global estimado, ressalvada eventual negociação admitida na fase própria do procedimento.

6.18.4 Os preços unitários adjudicados para UST e turmas de capacitação constituirão os valores máximos aplicáveis durante a execução contratual, sendo o pagamento condicionado exclusivamente às quantidades efetivamente demandadas, autorizadas e aceitas pelo Banco.

6.18.5 Não haverá obrigação de consumo mínimo ou integral das 5.000 UST nem das 3 (três) turmas de capacitação, não cabendo à CONTRATADA qualquer indenização, compensação ou recomposição em razão da não utilização total dos quantitativos estimados.

6.18.6 Não será admitida compensação, transferência ou redistribuição de preços entre itens durante a execução contratual com a finalidade de absorver quantitativos não utilizados ou alterar a composição econômica originalmente adjudicada, ressalvadas as hipóteses legal e contratualmente admitidas.

6.18.7 O Banco da Amazônia define incidente de segurança da informação como qualquer evento adverso, confirmado ou sob suspeita, que indique violação das Políticas e Normativos de Segurança da Informação e Cibernética da instituição, resultando no comprometimento de um ou mais dos princípios fundamentais da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade das informações e dos ativos tecnológicos sob sua responsabilidade.

6.18.8 Todas as atividades da CONTRATADA que envolvam interação com o Banco da Amazônia, seus sistemas, usuários ou equipes técnicas deverão ser conduzidas integralmente em língua portuguesa, abrangendo:

a) Atendimentos técnicos em todos os níveis;

b) Relatórios, dashboards e documentos técnicos;

c) Materiais de capacitação e treinamento;

d) Interfaces de portais e plataformas web;

e) Pesquisas de satisfação e comunicações eletrônicas.

6.18.9 Eventuais ferramentas, painéis ou softwares que não possuam tradução nativa para o idioma português poderão permanecer em idioma estrangeiro, desde que não comprometam a operação, a governança, a auditabilidade ou a conformidade da solução, devendo ser obrigatoriamente acompanhados de documentação explicativa em língua portuguesa fornecida pela CONTRATADA, garantindo plena compreensão, usabilidade e autonomia operacional pelas equipes do Banco da Amazônia.

6.18.10 A CONTRATADA será integralmente responsável pelas atividades de planejamento, implantação, configuração, integração, documentação técnica, operação, sustentação, manutenção, atualização e suporte da solução objeto desta contratação, assumindo responsabilidade fim a fim (end-to-end) pela entrega, desempenho, disponibilidade e efetividade dos serviços, devendo assegurar a integração nativa e o funcionamento contínuo de todas as capacidades da solução.

6.18.11 A execução deverá contemplar todas as fases necessárias para a entrega funcional dos serviços, incluindo planejamento detalhado, implantação, integração ao ambiente tecnológico do Banco da Amazônia, homologação técnica, operação assistida, estabilização e operação contínua, assegurando consistência dos dados, rastreabilidade das informações e continuidade operacional de toda a solução.

6.18.12 Compete à CONTRATADA gerenciar de forma eficiente os recursos humanos, tecnológicos e operacionais alocados ao contrato, garantindo a disponibilidade integral dos serviços em regime contínuo (24x7x365), o cumprimento dos prazos estabelecidos e a aderência aos níveis de serviço (SLA e NMS), sendo responsável pela execução coordenada, integrada e tempestiva de todas as atividades necessárias à operação da solução.

6.18.13 A CONTRATADA deverá adotar práticas formais de gestão de capacidade, continuidade, desempenho e qualidade de serviço, mantendo modelo estruturado de governança, com comunicação contínua e transparente com o Banco da Amazônia. Deverão ser estabelecidos mecanismos formais de monitoramento, controle, acionamento e escalonamento, assegurando fluxo operacional contínuo, rastreável, auditável e eficiente em toda a cadeia de prestação dos serviços.

6.18.14 Quanto aos níveis de acesso dos usuários do Banco nas plataformas disponibilizadas, os perfis deverão observar o princípio de menor privilégio (least privilege), contemplando, no mínimo, acessos de natureza operacional, de auditoria e de leitura, sendo sua definição detalhada realizada em conjunto com a CONTRATADA durante a fase de implantação, em conformidade com os normativos de segurança do Banco da Amazônia.

6.19 Do Serviço de Implantação, Integração, Migração, Homologação e Transição Operacional do Cyber Fusion Center

6.20 A contratação deverá contemplar o Serviço de Implantação, Integração, Migração, Homologação e Transição Operacional do Cyber Fusion Center, de execução única, destinado à implementação e entrada em operação do novo SOC no modelo de Cyber Fusion Center, compreendendo todas as atividades técnicas, operacionais e de coordenação necessárias à transição entre o ambiente vigente e a solução contratada.

6.21 O serviço de implantação decorre da necessidade de realizar uma única transição estruturada para o novo Cyber Fusion Center, abrangendo, em uma entrega integrada, a preparação, implantação, migração, homologação, entrada em produção e estabilização das capacidades contratadas, antes de sua consolidação no regime operacional continuado.

6.22 Os serviços deverão ser iniciados imediatamente após a conclusão do kick-off e da mobilização inicial, observando o cronograma de implantação estabelecido no Termo de Referência e o prazo máximo de 90 (noventa) dias corridos para conclusão integral da implantação e transição operacional.

6.23 O serviço deverá abranger, de forma integrada e coordenada, as capacidades de XDR baseado em SIEM, Gestão de Vulnerabilidades – GVUL e Resposta a Incidentes de Segurança na Primeira Linha de Defesa – SRIS, contemplando, no mínimo:

a) planejamento detalhado da implantação e da transição operacional;
b) levantamento e validação do ambiente tecnológico, ativos, endpoints, fontes de dados, integrações e dependências;
c) definição e documentação da arquitetura detalhada da solução;
d) disponibilização, configuração e parametrização dos componentes tecnológicos necessários à prestação dos serviços;
e) implantação e integração das capacidades de XDR baseado em SIEM, GVUL e SRIS;
f) integração das fontes de logs e eventos de segurança, incluindo configuração dos mecanismos de coleta, ingestão, normalização, enriquecimento e correlação;
g) integração com os sistemas e plataformas corporativas do Banco da Amazônia, incluindo, conforme aplicável, ServiceNow, GRC, Data Lake, serviços de identidade, ferramentas de observabilidade e demais soluções previstas no Termo de Referência;
h) configuração dos fluxos operacionais, regras de correlação, mecanismos de automação e orquestração, playbooks e procedimentos de resposta;
i) levantamento, análise, priorização, migração, recriação ou adequação dos casos de uso, regras de detecção, listas, parâmetros, indicadores e demais configurações relevantes existentes no ambiente vigente;
j) realização de ajustes de desempenho, redução de falsos positivos e falsos negativos, parametrização e tuning das soluções;
k) configuração das capacidades de Gestão de Vulnerabilidades, incluindo descoberta, classificação, priorização e acompanhamento do tratamento dos ativos abrangidos;
l) configuração e integração dos processos operacionais de SRIS com os mecanismos de detecção, análise, escalonamento e resposta;
m) realização dos testes técnicos, testes unitários, testes de integração, testes de capacidade e demais verificações necessárias à validação da solução;

n) realização dos Testes de Aceitação pelo Usuário – UAT, com participação e validação do Banco da Amazônia;

o) correção e reteste das inconsistências, não conformidades e falhas identificadas durante os testes e a homologação;

p) preparação e execução do Go-Live, mediante autorização formal do Banco da Amazônia;

q) operação assistida e estabilização do ambiente após a entrada em produção;

r) transferência de conhecimento necessária à adequada continuidade e governança dos serviços;

s) entrega e atualização da documentação técnica, operacional e de arquitetura, incluindo documentação as-built; e

t) demais atividades necessárias à conclusão da implantação e à transição segura para o novo modelo de Cyber Fusion Center.

6.24 A migração deverá priorizar a preservação do conhecimento acumulado no ambiente vigente, incluindo casos de uso, regras de detecção, integrações, fluxos operacionais, parâmetros e demais artefatos considerados relevantes pelo Banco da Amazônia, não sendo admitida sua simples descontinuidade sem avaliação técnica, justificativa e aprovação prévia do Banco.

6.25 A CONTRATADA deverá apresentar, na fase inicial da execução, Plano de Implantação e Transição Operacional, contendo, no mínimo:

a) cronograma detalhado das atividades;

b) etapas, marcos e entregáveis;

c) responsabilidades da CONTRATADA e do Banco;

d) dependências técnicas e operacionais;

e) relação das fontes, sistemas e integrações a serem tratadas;

f) estratégia de migração dos casos de uso e configurações existentes;

g) estratégia de testes e homologação;

h) critérios de prontidão para Go-Live;

i) plano de contingência e reversão (rollback);

j) estratégia de operação assistida e estabilização; e

k) riscos identificados e respectivas medidas de tratamento.

6.26 A implantação deverá ser executada de forma a minimizar riscos de indisponibilidade, perda de eventos, perda de rastreabilidade, interrupção do monitoramento ou redução da capacidade de resposta a incidentes durante a transição entre o ambiente vigente e o novo Cyber Fusion Center.

6.27 Sempre que tecnicamente necessário, deverá ser prevista coexistência temporária entre o ambiente vigente e a nova solução durante a migração e homologação, de forma a preservar a continuidade dos controles de segurança até que o Banco autorize formalmente a entrada definitiva em produção.

6.28 A conclusão técnica da implementação pela CONTRATADA não caracterizará, por si só, o aceite do serviço, que dependerá da realização satisfatória dos testes, da homologação pelo Banco, da conclusão do UAT, da correção das não conformidades impeditivas, da entrada em produção, da operação assistida e da estabilização da solução.

6.29 O fluxo de implantação deverá observar, como referência, a seguinte sequência:

6.30 Kick-off e Mobilização → Planejamento e Diagnóstico → Implementação e Integração → Migração/Adequação → Testes Unitários e de Integração → UAT/Homologação → Correções → Go-Live → Operação Assistida e Estabilização → Aceite da Implantação.

6.31 A Prova de Conceito – POC não integra o serviço de implantação previsto neste subitem, por constituir etapa anterior à contratação destinada à validação da solução ofertada. Os testes, UAT e homologação aqui previstos serão realizados sobre a solução efetivamente configurada e integrada ao ambiente do Banco da Amazônia.

6.32 O serviço terá natureza não continuada e de execução única, sendo sua demanda estimada da seguinte forma:

6.33 **Do Licenciamento da Solução de SIEM**

6.33.1 A Solução de SIEM (Security Information and Event Management) a ser fornecida deverá estar integralmente em conformidade com o Anexo I-A – Especificações Técnicas da Solução Completa, contemplando licenciamento, garantia, manutenção, suporte técnico, atualização contínua e evolução tecnológica, conforme os requisitos estabelecidos neste Termo de Referência e demais documentos integrantes do processo licitatório.

6.33.2 O licenciamento da Solução de SIEM deverá contemplar o processamento de, no mínimo, 600 GB/dia de logs e eventos, abrangendo todas as fontes de dados corporativos – incluindo infraestrutura, servidores, aplicações, endpoints, dispositivos de segurança, serviços em nuvem e sistemas críticos de negócio – assegurando o armazenamento dos logs por período mínimo de 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), garantindo integridade, rastreabilidade, disponibilidade e auditabilidade das informações.

6.33.3 A retenção de 48 (quarenta e oito) meses possui finalidade regulatória, forense e de auditoria. Os dados mantidos além dos 12 (doze) meses em camada “quente” não necessitam permanecer integralmente normalizados no SIEM, podendo ser consultados a partir de dados brutos indexados ou em formatos definidos na fase de implantação, desde que preservadas a integridade, a rastreabilidade e a auditabilidade.

6.33.4 A retenção complementar poderá ser atendida mediante exportação automática, segura, íntegra e auditável dos logs para ambiente sob custódia direta do Banco da Amazônia, cabendo à CONTRATADA a responsabilidade pela entrega, integridade, periodicidade, completude e segurança desse processo, bem como pela garantia de sua rastreabilidade.

6.33.5 O período de 12 (doze) meses de logs “quentes” fundamenta-se em requisitos regulatórios, auditoria, investigações e governança interna. Eventuais adequações poderão ser realizadas mediante validação prévia do Banco da Amazônia, desde que mantida a retenção total mínima de 60 (sessenta) meses.

6.33.6 O licenciamento deverá contemplar, de forma obrigatória e sem ônus adicional, todos os módulos, funcionalidades, conectores, agentes, coletores, APIs e demais componentes necessários ao pleno funcionamento da solução, assegurando integração nativa, operação contínua e correlação eficiente entre todas as capacidades da solução de segurança cibernética.

6.33.7 Todos os requisitos técnicos previstos neste Termo de Referência e em seus anexos deverão ser entregues integralmente licenciados, incluindo direitos de uso, atualizações, correções, suporte técnico e evolução tecnológica, não sendo admitida a cobrança adicional por funcionalidades necessárias ao pleno atendimento do escopo contratado.

6.33.8 As expressões “deve”, “deverá”, “suporta”, “possui”, “executa”, “proporciona” e correlatas caracterizam obrigatoriedade de entrega funcional e operacional, devendo cada requisito estar disponível, implementado e em pleno funcionamento no ambiente produtivo, sem dependência de licenças adicionais, módulos futuros ou customizações não previstas.

6.33.9 As capacidades técnicas descritas neste Termo de Referência representam requisitos mínimos obrigatórios, sendo admitida a oferta de capacidades superiores, desde que compatíveis com a arquitetura definida e sem acréscimo de custo para o Banco da Amazônia.

6.33.10 Não serão aceitas soluções baseadas em hardware proprietário dedicado, tampouco soluções baseadas exclusivamente em software de código aberto (open-source) de uso genérico, desacompanhadas de suporte corporativo, governança de fabricante e comprovação de operação em ambientes de segurança gerenciada de missão crítica. Soluções que utilizem componentes open-source como parte de arquitetura corporativa serão admitidas, desde que integradas a plataforma suportada oficialmente pelo fabricante.

6.33.11 A solução deverá ser disponibilizada como produto consolidado de mercado, com suporte oficial do fabricante, manutenção contínua e ciclo regular de atualizações, correções de segurança e evolução tecnológica, compatível com ambientes corporativos de alta criticidade.

6.33.12 Não serão aceitas soluções desenvolvidas sob medida exclusivamente para o Banco da Amazônia. Serão admitidas apenas soluções integrantes do portfólio oficial do fabricante, amplamente adotadas no mercado e destinadas a operações de segurança gerenciada, assegurando estabilidade, escalabilidade e suporte contínuo.

6.33.13 A solução de SIEM deverá ser concebida como plataforma integrada e completa, capaz de prover, de forma nativa, funcionalidades de monitoramento, correlação, análise, investigação, inteligência de ameaças e apoio à resposta a incidentes, incluindo suporte a mecanismos de automação e orquestração (SOAR), análise comportamental (UEBA) e integração com fluxos operacionais de resposta, assegurando operação contínua e integrada.

6.33.14 O acesso ao ambiente do SIEM deverá ser realizado exclusivamente por meio de credenciais individuais, nominativas e intransferíveis, com autenticação multifator (MFA), garantindo rastreabilidade completa das ações executadas e auditoria integral das atividades, sendo vedado o uso de credenciais genéricas, compartilhadas ou de serviço sem controle individualizado.

6.33.15 A CONTRATADA deverá assegurar a confidencialidade, integridade, autenticidade e imutabilidade dos registros de auditoria, mantendo logs de acesso, configuração e operação armazenados por, no mínimo, 12 (doze) meses em camada de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, garantindo sua rastreabilidade, disponibilidade e adequação para fins de auditoria, investigação forense e conformidade regulatória, em aderência ao Anexo I-B – Níveis Mínimos de Serviço (NMS).

6.33.16 A solução deverá permitir a exportação estruturada, segura e auditável de registros de auditoria, relatórios e dashboards, bem como sua integração com os sistemas corporativos do Banco da Amazônia, especialmente plataformas de governança, risco e conformidade (GRC) e o sistema de gerenciamento de serviços e incidentes (ITSM – ServiceNow), assegurando interoperabilidade com os fluxos operacionais e rastreabilidade das informações.

6.33.17 O Banco da Amazônia disponibilizará os acessos, perfis e integrações necessários no ambiente ITSM ServiceNow para viabilizar a integração com a solução contratada, cabendo à CONTRATADA a correta implementação, configuração e operação dessa integração.

6.33.18 Todos os dados e metadados tratados, processados ou armazenados pela solução deverão observar integralmente as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e demais normativos aplicáveis, cabendo à CONTRATADA assegurar mecanismos de proteção compatíveis com o nível de criticidade das informações, incluindo, no mínimo, segregação lógica, controle de acesso baseado em perfil, rastreabilidade, criptografia, anonimização quando aplicável e proteção contra acessos indevidos.

6.34 **Do Serviço Gerenciado de Monitoramento e Resposta de Incidentes de Cibersegurança e Fraudes**

6.34.1 O Serviço Gerenciado de Monitoramento e Resposta a Incidentes de Cibersegurança consiste na prestação contínua, especializada e integrada de serviços de detecção, análise, investigação, resposta e mitigação de ameaças e eventos de segurança, abrangendo todo o ambiente tecnológico do Banco da Amazônia, em regime ininterrupto (24x7x365), por meio de um Centro de Operações de Segurança (SOC), no modelo de Cyber Fusion Center, sob responsabilidade integral da CONTRATADA.

6.34.2 A CONTRATADA deverá manter processo contínuo de gestão do ciclo de vida dos casos de uso (use cases), contemplando criação, revisão, validação, versionamento e aprimoramento periódico das regras de detecção, correlação e resposta, com base em evidências operacionais, inteligência de ameaças e evolução do cenário de risco.

6.34.3 As regras de detecção deverão considerar, de forma integrada, eventos e logs técnicos, vulnerabilidades identificadas, contexto de negócio, criticidade dos ativos, comportamento de usuários e entidades (UEBA), bem como indicadores de risco e inteligência de ameaças, assegurando visão contextualizada, adaptativa e orientada a risco.

6.34.4 O SOC da CONTRATADA deverá operar em arquitetura totalmente redundante, com infraestrutura de contingência geograficamente segregada, independente e automaticamente acionável, garantindo continuidade integral do serviço, sem perda de dados, degradação de desempenho ou interrupção operacional, mesmo em cenários de falha ou desastre.

6.34.5 O SOC deverá centralizar e unificar a monitoração de segurança cibernética do Banco da Amazônia, contemplando detecção, análise, investigação, resposta, comunicação e prevenção de incidentes, em conformidade com o Anexo I-B – Níveis Mínimos de Serviço (NMS).

6.34.6 O SOC deverá integrar, correlacionar e analisar dados provenientes de múltiplas fontes internas e externas, incluindo logs, eventos de segurança, vulnerabilidades, indicadores de risco, dados operacionais e inteligência de ameaças, viabilizando análise multidimensional e suporte à tomada de decisão baseada em risco.

6.34.7 O SOC deverá atuar como núcleo integrador de inteligência cibernética, promovendo correlação contínua entre informações de segurança, vulnerabilidades, risco operacional, continuidade de negócios e conformidade, assegurando visão unificada e consistente do risco cibernético institucional.

6.34.8 A solução deverá, de forma automatizada e contínua, correlacionar alertas e eventos do SOC, vulnerabilidades identificadas, indicadores de risco operacional, dados de Threat Intelligence e demais fontes relevantes, permitindo priorização dinâmica de incidentes e antecipação de ameaças.

6.34.9 O modelo de Cyber Fusion Center deverá assegurar a convergência entre processos, tecnologias e funções de segurança, risco, continuidade e prevenção a fraudes, estabelecendo mecanismos formais de governança técnica, comunicação estruturada e integração operacional, viabilizando resposta coordenada, tempestiva e baseada em inteligência.

6.34.10 A CONTRATADA deverá garantir integração operacional efetiva, contínua e automatizada entre todos os componentes da solução (SIEM, XDR baseado em SIEM, GVUL e resposta a incidentes), sendo vedada a dependência de acionamento manual exclusivo pelo Banco para execução de fluxos críticos, devendo tais fluxos operar de forma orquestrada, auditável e baseada em playbooks previamente definidos e aprovados.

6.34.11 A integração entre os componentes da solução deverá contemplar, no mínimo:

a) Compartilhamento estruturado, tempestivo e bidirecional de alertas, eventos, indicadores e evidências técnicas entre as plataformas que compõem a solução;

b) Encadeamento automático de eventos, alertas e incidentes, garantindo correlação contínua e rastreável ao longo de todo o ciclo de tratamento;

c) Execução e orquestração de playbooks integrados de resposta a incidentes, com adoção de ações automatizadas sempre que tecnicamente aplicável;

d) Interoperabilidade com ferramentas corporativas do Banco da Amazônia (SIEM, ITSM, GRC e demais sistemas), assegurando consistência, integridade e rastreabilidade das informações;

e) Atuação coordenada e centralizada sob responsabilidade da CONTRATADA, com definição clara de papéis, sem sobreposição ou lacunas operacionais;

f) Garantia de continuidade do fluxo de resposta de ponta a ponta, vedada qualquer fragmentação operacional ou transferência indevida de responsabilidade.

6.34.12 Essa integração estruturada tem por objetivo evoluir o modelo de monitoramento para uma atuação preditiva, adaptativa e orientada por risco, sustentada por inteligência de ameaças, automação (SOAR) e análise comportamental (UEBA), em conformidade com o modelo de defesa cibernética do Banco da Amazônia.

6.34.13 A CONTRATADA será integralmente responsável pela análise inicial, classificação, priorização, tratamento e resolução dos eventos e incidentes detectados, assegurando continuidade operacional e tratamento completo, sem lacunas ou descontinuidade, independentemente das camadas tecnológicas envolvidas.

6.34.14 A integração entre os componentes da solução deverá ocorrer de forma automatizada, contínua e auditável, sendo vedada a dependência exclusiva de processos manuais, comunicações informais ou mecanismos não estruturados para o acionamento entre as etapas de detecção, análise e resposta.

6.34.15 Deverão ser estabelecidos mecanismos formais de governança técnica e operacional, contemplando:

a) Definição clara e documentada de papéis e responsabilidades;

b) Fluxos de escalonamento estruturados;

c) Pontos de integração entre os componentes da solução;

d) Mecanismos de acompanhamento contínuo dos incidentes e ações de resposta.

6.34.16 A integração deverá permitir a geração de análises multidimensionais, a identificação antecipada de ameaças e a execução coordenada de respostas a incidentes, consolidando uma atuação orientada por risco, inteligência e contexto operacional.

6.34.17 O SOC deverá operar com evolução contínua de maturidade, migrando de um modelo predominantemente reativo para uma abordagem preditiva e adaptativa, baseada em inteligência de ameaças, automação (SOAR) e análise comportamental (UEBA), em alinhamento com as diretrizes estratégicas de segurança cibernética do Banco da Amazônia.

6.34.18 O Banco da Amazônia poderá realizar, a qualquer tempo, auditorias técnicas, operacionais ou de segurança, presenciais ou remotas, sobre os serviços prestados, devendo a CONTRATADA assegurar pleno acesso a registros, logs, artefatos, evidências técnicas e trilhas de auditoria, em conformidade com as políticas institucionais de governança, segurança da informação e auditoria.

6.34.19 O modelo de Cyber Fusion Center deverá assegurar a convergência efetiva entre monitoramento, análise, gestão de vulnerabilidades e resposta a incidentes, promovendo interoperabilidade contínua entre os fluxos de detecção (XDR baseado em SIEM), análise e priorização (SOC) e correção (GVUL), sob responsabilidade unificada da CONTRATADA.

6.34.20 As soluções que compõem o SOC deverão operar de forma integrada, correlacionada e consistente, disponibilizando ao Banco da Amazônia visão unificada de risco, eventos, vulnerabilidades e incidentes, por meio de dashboards consolidados, independentemente da arquitetura tecnológica subjacente, assegurando integridade, rastreabilidade e consistência das informações.

6.34.21 A exigência de visão unificada não implica, obrigatoriamente, a adoção de uma única ferramenta monolítica, sendo admitidas arquiteturas federadas, desde que assegurem:

a) Correlação automática, contínua e bidirecional entre SIEM, XDR baseado em SIEM, GVUL e fontes de Threat Intelligence;
b) Consistência, sincronização e integridade das informações apresentadas;
c) Rastreabilidade completa das análises, decisões e ações operacionais;
d) Acesso centralizado aos indicadores estratégicos e operacionais;
e) Continuidade do fluxo operacional de ponta a ponta, sob responsabilidade integral da CONTRATADA, vedada qualquer fragmentação ou transferência indevida de responsabilidade.

6.34.22 A solução deverá permitir visualização integrada, no mínimo, das superfícies de ataque, vulnerabilidades, identidades, ameaças ativas e inteligência de ameaças contextualizada ao perfil institucional do Banco da Amazônia, com capacidade de correlação dinâmica entre esses elementos.

6.34.23 O serviço deverá ser estruturado em três níveis operacionais de análise, conforme segue:

a) Nível 1 (N1) – Responsável pelo monitoramento contínuo dos eventos e alertas provenientes das diversas fontes, realização de triagem inicial, classificação de severidade, enriquecimento básico das informações, registro e acompanhamento de tickets, bem como encaminhamento estruturado para níveis superiores;
b) Nível 2 (N2) – Responsável por investigações aprofundadas e resposta a incidentes de maior complexidade, incluindo correlação de múltiplos vetores, validação de hipóteses, identificação de causa raiz e definição de ações corretivas e preventivas;
c) Nível 3 (N3) – Composto por especialistas seniores, responsáveis por investigações críticas, resposta a incidentes complexos, análises forenses, engenharia reversa, threat intelligence avançada e evolução contínua dos processos, regras de detecção e playbooks operacionais.

6.34.24 O SOC deverá dispor de funções especializadas, incluindo analistas de inteligência de ameaças e de gestão de vulnerabilidades, atuando de forma integrada no fluxo operacional. As atividades relacionadas à prevenção e combate a fraudes deverão ocorrer de forma coordenada com as áreas competentes do Banco da Amazônia, respeitando as atribuições institucionais, sendo vedada qualquer sobreposição ou conflito de responsabilidades.

6.34.25 A CONTRATADA deverá manter supervisão técnica contínua do SOC, com equipe mínima de analistas de nível N2 em regime integral, responsável por assegurar a qualidade técnica das análises, a correta categorização dos incidentes, o cumprimento dos prazos de escalonamento (SLA/NMS) e a revisão obrigatória dos registros antes de sua comunicação ao Banco da Amazônia.

6.34.26 A ausência de supervisão técnica, a indisponibilidade de profissionais qualificados ou a não manutenção de equipe com perfil, experiência e certificações compatíveis será caracterizada como falha grave de execução contratual, sujeita às penalidades previstas, sem prejuízo da apuração de impactos operacionais.

6.34.27 Os serviços serão remunerados de forma mensal e continuada, vinculados à efetiva prestação dos serviços e ao atendimento dos indicadores de desempenho estabelecidos neste Termo de Referência e em seus anexos.

6.34.28 O modelo de prestação deverá ser orientado a resultados mensuráveis, com pagamentos condicionados à validação de indicadores de desempenho e qualidade (KPIs e NMS), conforme definido no Anexo I-B, incluindo obrigatoriamente:

a) Indicadores de desempenho dos serviços;

b) Indicadores de eficiência operacional e integração dos componentes da solução;

c) Indicadores de tempo de resposta fim a fim (end-to-end), da detecção à mitigação;

d) Indicadores de qualidade técnica das análises e efetividade das respostas.

6.34.29 O modelo operacional deverá contemplar processos formais de interação e governança com o Banco da Amazônia, incluindo:

a) Abertura, registro, classificação e acompanhamento de chamados técnicos;

b) Atendimento a consultas e demandas sob solicitação;

c) Monitoramento proativo de segurança e infraestrutura;

d) Resposta, contenção, erradicação e mitigação de incidentes;

e) Emissão de relatórios técnicos, boletins e painéis gerenciais;

f) Participação em reuniões técnicas, comitês operacionais e comitês de segurança;

g) Execução contínua, integrada e ininterrupta dos serviços, assegurando tratamento completo dos incidentes, sem lacunas operacionais, sem dependência de acionamento manual pelo Banco e sob responsabilidade integral da CONTRATADA.

6.34.30 O serviço deverá contemplar as seguintes atividades:

6.34.30.1 **Monitoramento e Detecção**

a) Monitorar continuamente os eventos coletados e correlacionados pelo ecossistema XDR baseado em SIEM, abrangendo dados técnicos, operacionais e, quando aplicável, transacionais, garantindo visibilidade integral do ambiente tecnológico do Banco da Amazônia.

b) Realizar revisões, pesquisas e análises estatísticas sobre o histórico de logs armazenados, com o objetivo de identificar comportamentos anômalos, ameaças emergentes e potenciais incidentes de segurança cibernética.

c) Enriquecer os dados de eventos com informações provenientes de fontes internas e externas de Threat Intelligence, incluindo indicadores de comprometimento (IoCs), contexto de ameaças, reputação de ativos e campanhas ativas.

d) Confirmar, validar e classificar eventos de segurança, eliminando falsos positivos e consolidando alertas correlacionados, com base em critérios técnicos e de risco previamente definidos.

e) Categorizar incidentes de forma padronizada, considerando criticidade, impacto, probabilidade, ativos envolvidos e contexto de negócio, assegurando consistência na priorização e no tratamento.

f) Assegurar o encaminhamento automático, estruturado e tempestivo dos eventos e incidentes para os fluxos de análise e resposta, incluindo acionamento integrado dos mecanismos de resposta a incidentes e correlação com vulnerabilidades identificadas, vedada qualquer dependência de acionamento manual pelo Banco.

g) Garantir que eventos e alertas estejam devidamente correlacionados a ativos, vulnerabilidades, identidades e contextos de risco, permitindo análise multidimensional e suporte à tomada de decisão baseada em risco.

6.34.30.2 **Triagem, Registro, Escalada e Acompanhamento**

a) Triar e categorizar tickets com base na severidade, contexto, criticidade e impacto do evento, considerando a correlação integrada entre eventos, vulnerabilidades, identidades e inteligência de ameaças.

b) Registrar e manter atualizados todos os tickets no sistema de ITSM do Banco da Amazônia (ServiceNow), contendo, no mínimo:

i) Identificador único do ticket;

ii) Severidade e classificação do incidente;

iii) Regra, sensor ou origem do evento;

iv) Logs e evidências coletadas;

v) Origem, categoria e impacto do ataque;

vi) Informações adicionais enriquecidas e correlacionadas.

c) Acionar imediatamente, por telefone ou canal crítico previamente definido, a equipe responsável do Banco da Amazônia em casos de incidentes críticos, observando a escala de sobreaviso e os níveis de serviço estabelecidos.

d) Classificar o resultado da análise como:

i) Confirmado – quando validada a ocorrência de incidente;

ii) Falso positivo – quando não caracterizado risco;

iii) Autorizado – quando se tratar de atividade legítima previamente conhecida;

iv) Indeterminado – quando não houver evidências conclusivas suficientes.

e) Manter registro técnico detalhado em cada ticket, incluindo: ações executadas, análise técnica, impacto nos pilares de segurança (confidencialidade, integridade e disponibilidade), técnicas identificadas (ex.: MITRE ATT&CK), categoria do ataque e avaliação da efetividade dos controles existentes.

f) Garantir o acionamento automático e coordenado dos mecanismos de resposta a incidentes sempre que identificado evento que demande contenção ou mitigação, sendo vedada qualquer fragmentação operacional ou transferência de responsabilidade, cabendo à CONTRATADA a execução ponta a ponta do fluxo de resposta.

g) Acompanhar integralmente o ciclo de vida do incidente, desde a detecção até a contenção, erradicação e recuperação, fornecendo suporte técnico contínuo e informações complementares às equipes do Banco da Amazônia.

h) Padronizar e manter atualizados os procedimentos de resposta a incidentes, com base em playbooks operacionais, melhores práticas e cenários recorrentes, assegurando consistência e eficiência na execução das ações corretivas.

i) Apoiar a construção, manutenção e evolução da base de conhecimento institucional, incluindo registro de lições aprendidas, padrões de ataque e estratégias de resposta.

j) Registrar obrigatoriamente todos os alertas e eventos analisados no módulo SIR (Security Incident Response) do ServiceNow do Banco da Amazônia, independentemente da classificação atribuída.

k) Garantir que toda análise realizada seja registrada em ticket no ITSM (ServiceNow), assegurando rastreabilidade integral, contendo no mínimo:

i) Descrição detalhada da análise técnica;

ii) Evidências coletadas;

iii) Hipóteses avaliadas;

iv) Conclusão ou status final;

v) Referência a relatórios, artefatos ou documentos complementares.

6.34.30.3 **Gestão e Manutenção das Regras de Detecção**

a) Estabelecer e manter linhas de base (baseline) de comportamento do ambiente monitorado, ajustando dinamicamente limiares de detecção com base em dados operacionais, eventos de segurança, vulnerabilidades e contexto de risco, visando à redução de falsos positivos e falsos negativos.

b) Implementar técnicas avançadas de detecção, alinhadas ao framework MITRE ATT&CK, baseadas, no mínimo, em:

i) Desvios em relação às linhas de base comportamentais;

ii) Análise comportamental, estatística e preditiva (UEBA);

iii) Análise de tendências e padrões temporais;

iv) Identificação de padrões esperados e anômalos de logs (inclusive ausência de eventos esperados);

v) Definição e ajuste de thresholds dinâmicos e valores unitários;

vi) Listas de exceção controladas (whitelisting), devidamente justificadas, registradas e auditáveis.

c) Criar, revisar, versionar e manter regras de correlação, casos de uso (use cases) e alertas, considerando:

i) Demandas técnicas e operacionais do Banco da Amazônia;

ii) Inteligência de ameaças (Threat Intelligence) interna e externa;

iii) Informações provenientes de análise de incidentes e investigações realizadas;

iv) Dados correlacionados de vulnerabilidades e exposições identificadas;

v) Identificação proativa de ameaças relevantes ao ambiente monitorado.

d) As regras de detecção deverão, obrigatoriamente, correlacionar eventos de segurança, vulnerabilidades, identidades, ativos críticos e contexto de risco, assegurando visão multidimensional e integrada do cenário de ameaças.

e) Toda criação, alteração ou remoção de regras deverá observar processo formal de governança, incluindo:

i) Elaboração de relatório técnico contendo objetivo, lógica de detecção, limiares, fontes de dados, técnicas associadas (MITRE ATT&CK) e justificativa;

ii) Submissão prévia à validação e homologação técnica do Banco da Amazônia;

iii) Execução de testes controlados de eficácia, com evidências documentadas da capacidade de detecção antes da ativação em produção.

f) Documentar integralmente os casos de uso e regras de detecção implementadas, garantindo rastreabilidade, padronização e auditabilidade.

g) Manter catálogo atualizado de regras, contendo, no mínimo: nome, objetivo, descrição funcional, tática e técnica (MITRE ATT&CK), lógica de correlação (sintaxe), fator de agregação, fontes de dados, data de criação, última modificação e referência ao ticket correspondente.

h) Realizar manutenção contínua e aprimoramento das regras, limiares e alertas, com base em:

i) Evolução das ameaças e novos vetores de ataque;

ii) Mudanças no ambiente tecnológico e no escopo monitorado;

iii) Feedbacks operacionais e análises de desempenho;

iv) Redução sistemática de falsos positivos, falsos negativos e lacunas de detecção.

i) Garantir a geração de trilhas de auditoria para toda criação, alteração e exclusão de regras, incluindo emissão de alertas específicos no SIEM para tais eventos.

j) Toda modificação em regras ou casos de uso deverá ser registrada formalmente no sistema de gestão de tickets (ITSM), incluindo histórico completo, justificativas e evidências associadas.

k) É vedada qualquer alteração unilateral de regras, casos de uso ou parâmetros de detecção sem prévia autorização formal do Banco da Amazônia.

l) Executar, no mínimo semestralmente, testes estruturados de efetividade das regras ativas, com os seguintes objetivos:

i) Identificar necessidade de ajustes ou revisão de fontes de dados;

ii) Detectar lacunas de cobertura e oportunidades de melhoria;

iii) Avaliar aderência das regras aos cenários reais de ameaça;

iv) Validar a efetividade da correlação entre eventos, vulnerabilidades e incidentes;

v) Registrar resultados, evidências e recomendações conforme roteiro aprovado pelo Banco da Amazônia.

6.34.30.4 **Integração e Operacionalização de Fontes de Logs**

a) Para fins deste Termo de Referência, consideram-se fontes de logs todos os sistemas, aplicações, dispositivos, serviços e ferramentas do Banco da Amazônia capazes de gerar dados técnicos, operacionais ou transacionais relevantes para a detecção, análise, correlação e resposta a incidentes de segurança cibernética.

b) A CONTRATADA deverá integrar, normalizar, correlacionar e operacionalizar as fontes de logs corporativas ao ecossistema XDR baseado em SIEM, assegurando sua utilização plena nos processos de detecção, análise e resposta a incidentes, observando, no mínimo:

i) Definição e implementação do método de coleta mais adequado para cada fonte (agent-based, agentless, API, syslog, streaming ou equivalente), considerando criticidade, volumetria e sensibilidade dos dados;

ii) Configuração dos parâmetros técnicos nas fontes de logs, incluindo habilitação de eventos relevantes, granularidade adequada e definição de atributos necessários para envio e correlação dos dados;

iii) Implementação de processos de ingestão, normalização, parsing, enriquecimento e agregação dos dados coletados, assegurando padronização e consistência das informações;

iv) Mapeamento dos dados para modelo comum e estruturado (normalização semântica), compatível com os mecanismos de correlação, análise comportamental (UEBA) e inteligência de ameaças;

v) Configuração do XDR baseado em SIEM para ingestão eficiente, segura e escalável dos dados, garantindo integridade, confidencialidade e disponibilidade das informações;

vi) Definição de metodologia de coleta que preserve o desempenho dos ativos monitorados, evitando impacto operacional nos sistemas produtivos;

vii) Validação técnica da integração, com evidências documentadas da correta coleta, ingestão, normalização e correlação dos dados;

viii) Monitoramento contínuo da ingestão de logs, com geração automática de alertas em caso de interrupção, degradação, perda de eventos ou comportamento anômalo no fluxo de dados;

ix) Monitoramento da integridade, disponibilidade e confiabilidade das fontes de logs, incluindo detecção de falhas de transmissão, inconsistências ou ausência de dados esperados;

x) Emissão de relatórios técnicos periódicos contendo, no mínimo, status das integrações, cobertura das fontes, volumetria de dados, eventuais falhas identificadas, ações corretivas adotadas e evidências operacionais.

6.34.30.5 **Relatórios, Indicadores e Base de Conhecimento**

a) A CONTRATADA deverá manter e disponibilizar base de conhecimento continuamente atualizada, contendo métricas operacionais, indicadores de comprometimento e ataque (IOCs/IOAs), padrões de comportamento, técnicas e táticas associadas (MITRE ATT&CK), bem como registros de incidentes, vulnerabilidades e evidências correlacionadas, permitindo análise evolutiva do cenário de ameaças e apoio à tomada de decisão baseada em risco.

b) A base de conhecimento deverá ser alimentada de forma contínua a partir dos dados coletados e correlacionados pelo ecossistema XDR baseado em SIEM, incluindo eventos de segurança, incidentes tratados, vulnerabilidades identificadas, inteligência de ameaças e aprendizados operacionais, assegurando visão integrada e contextualizada do ambiente do Banco da Amazônia.

c) A CONTRATADA deverá elaborar e apresentar relatórios mensais técnicos consolidados, contemplando, no mínimo:

i) Eventos e incidentes detectados, classificados por criticidade, origem, vetor de ataque e impacto;

ii) Indicadores operacionais e de desempenho (KPIs e NMS), incluindo, no mínimo, MTTD, MTTR, FCR, MRR e FIC;

iii) Análise de tendências, evolução de ameaças e variações comportamentais relevantes no ambiente monitorado;

iv) Correlação entre eventos, vulnerabilidades, ativos críticos e incidentes, com visão orientada a risco;

v) Avaliação da efetividade das regras de detecção, incluindo taxa de falsos positivos e falsos negativos;

vi) Recomendações técnicas para mitigação de riscos, melhoria de controles e evolução da postura de segurança;

vii) Incidentes com potencial impacto financeiro, reputacional ou regulatório, incluindo, quando aplicável, eventos relacionados a fraude, respeitadas as atribuições institucionais do Banco.

d) Os relatórios deverão apresentar visão unificada, integrada e consistente da postura de segurança cibernética do Banco da Amazônia, sendo vedada a apresentação de informações fragmentadas, desconectadas ou inconsistentes entre fontes de dados, ferramentas ou módulos da solução.

e) A CONTRATADA deverá disponibilizar dashboards interativos, atualizados em tempo próximo ao real, contendo indicadores operacionais, eventos, incidentes, vulnerabilidades, níveis de risco e métricas de desempenho, permitindo:

i) Visualização executiva e técnica da postura de segurança;

ii) Acompanhamento contínuo de indicadores estratégicos e operacionais;

iii) Análise multidimensional por ativos, usuários, ameaças e vulnerabilidades;

iv) Suporte à tomada de decisão em níveis operacional, tático e estratégico.

f) A CONTRATADA deverá registrar e reportar mensalmente todas as mudanças realizadas no ambiente de monitoração, incluindo alterações de regras, integrações, playbooks, configurações e parâmetros operacionais, com respectivas justificativas, evidências e impactos esperados.

g) Todos os relatórios, dashboards e artefatos de informação deverão assegurar rastreabilidade completa, consistência dos dados e alinhamento integral com os registros do ITSM do Banco da Amazônia (ServiceNow), garantindo aderência aos requisitos de auditoria, governança, conformidade regulatória e investigação forense.

h) Os relatórios deverão ser disponibilizados em formato estruturado, editável e auditável, em língua portuguesa, observando padrões definidos pelo Banco da Amazônia, devendo permitir exportação e integração com ferramentas corporativas de governança, risco e compliance (GRC).

6.34.30.6 **Investigações Complementares e Threat Hunting**

a) A CONTRATADA deverá realizar investigações complementares sempre que demandado pelo Banco da Amazônia ou quando identificado indício relevante durante as atividades operacionais, utilizando de forma integrada e correlacionada os dados provenientes do ecossistema XDR baseado em SIEM, gestão de vulnerabilidades, inteligência de ameaças, registros históricos e demais fontes disponíveis, assegurando visão contextualizada e orientada a risco.

b) A CONTRATADA deverá conduzir atividades contínuas e proativas de Threat Hunting, com periodicidade mínima semanal, com foco na identificação de ameaças avançadas, comportamentos anômalos e indicadores de comprometimento não detectados automaticamente pelos mecanismos tradicionais de monitoramento.

c) As atividades de Threat Hunting deverão ser baseadas em hipóteses (hypothesis-driven hunting), fundamentadas em inteligência de ameaças, táticas, técnicas e procedimentos (TTPs) associados ao framework MITRE ATT&CK, campanhas ativas, vulnerabilidades relevantes e contexto específico do ambiente do Banco da Amazônia.

d) As investigações e atividades de Threat Hunting deverão, obrigatoriamente, considerar a correlação multidimensional entre eventos, identidades, ativos, vulnerabilidades, comportamentos e inteligência de ameaças, permitindo:

i) Identificação de padrões de ataque e movimentos laterais;

ii) Detecção de ameaças persistentes avançadas (APT) e atividades stealth;

iii) Correlação entre vulnerabilidades exploráveis e eventos de segurança;

iv) Identificação de lacunas de detecção e oportunidades de melhoria dos controles.

e) Os resultados das atividades de Threat Hunting deverão ser utilizados para retroalimentação contínua do ecossistema de segurança, incluindo:

i) Criação ou ajuste de regras de detecção e casos de uso;

ii) Aprimoramento de playbooks de resposta automatizada (SOAR);

iii) Atualização da base de conhecimento e inteligência de ameaças;

iv) Recomendação de medidas preventivas e corretivas ao Banco da Amazônia.

f) A CONTRATADA deverá apoiar tecnicamente o Banco da Amazônia nas atividades de resposta a incidentes, sempre que solicitado ou quando identificado cenário que exija atuação especializada, incluindo:

i) Elaboração de análises técnicas aprofundadas para suporte à investigação;

ii) Apoio na coleta, preservação e análise de evidências digitais, observando cadeia de custódia;

iii) Participação em reuniões técnicas e comitês de crise, quando aplicável;

iv) Apoio na identificação de causa raiz, vetor de ataque e escopo de impacto;

v) Recomendações técnicas para contenção, erradicação e prevenção de recorrência.

g) As atividades de investigação deverão observar rigor técnico compatível com práticas de resposta a incidentes e análise forense, assegurando integridade das evidências, rastreabilidade das ações executadas e aderência às diretrizes de auditoria, governança e conformidade regulatória.

h) Todos os resultados das atividades de investigação e Threat Hunting deverão ser formalmente registrados no ITSM do Banco da Amazônia (ServiceNow), contendo, no mínimo:

i) Descrição detalhada da hipótese investigada;

ii) Fontes de dados utilizadas;

iii) Evidências coletadas e analisadas;

iv) Técnicas e métodos aplicados;

v) Conclusões e classificação do resultado;

vi) Recomendações técnicas e ações sugeridas;

vii) Referência a incidentes, alertas ou vulnerabilidades correlacionadas.

i) A CONTRATADA deverá apresentar relatórios periódicos de Threat Hunting, no mínimo mensais, contendo a consolidação das atividades realizadas, hipóteses investigadas, achados relevantes, indicadores de comprometimento identificados, lacunas de detecção e recomendações estratégicas para evolução da postura de segurança do Banco da Amazônia.

6.35 **Do Serviço de Detecção e Resposta Estendida**

6.35.1 O Serviço de Detecção e Resposta Estendida (XDR baseado em SIEM) tem como objetivo ampliar a capacidade do Banco da Amazônia de detecção, correlação, análise e resposta a incidentes de segurança cibernética, por meio da integração nativa e contínua de eventos provenientes de múltiplas camadas do ambiente tecnológico – incluindo endpoints, redes, identidades, aplicações, ambientes em nuvem e dispositivos de segurança, de forma centralizada, automatizada e orientada a risco.

6.35.2 A solução deverá estar em conformidade com o Anexo I-A – Especificações Técnicas da Solução Completa, incluindo licenciamento, garantia, manutenção, suporte técnico, atualização contínua e evolução tecnológica, sem ônus adicional ao Banco da Amazônia.

6.35.3 A solução deverá ser plenamente compatível com o ambiente tecnológico do Banco da Amazônia, incluindo workloads containerizados e arquiteturas baseadas em microsserviços executadas em Red Hat OpenShift Container Platform, abrangendo aplicações distribuídas, APIs REST e bancos de dados corporativos, devendo possuir conectores nativos ou compatíveis com os middlewares institucionais.

6.35.4 A solução deverá contemplar integralmente o ambiente containerizado, incluindo aproximadamente 3.000 workloads e respectivos hosts, sendo os quantitativos detalhados na fase de Due Diligence Técnica.

6.35.5 O licenciamento deverá abranger, no mínimo, 5.000 endpoints protegidos por mês, contemplando funcionalidades de detecção comportamental, contenção, isolamento e remediação automatizada de ameaças.

6.35.6 A solução deverá operar de forma nativamente integrada ao SOC (Cyber Fusion Center), compondo um ecossistema unificado de segurança cibernética, com correlação automática e bidirecional entre eventos, vulnerabilidades, identidades e incidentes, assegurando fluxo contínuo entre detecção, análise e resposta.

6.35.7 Essa integração deverá permitir correlação cruzada, automatizada e em tempo próximo ao real, viabilizando o refinamento contínuo da detecção e a execução orquestrada de respostas, com foco na redução do Tempo Médio de Detecção (MTTD) e do Tempo Médio de Resposta (MTTR).

6.35.8 A solução deverá dispor de mecanismos avançados de análise e correlação inteligente, utilizando inteligência artificial, aprendizado de máquina e análise comportamental (UEBA), permitindo a detecção de ameaças desconhecidas, comportamentos anômalos e ataques avançados não identificados por mecanismos tradicionais.

6.35.9 A solução deverá possuir integração nativa com mecanismos de automação e orquestração de resposta (SOAR), possibilitando execução automatizada, controlada e auditável de playbooks de resposta a incidentes.

6.35.10 A solução deverá abranger, no mínimo, as seguintes capacidades:

a) Monitoramento de endpoints: detecção e resposta a malware, ransomware, exploits e comportamentos suspeitos, com capacidade de contenção automatizada;

b) Monitoramento de rede: detecção de tráfego malicioso, movimentação lateral e tentativas de exfiltração;

c) Monitoramento de aplicações e nuvem: integração com ambientes SaaS, PaaS e IaaS (Microsoft 365, Azure, AWS, Google Cloud), com detecção de desvios de comportamento e violações de política;

d) SOAR: automação de resposta, enriquecimento contextual e execução de playbooks auditáveis;

e) UEBA: identificação de desvios comportamentais com base em perfis históricos e modelos analíticos;

f) Análise forense: reconstrução de eventos, consolidação de evidências e suporte a investigações;

g) Dashboards, indicadores e relatórios operacionais: disponibilização de painéis de controle e dashboards interativos, com geração de indicadores operacionais, táticos e estratégicos, bem como relatórios analíticos contendo métricas de segurança, desempenho e risco do ambiente monitorado, assegurando consistência, rastreabilidade e suporte à tomada de decisão.

h) Proteção de Identidade em Nuvem: a solução deverá prover mecanismos de proteção de identidade baseados em análise de risco, contemplando o monitoramento contínuo de contas em ambientes online, uso de inteligência de ameaças para identificação de contas potencialmente comprometidas, avaliação de risco associada a credenciais vazadas ou roubadas, correlação com o perfil do usuário e análise contextual de autenticações, incluindo origem de IP anônimo ou suspeito, reputação da rede, detecção de comportamento anômalo, como viagem impossível, e padrões atípicos de autenticação e uso. A solução deverá permitir a aplicação dinâmica de controles de acesso baseados em risco, incluindo bloqueio, desafio adicional ou restrição de sessão, bem como registrar, auditar e integrar esses eventos aos mecanismos de investigação e resposta a incidentes.

i) Proteção de Correio Eletrônico e Colaboração: a solução deverá prover capacidades avançadas de proteção contra ameaças em comunicações eletrônicas e plataformas de colaboração corporativa, incluindo proteção contra phishing, links maliciosos, anexos maliciosos, malware e comprometimento de contas. Deverá contemplar modelos baseados em machine learning para detecção de ataques direcionados, proteção diferenciada para usuários críticos, VIPs ou com privilégios elevados, análise pré-entrega e pós-entrega de links, detonação de anexos em ambiente seguro, proteção estendida para ferramentas de colaboração, troca de arquivos e mensagens, além de integração com os mecanismos de detecção e resposta a incidentes, permitindo correlação entre eventos de e-mail, identidade, endpoint, aplicações em nuvem e atividades suspeitas.

6.35.11 A CONTRATADA deverá disponibilizar plataforma XDR baseado em SIEM com acesso seguro via web, autenticada por MFA, com trilhas completas de auditoria, permitindo:

a) Monitoramento em tempo real dos incidentes e ações executadas;

b) Visualização consolidada e correlacionada de eventos;

c) Priorização automática baseada em risco;

d) Integração bidirecional com o ITSM (ServiceNow).

6.35.12 A solução deverá assegurar:

a) Correlação automática e contínua entre eventos, vulnerabilidades e incidentes;

b) Compartilhamento estruturado de dados entre camadas analíticas e operacionais;

c) Retroalimentação contínua dos mecanismos de detecção e resposta;

d) Continuidade do fluxo operacional sem dependência de intervenção manual.

6.35.13 A solução deverá:

a) Integrar-se a feeds de Threat Intelligence (IOC, IP, URL, hash);

b) Permitir análise contextual de ameaças relevantes ao setor financeiro;

c) Suportar atividades contínuas de Threat Hunting baseadas em hipóteses, com periodicidade mínima semanal;

d) Registrar formalmente todas as análises no ITSM do Banco;

e) Contemplar, pelo menos:

i) Identificação

ii) Contenção

iii) Erradicação

iv) Recuperação

v) Lições aprendidas (com análise de causa raiz e melhoria contínua)

6.35.14 A CONTRATADA deverá fornecer relatórios mensais contendo:

a) Incidentes classificados por severidade;

b) Indicadores (MTTD, MTTR, FCR, MRR, FIC);

c) Tendências e ameaças emergentes;

d) Recomendações técnicas;

e) Avaliação da efetividade das detecções e integrações.

6.35.15 A solução deverá manter histórico mínimo de 12 meses em camada de consulta imediata, garantindo suporte a auditorias e investigações.

6.35.16 A console da solução e os manuais do fabricante podem estar em inglês;

6.35.17 Toda documentação, relatórios e entregáveis deverão ser em português;

6.35.18 Não será admitido comprometimento operacional ou de auditoria por barreira de idioma.

6.35.19 A execução do serviço deverá estar alinhada ao Anexo I-A (Especificações Técnicas) e ao Anexo I-B (NMS), assegurando níveis de desempenho, qualidade e integração operacional compatíveis com o modelo de Cyber Fusion Center do Banco da Amazônia.

6.36 **Do Serviço de Gestão de Vulnerabilidades**

6.36.1 O Serviço de Gestão de Vulnerabilidades (GVUL) tem por finalidade identificar, analisar, classificar, priorizar e acompanhar o tratamento de vulnerabilidades em todos os ativos tecnológicos do Banco da Amazônia, abrangendo servidores, estações de trabalho, dispositivos de rede, aplicações, sistemas operacionais, bancos de dados, identidades e serviços em nuvem, conforme diretrizes estabelecidas neste Termo de Referência e seus anexos.

6.36.2 O Serviço de GVUL deverá compreender o ciclo completo de gestão de vulnerabilidades, incluindo identificação, análise, priorização, tratamento, validação da correção e acompanhamento das ações corretivas até sua efetiva resolução ou aceitação formal de risco.

6.36.3 A execução do serviço deverá ocorrer de forma contínua, automatizada e orientada a risco, integrando-se ao SOC no modelo de Cyber Fusion Center, bem como às capacidades de detecção, análise e resposta do ecossistema de segurança, possibilitando a identificação tempestiva de vulnerabilidades críticas e o apoio à priorização de medidas corretivas com base em risco efetivo.

6.36.4 O serviço de GVUL deverá compartilhar, de forma contínua, estruturada, automatizada e em tempo próximo ao real, as informações de vulnerabilidades, exposições e ativos críticos com os demais componentes do ecossistema de segurança, viabilizando:

a) Correlação entre vulnerabilidades, eventos e incidentes;

b) Priorização baseada em risco efetivo (risk-based vulnerability management);

c) Apoio ao acionamento automatizado de resposta;

d) Retroalimentação contínua dos mecanismos de detecção e prevenção.

6.36.5 A Solução de GVUL (Gestão de Vulnerabilidades) a ser fornecida deverá estar em conformidade com o Anexo I-A – Especificações Técnicas da Solução Completa, incluindo garantia, manutenção, suporte técnico, atualização e evolução dos produtos, conforme requisitos estabelecidos neste Termo de Referência e demais documentos integrantes do processo licitatório.

6.36.6 As varreduras deverão suportar ambientes containerizados, pipelines CI/CD e imagens Docker/OpenShift, incluindo capacidade de análise de vulnerabilidades em tempo de build (shift-left security), bem como integração com cofres de credenciais, mecanismos de autenticação e ferramentas de detecção e resposta.

6.36.7 A integração com soluções já existentes no ambiente do Banco não se caracteriza, em hipótese alguma, como fornecimento ou substituição por nova solução, sendo as versões e parâmetros técnicos informados à CONTRATADA durante a fase de transição contratual.

6.36.8 O licenciamento da Solução de GVUL deverá abranger, no mínimo, 5.000 (cinco mil) ativos monitorados por mês, incluindo servidores físicos e virtuais, estações de trabalho, equipamentos de rede, appliances de segurança e ativos em ambiente de nuvem sob responsabilidade do Banco da Amazônia.

6.36.9 A CONTRATADA deverá disponibilizar plataforma tecnológica dedicada para gestão centralizada das vulnerabilidades, com acesso seguro via web e credenciais individuais para os usuários designados pelo Banco da Amazônia, permitindo:

a) Visualização consolidada dos resultados das varreduras;

b) Classificação automática das vulnerabilidades conforme padrões reconhecidos (CVSS, CWE, NVD);

c) Correlação entre vulnerabilidades detectadas, ativos impactados e eventos de segurança correlacionados, quando aplicável;

d) Geração de relatórios, dashboards interativos e indicadores de desempenho (KPIs e NMS), com rastreabilidade, consistência e suporte à tomada de decisão;

e) Registro e acompanhamento do ciclo de tratamento das vulnerabilidades, desde a detecção até a remediação, validação da correção ou aceitação formal de risco.

6.36.10 Os perfis de acesso deverão observar o princípio do menor privilégio, contemplando perfis operacionais, de auditoria e de leitura, cuja definição detalhada será realizada em conjunto com a CONTRATADA durante a fase de implantação.

6.36.11 O serviço deverá contemplar varreduras internas e externas, com execução mínima semanal, podendo ser ampliada conforme criticidade do ativo, nível de exposição ou ocorrência de ameaças relevantes, garantindo cobertura contínua e adaptativa.

6.36.12 As vulnerabilidades deverão ser classificadas por severidade e criticidade, considerando, além dos critérios técnicos tradicionais, como CVSS (base), exploração ativa (exploitability), contexto do ativo, exposição, criticidade de negócio, inteligência de ameaças, devendo ser priorizadas para correção com base em risco efetivo ao ambiente.

6.36.13 A CONTRATADA deverá fornecer relatórios técnicos periódicos, contendo, no mínimo:

a) Listagem de vulnerabilidades detectadas, categorizadas por nível de criticidade;
b) Análise de tendência e evolução das vulnerabilidades ao longo do tempo;
c) Recomendações técnicas de mitigação e correção, com priorização baseada em risco;
d) Registro de vulnerabilidades reincidentes, não tratadas ou com tratamento em atraso;
e) Indicadores como MTTR, nível de exposição residual, taxa de vulnerabilidades críticas abertas e correlação com incidentes;
f) Identificação de vulnerabilidades críticas associadas a ativos de alta relevância para o negócio, quando aplicável.

6.36.14 O Banco da Amazônia deverá possuir acesso completo, irrestrito, auditável e em tempo real à base de dados da solução, incluindo evidências, relatórios e trilhas de auditoria, assegurando independência na validação das informações.

6.36.15 A CONTRATADA deverá manter registro histórico das vulnerabilidades identificadas e tratadas, com retenção mínima de 12 (doze) meses em camada de armazenamento de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, assegurando a integridade, rastreabilidade, imutabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória.

6.36.16 A retenção de 48 (quarenta e oito) meses tem finalidades regulatória, forense e de auditoria. Os dados além dos 12 meses "quentes" não precisam permanecer pesquisáveis em camada normalizada pelo SIEM, podendo as consultas ser realizadas a partir de dados brutos indexados ou em outros formatos definidos na fase de implantação.

6.36.17 A retenção dos 48 (quarenta e oito) meses poderá ser atendida mediante exportação automática, segura, íntegra e verificável dos registros para ambiente de armazenamento sob custódia direta do Banco da Amazônia, devendo a CONTRATADA ser responsável pela entrega, integridade, periodicidade, rastreabilidade e segurança dessa exportação.

6.36.18 O processo de gestão de vulnerabilidades deverá contemplar, no mínimo, as seguintes etapas:

a) Descoberta de ativos: mapeamento automatizado, contínuo e validado, incluindo ativos não gerenciados e shadow IT;
b) Varredura e identificação de vulnerabilidades: execução de scans autenticados e não autenticados, conforme a natureza e criticidade dos ativos;
c) Análise e classificação: aplicação de metodologia de priorização baseada em risco efetivo, considerando criticidade, exposição e contexto operacional;
d) Correção e mitigação: encaminhamento das vulnerabilidades para as áreas responsáveis, com integração aos processos de resposta a incidentes (SRIS), quando aplicável;
e) Validação e verificação: reexecução de varreduras para comprovar a efetividade da correção e fechamento formal do ciclo;
f) Relatórios e comunicação: emissão de relatórios técnicos e gerenciais, conforme periodicidade e formato acordados com o Banco, incluindo indicadores de desempenho e risco.

6.36.19 A CONTRATADA deverá apoiar a evolução contínua da maturidade do processo de gestão de vulnerabilidades, incluindo definição de políticas, métricas, SLAs e integração com gestão de riscos corporativos.

6.36.20 A integração com o ecossistema de segurança deverá ser contínua, automatizada e orientada a risco, assegurando consistência entre detecção, análise e resposta, sem dependência de processos manuais.

6.36.21 As métricas e indicadores de desempenho relativos ao serviço de GVUL deverão seguir os parâmetros definidos no Anexo I-B – Níveis Mínimos de Serviço (NMS), devendo a CONTRATADA assegurar o cumprimento dos níveis pactuados, sob pena de aplicação das penalidades contratuais cabíveis.

6.37 **Do Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS)**

6.37.1 O Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), integrante da solução contratada, consiste na prestação de serviços especializados de contenção, mitigação, erradicação e comunicação de incidentes de segurança cibernética, em regime contínuo (24x7x365), atuando de forma imediata, contínua e coordenada com o SOC (Segunda Linha de Defesa) e sob supervisão técnica da Gerência Executiva de Infraestrutura e Produção do Banco da Amazônia. O objetivo é garantir a pronta resposta a eventos que comprometam a disponibilidade, integridade ou confidencialidade dos ativos e informações do Banco, assegurando o restabelecimento rápido das operações e a mitigação de impactos.

6.37.2 A CONTRATADA deverá manter processo contínuo e documentado de tratamento de incidentes, contemplando as fases de identificação, análise, contenção, erradicação, recuperação e lições aprendidas, conforme normas ISO/IEC 27035 e NIST SP 800-61 (Revisão 3), observadas as práticas de identificação, contenção, erradicação, recuperação e lições aprendidas amplamente consolidadas pela indústria e originalmente detalhadas na Revisão 2 (2012) da referida norma. O processo deverá incluir registro detalhado no sistema ITSM do Banco da Amazônia (ServiceNow), com rastreabilidade completa de ações, evidências, comunicações e, quando aplicável, cadeia de custódia das evidências.

6.37.3 O serviço deverá operar em regime 24x7x365, com equipes de primeiro e segundo nível alocadas para o Banco da Amazônia.

6.37.4 A CONTRATADA deverá ainda disponibilizar profissionais de terceiro nível sob demanda, acionados pelo Banco ou pelos times operacionais, para atuação em incidentes complexos, análises forenses, erradicação de ameaças persistentes e apoio técnico especializado.

6.37.5 As equipes de primeiro e segundo nível deverão executar:

a) Triagem e classificação dos alertas recebidos do SOC, das plataformas XDR baseado em SIEM e de outras fontes de detecção integradas;
b) Validação de falsos positivos e priorização de incidentes com base em criticidade, impacto ao negócio e risco cibernético;
c) Ações imediatas de contenção e mitigação de ameaças;
d) Apoio à coleta e preservação de evidências;

e) Comunicação e escalonamento tempestivo ao SOC e à Gerência Executiva de Infraestrutura e Produção do Banco da Amazônia;

f) Abertura, atualização e encerramento de tickets com registros técnicos detalhados;

g) Elaboração de relatórios técnicos e executivos de incidentes, com indicadores de desempenho e recomendações preventivas.

6.37.6 O serviço deverá manter integração contínua com o SOC, com as plataformas de detecção (XDR baseado em SIEM) e com a gestão de vulnerabilidades (GVUL), possibilitando o intercâmbio de informações técnicas, evidências e indicadores de comprometimento (IoCs), garantindo sinergia entre as linhas de defesa e o fluxo unificado de resposta a incidentes. Essa integração deverá incluir:

a) Compartilhamento bidirecional de eventos, alertas e evidências;

b) Correlação entre incidentes ativos e vulnerabilidades associadas;

c) Retroalimentação contínua dos mecanismos de detecção e prevenção;

d) Alinhamento de priorização com base em risco real;

e) Reuniões operacionais semanais e comitês técnicos mensais com a equipe do SOC e representantes da Gerência Executiva de Infraestrutura e Produção do Banco da Amazônia;

f) Acionamento automatizado e orquestrado de respostas a partir de eventos críticos, sempre que tecnicamente aplicável.

6.37.7 Os serviços deverão operar sob modelo de responsabilidade compartilhada e integrada, sendo vedada a omissão de atuação, atraso injustificado ou transferência indevida de responsabilidade sob alegação de competência de outro componente da solução.

6.37.8 A CONTRATADA deverá atuar imediatamente sempre que houver acionamento oriundo do SOC, independentemente da origem do alerta, cabendo eventual apuração de responsabilidades ser tratada posteriormente no âmbito da governança contratual.

6.37.9 Os prazos de resposta a incidentes deverão considerar modelo de SLA integrado entre detecção, análise e resposta, sendo obrigatório o início da atuação dentro dos prazos definidos nos Níveis Mínimos de Serviço, contados a partir da geração ou escalonamento do alerta, considerando o fluxo fim a fim (end-to-end), desde a detecção até a mitigação efetiva do incidente.

6.37.10 A solução deverá permitir acionamento automatizado do serviço de resposta a incidentes a partir de eventos críticos identificados nas plataformas XDR baseado em SIEM, mediante integração com playbooks automatizados (SOAR), garantindo redução do tempo de resposta, eliminação de dependências manuais e rastreabilidade completa das ações executadas.

6.37.11 A CONTRATADA deverá assegurar a qualificação técnica da equipe, exigindo, no mínimo:

a) Profissionais de primeiro e segundo nível com certificações CompTIA Security+, CompTIA CySA+, CEH ou equivalentes reconhecidas internacionalmente;

b) Profissionais de terceiro nível com certificações CompTIA Security+, CompTIA CySA+, GCIH, GCFA, CHFI, OSCP ou equivalentes, com experiência comprovada em resposta a incidentes e forense digital.

6.37.12 O Banco da Amazônia poderá realizar auditorias técnicas e operacionais, presenciais ou remotas, para verificação da execução dos serviços, do acesso aos registros e da conformidade com os procedimentos e playbooks aprovados, em conformidade com as políticas internas de segurança da informação e auditoria.

6.37.13 O serviço será mensurado e remunerado conforme os indicadores quantitativos e qualitativos definidos neste Termo de Referência e nos anexos correspondentes, observando os Níveis Mínimos de Serviço (NMS) e os Indicadores-Chave de Desempenho (KPIs) aplicáveis.

6.37.14 A matriz RACI e o fluxo de escalonamento que definem a atuação entre detecção, análise e resposta deverão considerar obrigatoriamente a integração entre os componentes da solução, assegurando fluxo contínuo, coordenado e sem interrupções no tratamento de incidentes.

6.37.15 O serviço deverá assegurar capacidade de resposta orientada a risco, considerando, no mínimo:

a) Correlação entre criticidade do ativo, severidade do incidente e exposição associada;
b) Priorização dinâmica de resposta com base em risco efetivo;
c) Integração com indicadores de risco cibernético e inteligência de ameaças;
d) Atuação coordenada com os mecanismos de detecção, análise e gestão de vulnerabilidades.

6.38 **Dos Serviços Técnicos Especializados em Segurança da Informação**

6.38.1 Os Serviços Técnicos Especializados em Segurança da Informação, executados sob demanda, destinam-se a atender a necessidades pontuais, específicas e não contínuas do Banco da Amazônia, relacionadas à segurança cibernética, auditorias, investigações técnicas, análises forenses, testes de invasão (pentests), consultorias especializadas, revisões de configuração e outras atividades correlatas, conforme solicitação formal da área de Segurança da Informação e mediante autorização expressa do Banco.

6.38.2 Cada UST corresponderá a um conjunto de horas técnicas especializadas, prestadas por profissionais com qualificação compatível à complexidade da atividade demandada, sendo vedada a utilização de perfis inferiores para execução de atividades de maior criticidade, sob pena de glosa ou rejeição da entrega.

6.38.3 As demandas sob este regime poderão incluir, entre outras:

a) Análises forenses digitais de sistemas comprometidos, incluindo coleta, preservação, cadeia de custódia e análise de evidências;
b) Testes de invasão (internos, externos ou sobre aplicações), conforme metodologias reconhecidas (OWASP, NIST, PTES ou equivalentes);
c) Apoio técnico em resposta a incidentes críticos e investigações de ciberataques, em complemento aos serviços contínuos de detecção, análise e resposta a incidentes;
d) Revisão de regras, controles e políticas de segurança, com recomendações de endurecimento (hardening);
e) Consultorias sobre conformidade com normativos regulatórios (BACEN, CMN, LGPD e correlatos);
f) Apoio em auditorias internas e externas relacionadas à segurança da informação;
g) Elaboração de pareceres técnicos, relatórios especializados e análises de risco;

h) Apoio técnico em integrações avançadas, tuning de ferramentas e otimização de regras de detecção e resposta.

6.38.4 O Banco da Amazônia poderá demandar a execução dessas atividades, conforme a natureza, criticidade e urgência da demanda, devendo a CONTRATADA garantir a disponibilidade de profissionais certificados, com experiência comprovada e aderentes às tecnologias, metodologias e padrões exigidos, sem prejuízo dos níveis de serviço pactuados.

6.38.5 Todas as atividades executadas sob o regime de UST deverão gerar relatórios técnicos conclusivos, contendo, no mínimo:

a) Descrição detalhada do escopo executado;

b) Metodologia aplicada e ferramentas utilizadas;

c) Evidências coletadas e análises realizadas;

d) Conclusões, riscos identificados e recomendações técnicas;

e) Indicação da quantidade de USTs consumidas, com memória de cálculo detalhada;

f) Quando aplicável, correlação com eventos de segurança, vulnerabilidades ou incidentes registrados nos serviços de detecção, gestão de vulnerabilidades e resposta a incidentes;

g) Quando aplicável, recomendações de melhoria contínua para os mecanismos de detecção, prevenção e resposta.

6.38.6 As demandas de serviço técnico especializado deverão ser formalmente registradas pelo Banco da Amazônia, com detalhamento do escopo, objetivos, critérios de aceite, entregáveis esperados e estimativa de esforço, devendo ser previamente aprovadas antes de sua execução.

6.38.7 Após a entrega, os resultados deverão ser avaliados, validados e homologados pela área técnica responsável, servindo de base para a validação do faturamento correspondente, podendo o Banco solicitar ajustes, complementações ou reapresentações, caso identificadas inconsistências técnicas, insuficiência de evidências ou não conformidade com os requisitos estabelecidos.

6.38.8 A execução dos serviços técnicos especializados deverá observar integração com os demais componentes da solução, assegurando que os resultados produzidos retroalimentem os processos de monitoramento, detecção, gestão de vulnerabilidades, resposta a incidentes e gestão de risco cibernético, promovendo evolução contínua da postura de segurança do Banco da Amazônia.

6.39 **Da Capacitação Técnica**

6.39.1 A capacitação técnica tem como finalidade assegurar a transferência estruturada de conhecimento e o fortalecimento das competências internas das equipes do Banco da Amazônia, promovendo autonomia na operação, interpretação, análise e acompanhamento das soluções contratadas, bem como no uso das ferramentas de SOC, gestão de vulnerabilidades e detecção e resposta estendida (XDR baseado em SIEM).

6.39.2 A CONTRATADA deverá ofertar três (3) turmas de capacitação, com carga horária mínima de 40 (quarenta) horas cada e até 15 (quinze) participantes por turma, abordando os produtos, metodologias, processos operacionais e boas práticas empregadas na execução dos serviços objeto da contratação.

6.39.3 Os treinamentos serão realizados sob demanda e poderão ser ministrados presencialmente ou de forma remota, conforme solicitação do Banco da Amazônia, devendo ser conduzidos por instrutores qualificados, certificados nas tecnologias e plataformas utilizadas e com experiência comprovada em ambientes corporativos de segurança cibernética, sem prejuízo da qualidade do conteúdo e da efetividade do aprendizado.

6.39.4 O público-alvo, o nível de profundidade e o foco das capacitações serão definidos a critério do Banco da Amazônia, devendo priorizar as equipes técnicas e operacionais de Segurança Cibernética e Infraestrutura, de modo a garantir plena capacidade de operação, análise e acompanhamento das soluções e serviços contratados.

6.39.5 O conteúdo programático mínimo das capacitações deverá incluir, entre outros:

a) Operação, administração e configuração das plataformas de monitoramento, detecção, gestão de vulnerabilidades e resposta a incidentes;

b) Práticas de monitoramento, correlação e análise de eventos de segurança (SIEM/SOAR);

c) Gestão de vulnerabilidades, priorização baseada em risco e acompanhamento de remediação;

d) Técnicas de resposta a incidentes, análise forense e tratamento de evidências;

e) Interpretação de indicadores de desempenho (KPIs) e geração de relatórios técnicos e executivos;

f) Alinhamento às políticas internas de segurança e aos normativos regulatórios aplicáveis.

6.39.6 As capacitações deverão abranger também conteúdos relacionados ao modelo operacional de Cyber Fusion Center, incluindo:

a) Integração operacional entre os componentes de detecção, análise, gestão de vulnerabilidades e resposta a incidentes;

b) Correlação multidomínio entre eventos, vulnerabilidades e incidentes;

c) Uso de Threat Intelligence na análise e priorização de riscos;

d) Técnicas de análise comportamental (UEBA);

e) Automação e orquestração de resposta a incidentes por meio de playbooks (SOAR).

6.39.7 A CONTRATADA deverá fornecer material didático completo, atualizado e em língua portuguesa, em formato digital ou físico, contendo o conteúdo ministrado, exercícios práticos, estudos de caso e exemplos aplicáveis ao ambiente do Banco da Amazônia, assegurando a rastreabilidade e reuso do conhecimento.

6.39.8 As capacitações deverão contemplar, sempre que possível, atividades práticas (hands-on), simulações de cenários reais e estudos de caso, de modo a assegurar a efetiva assimilação dos conteúdos e a aplicabilidade operacional do conhecimento adquirido.

6.39.9 Ao final de cada turma, deverão ser aplicadas avaliações de aprendizagem, teóricas e/ou práticas, e emitidos certificados individuais de participação e conclusão, contendo carga horária, conteúdo programático, identificação do instrutor responsável e critérios de avaliação adotados.

6.39.10 A CONTRATADA deverá disponibilizar relatório consolidado de capacitação, contendo, no mínimo:

a) Lista de participantes;

b) Frequência e aproveitamento;

c) Resultados das avaliações aplicadas;

d) Conteúdos ministrados;

e) Recomendações de capacitação complementar, quando aplicável;

f) Avaliação qualitativa da turma e sugestões de melhoria.

6.39.11 O Banco da Amazônia poderá, a seu critério, solicitar turmas adicionais de capacitação ou reciclagem durante a vigência contratual, mediante utilização das Unidades de Serviço Técnico (UST), observadas as condições estabelecidas neste Termo de Referência.

6.39.12 As capacitações deverão estar alinhadas ao ambiente tecnológico, aos processos operacionais e às diretrizes de segurança do Banco da Amazônia, devendo a CONTRATADA adaptar os conteúdos sempre que necessário para refletir cenários reais, integrações existentes e casos de uso efetivamente aplicáveis ao contexto institucional.

6.40 **Da Fundamentação Técnica para a Arquitetura Adotada**

6.40.1 A arquitetura tecnológica e operacional descrita neste Termo de Referência foi definida a partir de estudos técnicos realizados pela área de Segurança da Informação do Banco da Amazônia, considerando requisitos de desempenho, escalabilidade, disponibilidade, resiliência cibernética, integração e conformidade regulatória aplicáveis ao ambiente corporativo da instituição.

6.40.2 Durante o processo de análise técnica, foram avaliados modelos alternativos de implantação e operação dos serviços gerenciados de segurança, incluindo soluções on-premise, híbridas e em nuvem, com o objetivo de identificar aquele que melhor atendesse aos princípios de economicidade, continuidade operacional, resiliência, soberania dos dados e eficiência operacional.

6.40.3 A opção pela arquitetura cloud-native, fornecida no modelo Software como Serviço (SaaS) e licenciada diretamente para o Banco da Amazônia, foi motivada por critérios de eficiência técnica, otimização de custos, escalabilidade automática, resiliência operacional, atualização contínua e alinhamento às melhores práticas de mercado e às normas do Banco Central do Brasil (Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025).

6.40.4 Essa escolha permite integrar, de forma nativa, contínua, automatizada e interoperável, as capacidades de monitoramento, detecção, análise, gestão de vulnerabilidades e resposta a incidentes, compondo uma arquitetura unificada de segurança gerenciada, com governança centralizada, elasticidade operacional e plena autonomia do Banco da Amazônia sobre dados, logs, evidências e licenças.

6.40.5 A fundamentação detalhada da decisão técnica e os benefícios decorrentes da adoção do modelo SaaS em ambiente de nuvem encontram-se descritos no item 4 – Escolha da Solução, que apresenta os aspectos técnicos, regulatórios e estratégicos que nortearam a definição da solução tecnológica a ser contratada.

6.40.6 A adoção do modelo de Cyber Fusion Center estabelece um novo patamar de maturidade cibernética para o Banco da Amazônia, unificando tecnologia, processos e pessoas sob uma governança integrada, colaborativa e orientada a risco.

6.40.7 O modelo deverá assegurar integração contínua, interoperabilidade obrigatória entre os componentes da solução e atuação coordenada, sendo vedada qualquer descontinuidade operacional decorrente de falhas de integração, permitindo a antecipação de riscos, a orquestração automatizada de respostas e a incorporação contínua de inteligência de ameaças.

6.40.8 Todo o tratamento de dados institucionais do Banco da Amazônia deverá observar rigorosamente a aderência à Lei nº 13.709/2018 (LGPD), a Resolução CD/ANPD nº 15/2024, relativa à comunicação de incidentes de segurança e, quando caracterizada transferência internacional de dados pessoais, a Resolução CD/ANPD nº 19/2024, bem como ao cumprimento da Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e à garantia de preservação da segurança jurídica, confidencialidade, integridade, disponibilidade e rastreabilidade das informações.

6.40.9 A arquitetura proposta deverá operar obrigatoriamente de forma integrada, contínua, automatizada e interoperável, sendo requisito mandatório que as soluções e serviços contratados:

a) Possuam mecanismos de integração nativa ou por meio de APIs abertas, documentadas, seguras e suportadas;

b) Permitam correlação automática e bidirecional de eventos entre os componentes de monitoramento, detecção, vulnerabilidades e resposta a incidentes;

c) Operem com playbooks integrados e fluxos automatizados de resposta (SOAR);

d) Compartilhem, em tempo real, informações de contexto, risco, ativos, vulnerabilidades e incidentes;

e) Garantam acionamento automático, rastreável e auditável entre as camadas de detecção, análise e resposta;

f) Assegurem consistência, integridade, sincronização e rastreabilidade dos dados;

g) Não imponham restrições técnicas, contratuais ou comerciais à integração com soluções e ferramentas existentes no ambiente do Banco da Amazônia;

h) Permitam auditoria completa dos fluxos de integração e das ações automatizadas executadas.

6.40.10 Os serviços contratados deverão observar modelo de governança integrada, sendo obrigatória a atuação coordenada, colaborativa e contínua entre os componentes da solução, vedada qualquer limitação de atuação sob alegação de responsabilidade isolada.

6.40.11 A execução dos serviços deverá ocorrer de forma coordenada, contínua e orientada à efetividade da resposta a incidentes e à mitigação de riscos cibernéticos, sendo responsabilidade da CONTRATADA garantir a integração operacional entre as capacidades de detecção, análise, vulnerabilidades e resposta.

6.40.12 Eventuais falhas de integração, atraso na troca de informações, ausência de interoperabilidade ou descontinuidade no fluxo de tratamento de incidentes serão consideradas falhas de execução contratual, sujeitas às penalidades previstas neste Termo de Referência.

6.41 **Da Composição e Qualificações Técnicas da Equipe:**

6.41.1 Em razão da criticidade, complexidade, continuidade e sensibilidade dos serviços objeto desta contratação, a CONTRATADA deverá disponibilizar equipe técnica qualificada, multidisciplinar e compatível com a execução integral dos serviços de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, contemplando, de forma integrada, as capacidades de monitoramento, detecção, análise, resposta a incidentes, gestão de vulnerabilidades, detecção e resposta estendida, inteligência de ameaças, automação de resposta, análise forense, suporte técnico especializado e capacitação técnica.

6.41.2 A equipe técnica da CONTRATADA deverá possuir composição, experiência, certificações e conhecimentos compatíveis com a criticidade do ambiente tecnológico do Banco da Amazônia, com a natureza dos serviços contratados, com os níveis mínimos de serviço pactuados e com as exigências de disponibilidade, rastreabilidade, segurança, governança, conformidade regulatória e continuidade operacional estabelecidas neste Termo de Referência e seus anexos.

6.41.3 A CONTRATADA deverá manter, durante toda a vigência contratual, equipe técnica suficiente para assegurar a prestação contínua dos serviços em regime 24x7x365, sem prejuízo do atendimento, sob demanda ou emergencial previsto neste Termo de Referência, observados os Níveis Mínimos de Serviço (NMS), os Indicadores-Chave de Desempenho (KPIs), os prazos de resposta e os fluxos de escalonamento definidos contratualmente.

6.41.4 A composição da equipe deverá observar o modelo operacional do Cyber Fusion Center do Banco da Amazônia, contemplando, no mínimo, os seguintes perfis funcionais, sem prejuízo de outros que se mostrem necessários à plena execução do objeto:

a) Gerente de Serviços de Segurança Cibernética / Gerente de SOC;

b) Coordenador Técnico ou Líder Operacional de SOC/Cyber Fusion Center;

c) Analista de Monitoramento e Triagem de Incidentes – Nível 1 (N1);

d) Analista de Investigação e Resposta a Incidentes – Nível 2 (N2);

e) Analista Avançado de Resposta a Incidentes, Forense Digital e Investigação Especializada – Nível 3 (N3);

f) Engenheiro de Segurança, Casos de Uso, Regras de Correlação, Playbooks e Automação;

g) Especialista em SIEM, SOAR, XDR baseado em SIEM, UEBA e integração de fontes de logs;

h) Analista de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence – CTI);

i) Analista de Threat Hunting;

j) Analista de Gestão de Vulnerabilidades, Exposição e Superfície de Ataque;

k) Especialista em Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS);

l) Especialista em Segurança de Ambientes em Nuvem, Containers, APIs, Microsserviços e DevSecOps;

m) Especialista em Segurança de Aplicações, testes técnicos, análise de vulnerabilidades, hardening e apoio a pentests, quando demandado por UST;

n) Instrutores ou especialistas responsáveis pela capacitação técnica das equipes do Banco da Amazônia.

6.41.5 A CONTRATADA poderá organizar internamente sua equipe por função, escala, célula técnica, centro de competência ou modelo equivalente, desde que assegure, de forma comprovável, a cobertura integral dos perfis funcionais necessários, a segregação adequada de responsabilidades, a continuidade dos serviços, a capacidade de atendimento simultâneo e o cumprimento dos níveis de serviço estabelecidos.

6.41.6 A indicação dos perfis funcionais não implica, necessariamente, dedicação exclusiva de todos os profissionais ao contrato, salvo quando expressamente previsto neste Termo de Referência, em Ordem de Serviço, no Plano de Implantação, no Plano de Operação ou nos requisitos específicos de prestação de serviços. Todavia, a CONTRATADA deverá comprovar que possui equipe disponível, qualificada e dimensionada de forma suficiente para executar o objeto contratado, sem degradação dos serviços.

6.41.7 A CONTRATADA deverá apresentar, durante a fase de implantação e sempre que solicitado pelo Banco da Amazônia, matriz de composição da equipe técnica, contendo, no mínimo:

a) Nome completo dos profissionais alocados ou vinculados à prestação dos serviços;
b) Função exercida no contrato;
c) Perfil profissional correspondente;
d) Modalidade de atuação;
e) Escala de trabalho, quando aplicável;
f) Formação acadêmica;
g) Experiência profissional relevante;
h) Certificações técnicas e respectivas validades;
i) Responsabilidades atribuídas no fluxo operacional;
j) Níveis de acesso necessários aos sistemas, plataformas ou ambientes do Banco da Amazônia;
k) Indicação de profissionais substitutos ou de contingência, quando aplicável.

6.41.8 Os profissionais da CONTRATADA que apresentarem certificações, formação acadêmica e experiência técnica para fins de comprovação da qualificação da equipe deverão ser, preferencialmente, os mesmos que atuarão na execução dos serviços e, quando aplicável, terão acesso aos sistemas, plataformas, informações, ambientes ou dados do Banco da Amazônia.

6.41.9 É vedada a apresentação de profissionais apenas para fins formais de qualificação, sem correspondência com a equipe efetivamente mobilizada para a execução contratual, especialmente nos perfis relacionados a operação do SOC, resposta a incidentes, gestão de vulnerabilidades, análise forense, engenharia de detecção, integração de fontes, automação, XDR baseado em SIEM, SIEM, SRIS e serviços técnicos especializados.

6.41.10 A substituição de profissional indicado pela CONTRATADA deverá ser previamente comunicada ao Banco da Amazônia, acompanhada da documentação comprobatória do profissional substituto, que deverá possuir qualificação técnica igual ou superior à do profissional substituído, observado o perfil funcional correspondente.

6.41.11 A substituição de profissionais não poderá comprometer a continuidade, a qualidade, a rastreabilidade ou a efetividade dos serviços contratados, devendo a CONTRATADA assegurar transição assistida, transferência de conhecimento e atualização dos registros operacionais, sempre que a substituição envolver profissional com atuação recorrente, função crítica ou acesso a informações sensíveis.

6.41.12 Durante afastamentos, férias, licenças, desligamentos, indisponibilidades, impedimentos ou impossibilidade de atuação de membros da equipe técnica, a CONTRATADA deverá providenciar reposição tempestiva por profissional com qualificação compatível, assegurando a continuidade operacional dos serviços, sem prejuízo dos níveis mínimos de serviço e sem ônus adicional ao Banco da Amazônia.

6.41.13 A ausência de profissional qualificado, a indisponibilidade de equipe compatível, a substituição por profissional sem qualificação equivalente, a utilização de perfil inferior ao exigido ou a não manutenção da equipe mínima necessária à execução dos serviços poderá caracterizar falha de execução contratual, sujeitando a CONTRATADA às glosas, penalidades e demais consequências previstas no contrato e seus anexos.

6.41.14 Todos os profissionais alocados à execução dos serviços deverão possuir, no mínimo, habilidades pessoais e profissionais compatíveis com a criticidade das atividades, incluindo:

a) Clareza, objetividade e precisão na comunicação técnica;

b) Boa redação técnica, especialmente para elaboração de tickets, relatórios, pareceres, registros de evidências e comunicações de incidentes;

c) Capacidade de atuação sob pressão, especialmente em cenários de incidente crítico, crise cibernética ou indisponibilidade operacional;

d) Discrição, sigilo e postura compatível com o tratamento de informações sensíveis;

e) Proatividade, organização e compromisso com prazos;

f) Capacidade de trabalho em equipe e de interação com áreas técnicas, operacionais, de negócio, governança, riscos, auditoria e segurança;

g) Conhecimento e observância de políticas, normativos, procedimentos e controles de segurança da informação;

h) Capacidade de registrar tecnicamente as ações executadas, decisões tomadas, evidências coletadas e recomendações apresentadas.

6.41.15 Todos os profissionais que atuarem na execução dos serviços deverão observar integralmente as políticas, normas, procedimentos, classificações da informação, regras de controle de acesso, diretrizes de privacidade, requisitos de confidencialidade e demais normativos internos do Banco da Amazônia, bem como as disposições legais e regulatórias aplicáveis, incluindo a Lei nº 13.709/2018 (LGPD), as Resoluções do Conselho Monetário Nacional e do Banco Central do Brasil aplicáveis à segurança cibernética, à continuidade operacional e à contratação de serviços de tecnologia.

6.41.16 A formação acadêmica mínima exigida para os perfis técnicos será diploma de conclusão de curso superior reconhecido pelo Ministério da Educação – MEC, preferencialmente nas áreas de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Engenharia da Computação, Segurança da Informação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas.

6.41.17 Será admitido profissional com graduação em área diversa, desde que possua pós-graduação, especialização, mestrado, doutorado, certificações técnicas ou experiência profissional comprovada compatível com o perfil funcional exigido, cabendo ao Banco da Amazônia avaliar a suficiência e aderência da comprovação apresentada.

6.41.18 A comprovação da formação acadêmica deverá ocorrer mediante apresentação de diploma, certificado ou declaração emitida por instituição de ensino reconhecida, observadas as exigências legais aplicáveis e a possibilidade de diligência pelo Banco da Amazônia.

6.41.19 Para os perfis classificados como plenos, a CONTRATADA deverá comprovar experiência mínima de 3 (três) anos em atividades compatíveis com o perfil funcional correspondente.

6.41.20 Para os perfis classificados como seniores, especialistas, líderes técnicos, arquitetos, gerentes ou profissionais de terceiro nível, a CONTRATADA deverá comprovar experiência mínima de 5 (cinco) anos em atividades compatíveis com o perfil funcional correspondente.

6.41.21 A comprovação da experiência profissional poderá ser realizada por meio de registro em carteira de trabalho, contrato de prestação de serviços, declaração de capacidade técnica, declaração de empregador, currículos documentados, atestados, portfólios técnicos, ordens de serviço executadas ou outros documentos idôneos que demonstrem a participação efetiva do profissional nas atividades compatíveis com o perfil exigido.

6.41.22 Será admitida a soma de experiências profissionais não simultâneas para fins de comprovação do tempo mínimo exigido, desde que as atividades sejam compatíveis com o perfil profissional e devidamente comprovadas.

6.41.23 As certificações exigidas deverão estar válidas na data de sua apresentação, quando a própria certificação possuir prazo de validade. Caso a certificação não possua validade expressa, a CONTRATADA deverá demonstrar que o conhecimento técnico permanece aderente às tecnologias, metodologias e práticas exigidas para a execução contratual.

6.41.24 Caso alguma certificação seja descontinuada, substituída, renomeada ou incorporada por outro programa de certificação durante a vigência contratual, poderá ser aceita certificação equivalente, sucessora ou tecnicamente compatível, desde que apresentada justificativa pela CONTRATADA e aprovada pelo Banco da Amazônia.

6.41.25 O Banco da Amazônia poderá aceitar certificações similares ou equivalentes às indicadas neste Termo de Referência, desde que demonstrada, pela CONTRATADA, equivalência técnica quanto ao conteúdo, escopo, nível de complexidade e aderência ao perfil profissional exigido.

6.41.26 Para o perfil de Gerente de Serviços de Segurança Cibernética, Gerente de SOC ou função equivalente, o profissional deverá possuir experiência comprovada em gestão de serviços gerenciados de segurança, operação de SOC, coordenação de equipes multidisciplinares, governança operacional, gestão de indicadores, relacionamento executivo, gestão de crises cibernéticas, acompanhamento de níveis de serviço e evolução de maturidade de segurança. Deverá possuir, preferencialmente, uma ou mais certificações compatíveis com gestão, governança, risco, segurança da informação, continuidade ou serviços de TI, tais como CISSP, CISM, CISA, CRISC, CGRC, CCISO, ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ITIL, PMP, GIAC Security Leadership ou equivalentes.

6.41.27 Para o perfil de Coordenador Técnico, Líder Operacional de SOC ou função equivalente, o profissional deverá possuir experiência comprovada em coordenação operacional de SOC, CSIRT, Blue Team, Cyber Fusion Center ou serviços gerenciados de segurança, incluindo acompanhamento de escalas, supervisão técnica, revisão de tickets, priorização de incidentes, controle de qualidade das análises, escalonamento operacional e interface com equipes internas do contratante. Deverá possuir, preferencialmente, certificações como CISSP, CISM, CySA+, CASP+, SC-200, GCIH, GCIA, GMON, BTL2, ITIL ou equivalentes.

6.41.28 Para o perfil de Analista de Monitoramento e Triagem de Incidentes – Nível 1 (N1), o profissional deverá possuir experiência em monitoração contínua de eventos e alertas de segurança, triagem inicial, classificação de severidade, enriquecimento básico de eventos, validação preliminar de falsos positivos, abertura e atualização de tickets, acompanhamento de filas, registro de evidências e escalonamento estruturado para níveis superiores. Deverá possuir, preferencialmente, certificações como CompTIA Security+, CompTIA CySA+, Microsoft Security Operations Analyst SC-200, Security Blue Team BTL1, CEH ou equivalentes.

6.41.29 Para o perfil de Analista de Investigação e Resposta a Incidentes – Nível 2 (N2), o profissional deverá possuir experiência em investigação de incidentes de segurança, correlação de eventos, análise de logs, validação de hipóteses, execução de playbooks, definição de ações de contenção e mitigação, apoio à erradicação, identificação de causa raiz, documentação de evidências e elaboração de relatórios técnicos. Deverá possuir, preferencialmente, certificações como CompTIA Security+, CompTIA CySA+, CompTIA CASP+, CEH, CHFI, GCIH, GCIA, GMON, SC-200, BTL2 ou equivalentes.

6.41.30 Para o perfil de Analista Avançado de Resposta a Incidentes, Forense Digital e Investigação Especializada – Nível 3 (N3), o profissional deverá possuir experiência sênior em resposta a incidentes complexos, análise forense, investigação de ameaças persistentes, análise de artefatos, apoio à cadeia de custódia, análise de causa raiz, erradicação de ameaças, suporte a crises cibernéticas, elaboração de relatórios conclusivos e recomendação de melhorias estruturais. Deverá possuir, preferencialmente, certificações como CompTIA Security+, CompTIA CySA+, CISSP, CISM, GCIH, GCIA, GCFA, CHFI, OSCP, GREM, CASP+, BTL2 ou equivalentes.

6.41.31 Para o perfil de Engenheiro de Segurança, Casos de Uso, Regras de Correlação, Playbooks e Automação, o profissional deverá possuir experiência em engenharia de detecção, criação e tuning de regras de correlação, desenvolvimento de casos de uso, mapeamento MITRE ATT&CK, integração de fontes de logs, automação e orquestração de resposta, redução de falsos positivos, validação de efetividade de detecções e documentação técnica. Deverá possuir, preferencialmente, certificações como SC-200, GMON, GCDA, GCIA, GCIH, GCTI, MITRE ATT&CK Defender, Elastic Certified Analyst, BTL2, certificações oficiais do fabricante das soluções ofertadas ou equivalentes.

6.41.32 Para o perfil de Especialista em SIEM, SOAR, XDR baseado em SIEM, UEBA e integração de fontes de logs, o profissional deverá possuir experiência comprovada na implantação, configuração, sustentação, integração e operação de plataformas de segurança, incluindo coleta, parsing, normalização, correlação, enriquecimento, integração por API, conectores, agentes, coletores, automação de resposta, análise comportamental, detecção baseada em identidade e integração com ITSM, GRC, Data Lake ou ferramentas equivalentes. Deverá possuir, preferencialmente, certificações oficiais do fabricante da solução ofertada, além de certificações correlatas como SC-200, AZ-500, CySA+, CASP+, GMON, GCIA, GCIH, GCDA ou equivalentes.

6.41.33 Para o perfil de Analista de Inteligência de Ameaças Cibernéticas (CTI), o profissional deverá possuir experiência em coleta, análise, correlação e disseminação de inteligência de ameaças, incluindo uso de fontes abertas, comerciais e comunitárias, análise de campanhas, atores de ameaça, TTPs, IOCs, IOAs, vulnerabilidades exploradas ativamente, ameaças relevantes ao setor financeiro e recomendações de mitigação. Deverá possuir, preferencialmente, certificações como CTIA, GCTI, GREM, GCFA, CySA+, CASP+, BTL2 ou equivalentes.

6.41.34 Para o perfil de Analista de Threat Hunting, o profissional deverá possuir experiência em caça proativa de ameaças baseada em hipóteses, investigação de comportamento anômalo, análise retrospectiva de logs, uso de frameworks como MITRE ATT&CK, análise de endpoints, investigação de movimentação lateral, identificação de ameaças não detectadas automaticamente e retroalimentação de regras de detecção e playbooks. Deverá possuir, preferencialmente, certificações como GCTH, GCDA, GDAT, GCIA, GMON, GCTI, SC-200, CySA+, CASP+, BTL2 ou equivalentes.

6.41.35 Para o perfil de Analista de Gestão de Vulnerabilidades, Exposição e Superfície de Ataque, o profissional deverá possuir experiência em descoberta de ativos, execução de varreduras autenticadas e não autenticadas, gestão do ciclo de vida de vulnerabilidades, priorização baseada em risco, CVSS, EPSS, inteligência de ameaças, exposição externa, shadow IT, validação de falsos positivos, acompanhamento de remediação, patch management, hardening e elaboração de relatórios técnicos e executivos. Deverá possuir, preferencialmente, certificações como CySA+, CASP+, Certified Vulnerability Assessor, GIAC Enterprise Vulnerability Assessor, GSNA, Qualys Vulnerability Management, Tenable/Nessus, AZ-500, SC-300 ou equivalentes.

6.41.36 Para os perfis vinculados ao Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), a CONTRATADA deverá assegurar profissionais com experiência em contenção, mitigação, erradicação, recuperação, execução de procedimentos operacionais, registro de evidências, acionamento de equipes técnicas, comunicação de incidentes, atualização de tickets e integração operacional com o SOC, XDR baseado em SIEM e GVUL. Para profissionais de primeiro e segundo nível, deverão ser aceitas, preferencialmente, certificações como Security+, CySA+, CEH, SC-200, BTL1 ou equivalentes. Para profissionais de terceiro nível, deverão ser aceitas, preferencialmente, certificações como GCIH, GCFA, CHFI, OSCP, GCIA, GREM, CASP+, BTL2 ou equivalentes.

6.41.37 Para os perfis de Segurança de Ambientes em Nuvem, Containers, APIs, Microsserviços e DevSecOps, a CONTRATADA deverá possuir profissionais com experiência em segurança de workloads em nuvem, ambientes SaaS, PaaS e IaaS, Red Hat OpenShift, containers, imagens, pipelines CI/CD, APIs REST, microsserviços, análise de vulnerabilidades em aplicações e infraestrutura como código, integração de controles de segurança em esteiras DevSecOps, segurança de identidades em nuvem e proteção de ambientes híbridos. Deverão ser aceitas, preferencialmente, certificações como AZ-500, SC-300, certificações oficiais de provedores de nuvem, certificações de containers/Kubernetes/OpenShift, certificações de AppSec, CySA+, CASP+, Security+ ou equivalentes.

6.41.38 Para os perfis relacionados aos Serviços Técnicos Especializados sob demanda, a CONTRATADA deverá disponibilizar profissionais com qualificação compatível com a complexidade da Ordem de Serviço, abrangendo, conforme o caso, análise forense, resposta a incidentes críticos, testes de invasão, revisão de configuração, hardening, auditoria técnica, análise de risco, segurança de aplicações, DevSecOps, análise de malware, segurança em nuvem, integração avançada, tuning de ferramentas, elaboração de pareceres técnicos e apoio a auditorias. As certificações exigíveis deverão guardar relação direta com a atividade demandada, podendo incluir, entre outras, CISSP, CISM, CISA, CRISC, OSCP, GPEN, GWAPT, CHFI, GCFA, GCIH, GREM, CEH, CySA+, CASP+, certificações de fabricantes ou equivalentes.

6.41.39 Para os profissionais responsáveis pela capacitação técnica, a CONTRATADA deverá comprovar experiência na tecnologia, solução, metodologia ou processo objeto do treinamento, bem como certificação técnica compatível com a solução ofertada ou com o conteúdo a ser ministrado. Os instrutores deverão possuir capacidade didática, domínio técnico e experiência prática suficiente para conduzir treinamentos com atividades teóricas, práticas, estudos de caso, simulações e exercícios aplicáveis ao ambiente do Banco da Amazônia.

6.41.40 A CONTRATADA deverá assegurar que os profissionais responsáveis por funções críticas, incluindo operação do SOC, resposta a incidentes, administração de plataformas, integração de fontes de logs, alteração de regras, execução de playbooks, análise forense, gestão de vulnerabilidades e acesso a dados sensíveis, utilizem credenciais individuais, nominativas e intransferíveis, com autenticação multifator, segregação de funções e rastreabilidade integral das ações executadas.

6.41.41 O acesso dos profissionais da CONTRATADA aos ambientes, sistemas, plataformas, dados, logs, evidências, tickets, dashboards ou informações do Banco da Amazônia deverá ser limitado ao estritamente necessário à execução das atividades autorizadas, observando o princípio do menor privilégio, a necessidade de conhecimento, a segregação de funções e os procedimentos de concessão, revisão e revogação de acessos definidos pelo Banco.

6.41.42 A CONTRATADA deverá manter registro atualizado dos profissionais autorizados a acessar ambientes ou informações do Banco da Amazônia, incluindo data de concessão, perfil de acesso, justificativa, função exercida, período de validade e data de revogação, quando aplicável.

6.41.43 Antes do início da atuação em ambientes do Banco da Amazônia, os profissionais da CONTRATADA deverão assinar termo de confidencialidade, ciência de responsabilidade, compromisso de observância às políticas de segurança da informação e demais instrumentos exigidos pelo Banco, quando aplicável.

6.41.44 A CONTRATADA deverá garantir que seus profissionais atuem em conformidade com os procedimentos, playbooks, fluxos de escalonamento, critérios de classificação de incidentes, matriz RACI, políticas internas, normas de segurança e orientações operacionais aprovadas pelo Banco da Amazônia.

6.41.45 A CONTRATADA deverá manter programa interno de capacitação, reciclagem e atualização técnica de sua equipe, assegurando aderência contínua às tecnologias contratadas, às ameaças emergentes, às melhores práticas de segurança cibernética, aos frameworks aplicáveis e às mudanças no ambiente tecnológico do Banco da Amazônia.

6.41.46 Sempre que houver atualização relevante das soluções contratadas, alteração de arquitetura, inclusão de novos módulos, mudança de fabricante, integração de novas fontes, revisão de playbooks ou alteração de procedimentos críticos, a CONTRATADA deverá assegurar a atualização técnica dos profissionais envolvidos, sem ônus adicional ao Banco da Amazônia.

6.41.47 A CONTRATADA deverá apresentar, quando solicitado, evidências de capacitação, reciclagem, certificação, experiência e atualização técnica da equipe, incluindo certificados, registros de treinamento, currículos, declarações, relatórios de participação, provas de proficiência ou documentos equivalentes.

6.41.48 O Banco da Amazônia poderá realizar diligências, entrevistas técnicas, validações documentais, auditorias ou reuniões de avaliação com os profissionais indicados pela CONTRATADA, com o objetivo de verificar a aderência entre a qualificação apresentada e as atividades executadas.

6.41.49 A apresentação de documentação inverídica, inconsistente, incompleta, desatualizada ou incompatível com o perfil profissional indicado poderá ensejar rejeição do profissional, solicitação de substituição, glosa, aplicação de penalidade ou adoção das demais medidas previstas contratualmente, sem prejuízo de apuração de responsabilidade.

6.41.50 A CONTRATADA deverá apresentar, no Plano de Implantação e no Plano de Operação, a estratégia de mobilização, composição, escala, cobertura, acionamento e substituição da equipe técnica, demonstrando como será assegurada a prestação contínua dos serviços, a cobertura dos diferentes níveis de análise, a atuação prevista, o atendimento a incidentes críticos e o suporte às demandas sob UST.

6.41.51 O Plano de Operação deverá contemplar, no mínimo:

a) Estrutura organizacional da equipe técnica;
b) Papéis e responsabilidades por perfil;
c) Fluxos de acionamento e escalonamento;
d) Escala de atendimento 24x7x365;
e) Modelo de supervisão técnica;
f) Profissionais responsáveis por comunicação com o Banco da Amazônia;
g) Mecanismos de continuidade em caso de indisponibilidade de profissionais;
h) Procedimentos de handover entre turnos;
i) Processo de substituição e transição assistida;
j) Estratégia de controle de qualidade das análises e registros;
k) Processo de revisão periódica da aderência da equipe aos requisitos contratuais.

6.41.52 A CONTRATADA deverá assegurar que a operação 24x7x365 conte com mecanismos formais de handover entre turnos, contendo registro das ocorrências abertas, incidentes em andamento, hipóteses investigadas, pendências, escalonamentos, ações executadas, riscos identificados, eventos críticos e demais informações necessárias à continuidade da análise e resposta.

6.41.53 A equipe técnica deverá estar apta a atuar de forma integrada com as equipes do Banco da Amazônia, incluindo Segurança Cibernética, Infraestrutura, Produção, Governança de TI, Gestão de Riscos, Privacidade, Auditoria, Jurídico, Continuidade de Negócios, Canais Digitais, Prevenção a Fraudes e demais áreas envolvidas no tratamento de incidentes, observadas as competências institucionais de cada área.

6.41.54 A atuação da equipe da CONTRATADA não substitui as responsabilidades institucionais do Banco da Amazônia, mas deverá assegurar suporte técnico especializado, execução operacional, análise qualificada, registro tempestivo, recomendações técnicas e apoio à tomada de decisão, conforme os papéis e responsabilidades definidos no contrato, na matriz RACI e nos procedimentos aprovados.

6.41.55 A CONTRATADA deverá assegurar que os profissionais alocados ao contrato conheçam e observem as regras de classificação da informação, proteção de dados, sigilo bancário, privacidade, segurança cibernética, confidencialidade, continuidade operacional e resposta a incidentes aplicáveis ao Banco da Amazônia.

6.41.56 O Banco da Amazônia poderá, a qualquer tempo, solicitar a substituição de profissional da CONTRATADA que não demonstre qualificação compatível, descumpra normas internas, apresente conduta inadequada, comprometa a segurança das informações, deixe de cumprir procedimentos estabelecidos, registre análises insuficientes ou cause risco operacional, de segurança, regulatório ou reputacional.

6.41.57 A substituição solicitada pelo Banco da Amazônia deverá ocorrer em prazo compatível com a criticidade da função, sem prejuízo da continuidade dos serviços e sem ônus adicional, devendo o profissional substituto atender integralmente aos requisitos de qualificação exigidos para o perfil correspondente.

6.41.58 A CONTRATADA deverá garantir que a equipe técnica mantenha conhecimento atualizado sobre o ambiente tecnológico do Banco da Amazônia, seus ativos críticos, integrações, fontes de logs, sistemas monitorados, fluxos de resposta, ferramentas corporativas, parâmetros de criticidade e contexto de negócio necessário à correta priorização de eventos, vulnerabilidades e incidentes.

6.41.59 A equipe técnica deverá atuar de forma orientada a risco, considerando, em suas análises, a criticidade dos ativos, a exposição, a severidade técnica, a probabilidade de exploração, a inteligência de ameaças, os impactos operacionais, financeiros, reputacionais e regulatórios, bem como os requisitos de continuidade e conformidade aplicáveis ao Banco da Amazônia.

6.41.60 O não atendimento aos requisitos de composição, qualificação, certificação, experiência, disponibilidade, atualização, substituição, documentação ou comprovação da equipe técnica poderá ensejar glosas, rejeição de entregas, impedimento de atuação do profissional, aplicação de penalidades e demais medidas previstas neste Termo de Referência, no contrato e em seus anexos, sem prejuízo da apuração de eventuais impactos operacionais, de segurança ou regulatórios.

6.42 **Quadros Consolidados da Composição e Qualificações Técnicas da Equipe de Profissionais para a Realização dos Serviços:**

6.42.1 Os quadros a seguir apresentam a relação dos perfis profissionais mínimos, organizados por categoria de serviço, com seus respectivos códigos de identificação, CBOs de referência, função, modalidade de atuação e observação de dimensionamento.

CATEGORIA 1 – SERVIÇOS DE SOC, XDR BASEADO EM SIEM, MONITORAMENTO E RESPOSTA A INCIDENTES – REGIME 24X7X365

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços de SOC – Nível 1	Analista de Monitoramento e Triagem de Incidentes SOC – N1	Analista de Monitoramento e Triagem de Incidentes Pleno	2124-10 / 2123-10	SOC-N1	24x7x365, conforme Plano de Operação aprovado pelo Banco	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Serviços de SOC – Nível 2	Analista de Investigação e Resposta a Incidentes SOC – N2	Analista de Investigação e Resposta a Incidentes Pleno	2123-20	SOC-N2	24x7x365, conforme Plano de Operação aprovado pelo Banco	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Serviços de SOC – Nível 3	Analista Avançado de Resposta a Incidentes SOC – N3	Analista de Investigação, Resposta a Incidentes e Forense Digital Sênior	2123-20	SOC-N3	24x7x365, conforme criticidade	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Engenharia de Detecção e Automação	Engenheiro de Casos de Uso, Regras de Correlação e Playbooks	Engenheiro de Segurança da Informação Sênior	2124-15 / 2124-25	ENG-DET	Conforme necessidade do serviço	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Gestão do SOC / Cyber Fusion Center	Gerente de Serviços de Segurança Cibernética / Gerente de SOC	Gerente de SOC Sênior / Gerente Geral MSSP	1425-25	GER-SOC	Atuação com disponibilidade para reuniões executivas e crises	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação

Coordenação Operacional	Coordenador Técnico / Líder Operacional de SOC	Coordenador Técnico de SOC / Líder de Operações de Segurança	1425-25 / 2123-20	COORD-SOC	Atuação conforme Plano de Operação aprovado pelo Banco	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 1 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco, suficiente para regime 24x7x365, cumprimento dos Níveis Mínimos de Serviço e fluxos de detecção, análise, resposta, escalonamento e gestão operacional.

CATEGORIA 2 – SERVIÇOS DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS – CTI

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços de CTI	Analista de Inteligência de Ameaças	Analista de Inteligência de Ameaças Pleno ou Sênior	2123-20	CTI	Atuação conforme necessidade do serviço	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Serviços de CTI	Especialista em Análise de Malware e Artefatos Maliciosos	Especialista em Análise de Malware Sênior	2123-20	MALWARE	Sob demanda ou em apoio a incidentes críticos	Conforme demanda e Plano de Operação	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 2 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco, suficiente para suportar inteligência de ameaças, enriquecimento de alertas, produção de relatórios, apoio ao SOC, Threat Hunting, GVUL e resposta a incidentes.

CATEGORIA 3 – SERVIÇOS DE THREAT HUNTING

Categoria de	**Função**	**Perfil**	**CBO de**	**Cód.**	**Modalidade**	**Qtde Total**	**Qtde Inicial**

Serviço		Profissional	Referência	Identificação do Perfil			
Serviços de Threat Hunting	Analista de Caçada de Ameaças	Analista de Threat Hunting Pleno ou Sênior	2123-20	THREAT-HUNT	Atuação conforme TR e Plano de Operação	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 3 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco da Amazônia, suficiente para execução de atividades contínuas e proativas de Threat Hunting, com periodicidade mínima definida neste Termo de Referência.

CATEGORIA 4 – SERVIÇOS DE GESTÃO DE VULNERABILIDADES, EXPOSIÇÃO E SUPERFÍCIE DE ATAQUE

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços de GVUL	Analista de Gestão de Vulnerabilidades, Exposição e Superfície de Ataque	Analista de Gestão de Vulnerabilidades Pleno ou Sênior	2123-20	GVUL	Atuação conforme necessidade do serviço	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 4 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco, suficiente para suportar a gestão de, no mínimo, 5.000 ativos monitorados por mês, conforme previsto neste Termo de Referência.

CATEGORIA 5 – SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA NA PRIMEIRA LINHA DE DEFESA – SRIS

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços de SRIS – Nível 1	Analista de Resposta a Incidentes de Primeira Linha – N1	Analista de Resposta a Incidentes Pleno	2123-20 / 2124-10	SRIS-N1	Atuação conforme TR e Plano de Operação	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação

Serviços de SRIS – Nível 2	Analista de Resposta a Incidentes de Primeira Linha – N2	Analista de Resposta a Incidentes Pleno ou Sênior	2123-20	SRIS-N2	Atuação conforme TR e Plano de Operação	Conforme dimensionamento da CONTRATADA aprovado pelo Banco	Conforme Plano de Implantação e Operação
Serviços de SRIS – Nível 3	Especialista Avançado em Resposta a Incidentes, Forense e Erradicação	Especialista em Resposta a Incidentes Sênior	2123-20	SRIS-N3	Atuação conforme criticidade	Conforme demanda e Plano de Operação	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 5 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco, suficiente para assegurar atuação imediata, contínua e coordenada nas fases de contenção, mitigação, erradicação, recuperação e comunicação de incidentes.

CATEGORIA 6 – SERVIÇOS DE SEGURANÇA EM NUVEM, CONTAINERS, APIs, MICROSSERVIÇOS E DEVSECOPS

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços de Segurança em Nuvem, Containers e DevSecOps	Especialista em Segurança de Nuvem, Containers, APIs, Microsserviços e DevSecOps	Especialista em Segurança da Informação / AppSec / DevSecOps Pleno ou Sênior	2123-20 / 2124-15	CLOUD-DEVSECOPS	Atuação conforme necessidade	Conforme demanda e Plano de Operação	Conforme Plano de Implantação e Operação

TOTAL CATEGORIA 6 – Quantitativo dimensionado pela CONTRATADA e aprovado pelo Banco, suficiente para suportar integração, monitoramento e segurança de ambientes cloud-native, SaaS, Red Hat OpenShift, containers, APIs, microsserviços e pipelines CI/CD.

CATEGORIA 7 – SERVIÇOS TÉCNICOS ESPECIALIZADOS SOB DEMANDA

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Serviços	Especialista	Especialista	2123-20 /	ESP-UST	Atuação	Conforme	Conforme

Técnicos Especializados	em Segurança da Informação sob demanda	compatível com a Ordem de Serviço, podendo abranger forense, pentest, hardening, AppSec, malware, nuvem, auditoria, integração avançada, tuning ou parecer técnico	2124-15 / 2124-25		conforme necessidade	Ordem de Serviço	Ordem de Serviço

TOTAL CATEGORIA 7 – Serviços executados sob demanda, mediante Ordem de Serviço, mensurados em Unidades de Serviço Técnico (UST), observados os critérios de aceite, qualificação e complexidade definidos neste Termo de Referência e seus anexos.

CATEGORIA 8 – SERVIÇOS DE CAPACITAÇÃO TÉCNICA

Categoria de Serviço	Função	Perfil Profissional	CBO de Referência	Cód. Identificação do Perfil	Modalidade	Qtde Total	Qtde Inicial
Capacitação Técnica	Instrutor Técnico / Especialista de Capacitação	Instrutor ou Especialista certificado na tecnologia, solução, metodologia ou processo objeto do treinamento	2123-20 / 2332-25, quando aplicável	INSTRUTOR	Atuação conforme solicitação do Banco	Conforme turmas previstas no TR	Conforme solicitação do Banco

TOTAL CATEGORIA 8 – Serviços prestados sob demanda, conforme turmas, carga horária, conteúdo programático e critérios de aceite previstos neste Termo de Referência.

6.42.2 Qualificação dos Profissionais por Categoria de Serviço

I - SERVIÇOS DE SOC – NÍVEL 1

Função: Analista de Monitoramento e Triagem de Incidentes SOC – N1	
Perfil Profissional: Analista de Monitoramento e Triagem de Incidentes	
Responsável pelo monitoramento contínuo, triagem inicial, classificação de severidade, enriquecimento básico de eventos, validação preliminar de falsos positivos, abertura e atualização de tickets e escalonamento estruturado para níveis superiores.	
Formação Acadêmica	Modo de Comprovação
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	Modo de Comprovação
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em atividades relacionadas à triagem inicial de alertas de segurança em ambientes de monitoramento contínuo, SOC, NOC, CSIRT ou Blue Team, abrangendo classificação preliminar de incidentes, validação básica de falsos positivos, abertura e categorização de tickets, enriquecimento de contexto, acompanhamento de SLAs/NMS, escalonamento e participação em handovers de turno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	Modo de Comprovação
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: Microsoft Security Operations Analyst SC-200; EC-Council Certified Ethical Hacker – CEH; CompTIA Security+; CompTIA Cybersecurity Analyst – CySA+; Security Blue Team – Blue Team Level 1 – BTL1; ou	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

certificação similar ou equivalente aprovada pelo Banco da Amazônia.	

II - SERVIÇOS DE SOC – NÍVEL 2

Função: Analista de Investigação e Resposta a Incidentes SOC – N2	
Perfil Profissional: Analista de Investigação e Resposta a Incidentes	
Responsável por investigações aprofundadas, correlação de múltiplos eventos, análise de logs, validação de hipóteses, execução de playbooks, definição de ações de contenção e mitigação, identificação de causa raiz, documentação técnica e apoio à resposta a incidentes.	
Formação Acadêmica	Modo de Comprovação
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	Modo de Comprovação
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em atividades relacionadas à resposta a incidentes de segurança em ambientes SOC, CSIRT ou Blue Team, incluindo execução de playbooks, correlação de eventos, análise técnica de alertas, coordenação com equipes de infraestrutura, recomendação de ações corretivas, validação de medidas implementadas, preparação de evidências digitais e elaboração de relatórios técnicos. Perfil Sênior, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência nas mesmas atividades do perfil pleno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	Modo de Comprovação
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: ISC2 CISSP; EC-Council CEH; EC-Council CHFI; OSCP; CompTIA CySA+; CompTIA CASP+; GIAC GMON; GIAC GCIA; GIAC GCIH; Security Blue Team BTL2; Microsoft SC-200; ou certificação similar ou equivalente aprovada pelo Banco.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

III - SERVIÇOS DE SOC – NÍVEL 3

Função: Analista Avançado de Resposta a Incidentes SOC – N3	
Perfil Profissional: Analista de Investigação, Resposta a Incidentes e Forense Digital	
Responsável pelo tratamento de incidentes complexos, análise forense, investigação de ameaças persistentes, análise de artefatos, apoio à cadeia de custódia, erradicação de ameaças, suporte a crises cibernéticas, análise de causa raiz e elaboração de relatórios conclusivos.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Sênior: deve possuir, no mínimo, 5 (cinco) anos de experiência profissional em atividades relacionadas à resposta avançada a incidentes de segurança em ambientes SOC, CSIRT ou Blue Team, com atuação em incidentes complexos, análise forense, investigação de ameaças persistentes, erradicação de ameaças, análise de causa raiz, preparação e preservação de evidências digitais, participação em comitês de crise e apoio técnico à recuperação de ambientes comprometidos.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.

Certificações	Modo de Comprovação
Deve possuir, preferencialmente, certificações compatíveis com resposta avançada, investigação ou forense digital, tais como: ISC2 CISSP; ISACA CISM; EC-Council CEH; EC-Council CHFI; OSCP; GIAC GCIH; GIAC GCIA; GIAC GCFA; GIAC GREM; CompTIA CASP+; Security Blue Team BTL2; ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

IV - ENGENHARIA DE CASOS DE USO, REGRAS DE CORRELAÇÃO E PLAYBOOKS

Função: Engenheiro de Casos de Uso, Regras de Correlação e Playbooks	
Perfil Profissional: Engenheiro de Segurança da Informação	
Responsável pela engenharia de detecção, criação e tuning de regras de correlação, desenvolvimento de casos de uso, mapeamento MITRE ATT&CK, integração de fontes de logs, automação e orquestração de resposta, validação de efetividade de detecções e documentação técnica.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Sênior: deve possuir, no mínimo, 5 (cinco) anos de experiência profissional em engenharia de detecção de ameaças cibernéticas, desenvolvimento de casos de uso para plataformas SIEM, criação e otimização de regras de correlação, redução de falsos positivos, desenvolvimento de playbooks automatizados para SOAR, integração de feeds de Threat Intelligence, validação de analytics de segurança e colaboração com equipes de SOC, CTI, Threat Hunting e resposta a incidentes.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: CompTIA CASP+; CompTIA CySA+; Elastic Certified Analyst; GIAC GMON; GIAC GCTI; GIAC GDAT; GIAC GCDA; GIAC GCIH; GIAC GCIA; Microsoft SC-200; MITRE ATT&CK Defender; Security Blue Team BTL2; certificações oficiais do fabricante da solução ofertada; ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

V - GESTÃO DO SOC / CYBER FUSION CENTER

Função: Gerente de Serviços de Segurança Cibernética / Gerente de SOC	
Perfil Profissional: Gerente de SOC Sênior / Gerente Geral MSSP	
Responsável pela gestão, governança, supervisão executiva e acompanhamento dos serviços de SOC, Cyber Fusion Center, XDR baseado em SIEM, GVUL, SRIS, serviços técnicos especializados e capacitação técnica, assegurando a qualidade, continuidade, integração e evolução dos serviços contratados.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas, Administração, Engenharia ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado em Tecnologia da Informação, Segurança da Informação, Governança, Gestão de Riscos, Continuidade ou Gestão de Projetos.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Sênior: deve possuir, no mínimo, 5 (cinco) anos de experiência profissional em gestão de serviços gerenciados de segurança, liderança de SOC, CSIRT, Blue Team ou Cyber Fusion Center, coordenação de equipes multidisciplinares, gestão de indicadores, relacionamento executivo, governança contratual, gestão de crises cibernéticas, acompanhamento de níveis de serviço, planejamento de evolução de maturidade e interface com áreas de segurança, infraestrutura, riscos, auditoria, jurídico, privacidade e negócio.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, certificações compatíveis com gestão, governança, risco, segurança da informação, continuidade ou serviços de TI, tais como: ISC2 CISSP; ISACA CISM; ISACA CISA; ISACA CRISC; ISC2 CGRC; EC-Council CCISO; ISO/IEC 27001; ISO/IEC 27005; ISO 31000; ITIL; PMP; GIAC Security Leadership; ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

VI - SERVIÇOS DE CTI

Função: Analista de Inteligência de Ameaças

Perfil Profissional: Analista de Inteligência de Ameaças Cibernéticas
Responsável pela coleta, produção, análise, correlação e disseminação de inteligência de ameaças cibernéticas, com foco em campanhas, atores de ameaça, TTPs, IOCs, IOAs, ameaças relevantes ao setor financeiro e recomendações de mitigação.

Formação Acadêmica	Modo de Comprovação
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em atividades relacionadas à produção de inteligência de ameaças cibernéticas, incluindo coleta, análise e correlação de informações provenientes de fontes abertas, comerciais e comunitárias, elaboração de relatórios táticos e operacionais, análise de campanhas, atores de ameaça, TTPs, IOCs e apoio à priorização de riscos. Perfil Sênior, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência nas mesmas atividades do perfil pleno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: CompTIA CASP+; CompTIA CySA+; CREST Registered Threat Intelligence Analyst – CRTIA; EC-Council CTIA; GIAC GCTI; GIAC GCFA; GIAC GREM; Security Blue Team BTL2; ou certificação similar ou equivalente aprovada pelo Banco.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

VII - SERVIÇOS DE THREAT HUNTING

Função: Analista de Caçada de Ameaças

Perfil Profissional: Analista de Threat Hunting	
Responsável pela investigação e busca proativa de ameaças não detectadas automaticamente nos ambientes, sistemas, identidades, redes, aplicações, endpoints e serviços em nuvem do Banco da Amazônia.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em atividades de caça e investigação proativa de ameaças cibernéticas em ambientes SOC, CTI, CTH, CSIRT ou Blue Team, incluindo hunting baseado em hipóteses, uso de frameworks como MITRE ATT&CK, análise de endpoints, investigação de logs, buscas retrospectivas no SIEM, identificação de movimentação lateral, elaboração de relatórios de hunting e colaboração com equipes de SOC e resposta a incidentes. Perfil Sênior, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência nas mesmas atividades do perfil pleno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.

Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: CompTIA CASP+; CompTIA CySA+; GIAC GCTH; GIAC GCDA; GIAC GDAT; GIAC GCIA; GIAC GMON; GIAC GCTI; Microsoft SC-200; Security Blue Team BTL2; Elastic Certified Analyst; ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

VIII – SERVIÇOS DE GESTÃO DE VULNERABILIDADES

Função: Analista de Gestão de Vulnerabilidades, Exposição e Superfície de Ataque	
Perfil Profissional: Analista de Gestão de Vulnerabilidades	
Responsável pela descoberta contínua, análise, priorização e gestão do ciclo de vida de vulnerabilidades e da superfície de ataque nos ecossistemas híbridos do Banco da Amazônia, incluindo servidores, estações, redes, nuvem, aplicações, identidades, containers e ativos expostos.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em Gestão de Vulnerabilidades, incluindo execução de varreduras autenticadas e não autenticadas, priorização baseada em risco, CVSS, EPSS, inteligência de ameaças, gestão do ciclo de remediação, patch management, validação de falsos positivos, descoberta de ativos, identificação de exposição externa, shadow IT, recomendações de hardening e elaboração de relatórios técnicos e executivos. Perfil Sênior, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência nas mesmas atividades do perfil pleno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, no mínimo uma das certificações abaixo, dentro do período de validade, quando aplicável: CompTIA CySA+; CompTIA CASP+; EC-Council Certified Vulnerability Assessor – CVA; GIAC Enterprise Vulnerability Assessor – GEVA; GIAC GSNA; Microsoft SC-300; Microsoft AZ-500; Qualys Vulnerability Management; Tenable/Nessus; ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

Função: Analista ou Especialista de Resposta a Incidentes de Segurança na Primeira Linha de Defesa	
Perfil Profissional: Analista de Resposta a Incidentes / Especialista em SRIS	
Responsável pela atuação operacional imediata na contenção, mitigação, erradicação, recuperação, registro de evidências, acionamento de equipes técnicas, comunicação de incidentes, atualização de tickets e integração operacional com SOC, XDR baseado em SIEM e GVUL.	
Formação Acadêmica	**Modo de Comprovação**
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfis N1 e N2: devem possuir, no mínimo, 3 (três) anos de experiência profissional em atividades de resposta a incidentes, suporte técnico especializado, contenção, mitigação, registro de evidências, execução de procedimentos operacionais, escalonamento e atualização de chamados. Perfil N3 ou especialista, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência em resposta avançada a incidentes, análise forense, erradicação de ameaças persistentes, recuperação de ambientes e apoio técnico em crises cibernéticas.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Para profissionais de primeiro e segundo nível, devem ser aceitas, preferencialmente, certificações como CompTIA Security+, CompTIA CySA+, CEH, Microsoft SC-200, BTL1 ou equivalentes. Para profissionais de terceiro nível, devem ser aceitas, preferencialmente, certificações como GIAC GCIH, GIAC GCFA, CHFI, OSCP, GIAC GCIA, GIAC GREM, CompTIA CASP+, BTL2 ou equivalentes.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

X – SEGURANÇA EM NUVEM, CONTAINERS, APIs, MICROSSERVIÇOS E DEVSECOPS

Função: Especialista em Segurança de Nuvem, Containers, APIs, Microsserviços e DevSecOps
Perfil Profissional: Especialista em Segurança da Informação / AppSec / DevSecOps

Responsável por apoiar a segurança de workloads em nuvem, ambientes SaaS, PaaS e IaaS, Red Hat OpenShift, containers, imagens, pipelines CI/CD, APIs REST, microsserviços, infraestrutura como código, identidades em nuvem e ambientes híbridos.

Formação Acadêmica	Modo de Comprovação
Todos os integrantes devem possuir diploma de conclusão de curso de graduação na área de Tecnologia da Informação, Ciência da Computação, Sistemas de Informação, Segurança da Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas, em curso reconhecido pelo Ministério da Educação, ou nível superior completo em outra área, com pós-graduação, especialização, mestrado ou doutorado na área de Tecnologia da Informação ou Segurança da Informação.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
Perfil Pleno: deve possuir, no mínimo, 3 (três) anos de experiência profissional em atividades relacionadas à segurança de ambientes em nuvem, containers, pipelines CI/CD, APIs, microsserviços, DevSecOps, AppSec ou infraestrutura como código. Perfil Sênior, quando aplicável: deve possuir, no mínimo, 5 (cinco) anos de experiência nas mesmas atividades do perfil pleno.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, ordens de serviço executadas ou documentação equivalente que comprove a participação efetiva do profissional nas atividades.
Certificações	**Modo de Comprovação**
Deve possuir, preferencialmente, certificações compatíveis com o escopo, tais como Microsoft AZ-500, Microsoft SC-300, certificações oficiais de provedores de nuvem, certificações de containers, Kubernetes, OpenShift, AppSec, DevSecOps, CompTIA Security+, CompTIA CySA+, CompTIA CASP+, ou certificação similar ou equivalente aprovada pelo Banco da Amazônia.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

XI – SERVIÇOS TÉCNICOS ESPECIALIZADOS SOB DEMANDA

Função: Especialista em Segurança da Informação sob demanda	
Perfil Profissional: Especialista compatível com a Ordem de Serviço	
Responsável pela execução de atividades sob demanda, incluindo análise forense, resposta a incidentes críticos, testes de invasão, revisão de configuração, hardening, auditoria técnica, análise de risco, segurança de aplicações, DevSecOps, análise de malware, segurança em nuvem, integração avançada, tuning de ferramentas, pareceres técnicos e apoio a auditorias.	
Formação Acadêmica	**Modo de Comprovação**
O profissional deverá possuir formação acadêmica compatível com a natureza, criticidade e complexidade da Ordem de Serviço, preferencialmente na área de Tecnologia da Informação, Segurança da Informação, Ciência da Computação, Sistemas de Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas ou áreas correlatas.	Diploma, certificado ou declaração de conclusão de curso, fornecido por instituição de ensino reconhecida, sem prejuízo de diligência pelo Banco da Amazônia.
Experiência / Qualificação	**Modo de Comprovação**
O profissional deverá possuir experiência comprovada compatível com a complexidade da atividade demandada na Ordem de Serviço, sendo vedada a utilização de perfil inferior para execução de atividades de maior criticidade. Para atividades especializadas, críticas ou de alta complexidade, deverá ser comprovada experiência mínima de 5 (cinco) anos em atividades correlatas.	Registro em carteira de trabalho, contrato de prestação de serviços, declaração de empregador, atestado de capacidade técnica, currículo documentado, portfólio técnico, ordens de serviço executadas ou documentação equivalente.
Certificações	**Modo de Comprovação**
As certificações deverão guardar relação direta com a atividade demandada, podendo incluir, entre outras: CISSP, CISM, CISA, CRISC, OSCP, GPEN, GWAPT, CHFI, GCFA, GCIH, GREM, CEH, CySA+, CASP+, certificações oficiais de fabricantes, certificações de nuvem, AppSec, DevSecOps, forense, pentest ou equivalentes.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

XII – CAPACITAÇÃO TÉCNICA

Função: Instrutor Técnico / Especialista de Capacitação	
Perfil Profissional: Instrutor ou Especialista certificado na tecnologia, solução, metodologia ou processo objeto do treinamento	
Responsável pela transferência estruturada de conhecimento às equipes do Banco da Amazônia, por meio de treinamentos técnicos, atividades práticas, estudos de caso, simulações, exercícios e materiais didáticos.	
Formação Acadêmica	Modo de Comprovação
O instrutor deverá possuir formação acadêmica ou experiência	Diploma, certificado, declaração de conclusão de curso,

técnica compatível com o conteúdo a ser ministrado, preferencialmente na área de Tecnologia da Informação, Segurança da Informação, Ciência da Computação, Sistemas de Informação, Engenharia da Computação, Redes de Computadores, Análise e Desenvolvimento de Sistemas, Educação Corporativa ou áreas correlatas.	comprovação de experiência como instrutor, currículo documentado ou documentação equivalente.
Experiência / Qualificação	Modo de Comprovação
O instrutor deverá comprovar experiência prática na tecnologia, solução, metodologia ou processo objeto do treinamento, bem como capacidade didática para conduzir atividades teóricas, práticas, estudos de caso, simulações e exercícios aplicáveis ao ambiente do Banco da Amazônia.	Currículo documentado, declaração de empregador, atestado de capacidade técnica, certificados de instrutoria, avaliações de treinamentos anteriores, portfólio ou documentação equivalente.
Certificações	Modo de Comprovação
O instrutor deverá possuir certificação técnica compatível com a solução, tecnologia, metodologia ou processo objeto do treinamento, incluindo, quando aplicável, certificações oficiais do fabricante ou certificações reconhecidas em segurança da informação, SOC, SIEM, XDR baseado em SIEM, SOAR, GVUL, resposta a incidentes, forense, nuvem, DevSecOps ou áreas correlatas.	Apresentação dos certificados, declarações oficiais, registros públicos de certificação ou documentação equivalente, sujeita à validação pelo Banco da Amazônia.

6.42.3 Regras Complementares de Acesso, Conduta e Manutenção da Equipe

Requisito	Exigência	Modo de Comprovação / Observação
Controle de acesso	Os profissionais que atuarem em funções críticas deverão utilizar credenciais individuais, nominativas e intransferíveis, com autenticação multifator, segregação de funções e rastreabilidade integral das ações executadas.	Evidências de configuração de acesso, trilhas de auditoria, registros de concessão, revisão e revogação de acessos.
Princípio do menor privilégio	O acesso aos sistemas, plataformas, dados, logs, evidências, tickets, dashboards e informações do Banco da Amazônia deverá ser limitado ao estritamente necessário à execução das atividades autorizadas.	Matriz de acessos, registros de autorização, perfis concedidos e evidências de revisão periódica.
Termo de confidencialidade	Antes do início da atuação em ambientes do Banco da Amazônia, os profissionais da CONTRATADA deverão assinar termo de confidencialidade, ciência de responsabilidade e compromisso de	Termos assinados e arquivados, disponibilizados ao Banco quando solicitado.

	observância às políticas internas do Banco.	
Atualização técnica	A CONTRATADA deverá manter programa interno de capacitação, reciclagem e atualização técnica da equipe, abrangendo tecnologias contratadas, ameaças emergentes, melhores práticas, frameworks aplicáveis e mudanças no ambiente do Banco.	Certificados, registros de treinamento, trilhas de capacitação, relatórios de participação ou provas de proficiência.
Plano de Operação	A CONTRATADA deverá apresentar Plano de Operação contendo estrutura organizacional da equipe, papéis e responsabilidades, fluxos de acionamento, escala 24x7x365, supervisão técnica, comunicação com o Banco, handover entre turnos, substituição e controle de qualidade.	Plano de Operação aprovado pelo Banco da Amazônia, atualizado durante toda a vigência contratual.
Handover entre turnos	A operação 24x7x365 deverá contar com mecanismos formais de passagem de turno, contendo incidentes em andamento, hipóteses investigadas, pendências, escalonamentos, ações executadas, riscos identificados e eventos críticos.	Registros de passagem de turno, tickets, relatórios operacionais e evidências no ITSM.
Diligência e validação	O Banco da Amazônia poderá realizar diligências, entrevistas técnicas, validações documentais, auditorias ou reuniões de avaliação com os profissionais indicados pela CONTRATADA.	Documentação apresentada pela CONTRATADA, entrevistas técnicas e registros de validação pelo Banco.
Substituição por solicitação do Banco	O Banco da Amazônia poderá solicitar substituição de profissional que não demonstre qualificação compatível, descumpra normas internas, apresente conduta inadequada, comprometa a segurança ou gere risco operacional, regulatório ou reputacional.	Comunicação formal do Banco e apresentação de substituto com qualificação igual ou superior.
Penalidades por não conformidade	O não atendimento aos requisitos de composição, qualificação, certificação, experiência, disponibilidade, atualização, substituição, documentação ou comprovação da equipe técnica poderá ensejar glosas, rejeição de entregas, impedimento de atuação do profissional e aplicação de penalidades.	Apuração contratual, relatórios de não conformidade, registros de NMS/KPI, auditorias e demais evidências aplicáveis.

6.43 **Informações Complementares:**

6.43.1 Quantidade de marcas do Banco da Amazônia: atualmente duas marcas institucionais (“Banco da Amazônia” e “BASA”), bem como marcas de produtos (“Verdinho” e “Verdinha”), com previsão de expansão conforme crescimento da atuação institucional.

6.43.2 Quantidade de IPs do Banco da Amazônia: aproximadamente 2.048 endereços IP, compreendendo dois blocos /24 IPv4 e um bloco /48 IPv6.

6.43.3 Quantidade de domínios do Banco da Amazônia: aproximadamente 30 domínios institucionais.

6.43.4 Quantidade de takedowns: média de 10 (dez) takedowns efetivos por mês, acumuláveis ao longo do ano, considerando a utilização de solução de Digital Risk Protection (DRP) que o Banco dispõe (Plataforma Vydar).

7 DIRETRIZES GERAIS DA CONTRATAÇÃO

7.1 A contratação deverá observar o modelo de Serviços Gerenciados de Segurança Operacional Cibernética (SOC), estruturado como Cyber Fusion Center (CFC), com prestação integrada das capacidades de XDR baseado em SIEM, Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), conforme as especificações técnicas deste Termo de Referência e seus anexos.

7.2 A CONTRATADA será responsável pela disponibilização, implantação, integração, operação, sustentação, manutenção, suporte, atualização e evolução contínua das soluções e serviços necessários à execução integral do objeto, assumindo responsabilidade fim a fim pelos resultados contratados.

7.3 Os serviços continuados deverão ser prestados em regime 24x7x365, observados os Níveis Mínimos de Serviço estabelecidos no Anexo I-B e os requisitos específicos aplicáveis a cada componente da solução.

7.4 A solução deverá ser fornecida em arquitetura cloud-native, no modelo Software como Serviço (SaaS), incluindo todas as licenças, subscrições, direitos de uso, infraestrutura, armazenamento, processamento, agentes, coletores, APIs, conectores, suporte e demais componentes necessários à prestação dos serviços, sem caracterizar aquisição definitiva, licenciamento patrimonial autônomo, cessão permanente de direitos de uso ou incorporação de ativos ao patrimônio do Banco da Amazônia.

7.5 As capacidades que compõem o Cyber Fusion Center deverão operar de forma integrada, interoperável e coordenada, assegurando compartilhamento contínuo de informações, preservação do contexto e correlação entre eventos, vulnerabilidades, ativos, identidades, alertas e incidentes, bem como fluxo contínuo e auditável entre detecção, análise e resposta.

7.6 A solução deverá possuir capacidade de integração com o ecossistema tecnológico do Banco, por meio de APIs abertas, conectores nativos ou mecanismos equivalentes, incluindo, quando aplicável, ITSM/ServiceNow, GRC, Data Lake, Active Directory, ferramentas de observabilidade, ambientes de microsserviços, containers e Red Hat OpenShift Container Platform.

7.7 Os requisitos funcionais, técnicos, de capacidade, desempenho, segurança, integração e operação específicos das soluções de XDR baseado em SIEM, GVUL e SRIS serão aqueles definidos no capítulo Descrição da Solução e Especificações Técnicas dos

Serviços, no Anexo I-A e nos demais anexos aplicáveis, evitando-se sua reprodução neste item.

7.8 A implantação e a transição operacional deverão observar integralmente os marcos, etapas e prazos estabelecidos no Item 4 deste Termo de Referência, incluindo planejamento, implementação, testes, UAT, Go-Live, operação assistida, estabilização e aceite.

7.9 A solução ofertada será submetida à Prova de Conceito – POC, anteriormente à contratação e conforme o Anexo I-C, não se confundindo essa etapa com os testes, homologação, UAT e aceite da solução efetivamente implantada.

7.10 Os Serviços Técnicos Especializados serão prestados exclusivamente sob demanda, mediante Ordem de Serviço previamente autorizada pelo Banco, até o limite estimado de 5.000 UST, sem obrigação de consumo mínimo ou integral, observados os critérios estabelecidos no Catálogo de Serviços Técnicos Especializados em UST.

7.11 As três turmas de capacitação técnica previstas na contratação serão executadas sob demanda, nos termos das especificações deste Termo de Referência, sem obrigação de utilização integral pelo Banco.

7.12 A CONTRATADA deverá manter equipe multidisciplinar, qualificada e adequadamente dimensionada para executar integralmente os serviços, cumprir os NMS e assegurar continuidade operacional, observados os perfis, experiências, qualificações, regras de substituição e demais requisitos definidos no capítulo específico de composição e qualificação da equipe técnica.

7.13 A CONTRATADA deverá observar integralmente os requisitos de segurança da informação, confidencialidade, sigilo bancário, proteção de dados pessoais, gestão de acessos, rastreabilidade, integridade de evidências, auditabilidade e demais controles estabelecidos pelo Banco da Amazônia e pela legislação e regulamentação aplicáveis.

7.14 A solução deverá assegurar alta disponibilidade, resiliência, continuidade operacional, escalabilidade e mecanismos de contingência e recuperação compatíveis com a criticidade dos serviços contratados.

7.15 A CONTRATADA deverá manter documentação técnica e operacional completa, atualizada, versionada e auditável, abrangendo arquitetura, integrações, fontes de dados, configurações relevantes, casos de uso, regras de detecção, playbooks, procedimentos, fluxos de escalonamento e demais artefatos necessários à operação, fiscalização e transição dos serviços.

7.16 Será admitida subcontratação parcial exclusivamente nas hipóteses, limites e condições definidos neste Termo de Referência, permanecendo vedada a transferência a terceiros da responsabilidade pelos serviços essenciais do núcleo operacional contínuo do Cyber Fusion Center e permanecendo a CONTRATADA integralmente responsável perante o Banco por todas as obrigações contratuais.

7.17 A CONTRATADA deverá assegurar ao Banco acesso, disponibilidade e portabilidade de seus dados, logs, evidências, registros, configurações e documentação, inclusive durante a transição ou encerramento contratual, sendo vedada sua retenção como condição para encerramento dos serviços.

7.18 Todos os custos necessários ao atendimento dos requisitos da contratação deverão estar contemplados nos preços ofertados, não sendo admitida cobrança adicional por licenças, módulos, funcionalidades, infraestrutura ou componentes necessários ao atendimento integral dos requisitos obrigatórios.

7.19 O atendimento aos requisitos deste item deverá ocorrer em conjunto com as especificações técnicas, Níveis Mínimos de Serviço, critérios de medição, requisitos de implantação, POC e demais condições estabelecidas neste Termo de Referência e seus anexos.

8 ESCOLHA DA SOLUÇÃO

8.1 Considerando as limitações técnicas e operacionais do modelo atualmente empregado pelo Banco da Amazônia, baseado em solução de SIEM on-premise licenciada para a CONTRATADA, optou-se pela adoção de uma arquitetura cloud-native, fornecida integralmente no modelo Software como Serviço (SaaS), com licenciamento direto em nome do Banco da Amazônia e operação integrada aos serviços gerenciados de segurança cibernética, contemplando, de forma unificada, as capacidades de monitoramento, detecção, gestão de vulnerabilidades e resposta a incidentes, assegurada a interoperabilidade obrigatória entre todos os componentes da solução.

8.2 Da Realização de Prova de Conceito (POC)

8.2.1 Como etapa obrigatória do processo licitatório, a licitante classificada em primeiro lugar deverá submeter a solução ofertada à Prova de Conceito (Proof of Concept – POC), conforme critérios, condições, escopo e metodologia estabelecidos no Anexo I-C – Prova de Conceito (POC), parte integrante deste Termo de Referência.

8.2.2 A POC tem por finalidade validar, de forma prática e objetiva, a aderência técnica, funcional, operacional e de integração da solução aos requisitos definidos neste Termo de Referência, especialmente no contexto do modelo de Cyber Fusion Center, incluindo as capacidades de:

a) Monitoramento e detecção (XDR baseado em SIEM);

b) Gestão de vulnerabilidades (GVUL);

c) Resposta a incidentes (SRIS);

d) Integração multidomínio, correlação e automação (SOAR/UEBA);

e) Governança, rastreabilidade e geração de indicadores.

8.2.3 A realização da POC possui caráter eliminatório, sendo condição obrigatória para aceitação da proposta, nos termos definidos no Anexo I-C – Prova de Conceito (POC).

8.2.4 A solução será considerada APROVADA, quando atender integralmente aos requisitos mínimos estabelecidos ou REPROVADA, quando não atender a qualquer requisito obrigatório.

8.2.5 Em caso de reprovação na POC, a licitante será desclassificada, sendo convocada a próxima classificada, observada a ordem de classificação do certame.

8.2.6 A POC deverá ser executada conforme cronograma, formato, critérios de avaliação e regras de execução definidos no Anexo I-C – Prova de Conceito (POC), incluindo:

a) Execução prática em ambiente controlado ou remoto;

b) Demonstração funcional completa da solução;

c) Apresentação de evidências técnicas;

d) Validação pela equipe técnica do Banco da Amazônia.

8.2.7 A licitante deverá disponibilizar todos os recursos necessários à execução da POC, sem qualquer ônus para o Banco da Amazônia, incluindo:

a) Ambiente funcional da solução;

b) Acesso às funcionalidades necessárias;

c) Profissionais qualificados para demonstração.

8.2.8 O resultado da POC será formalizado por meio de relatório técnico emitido pela área competente do Banco da Amazônia, contendo evidências, análises e conclusão quanto à aprovação ou reprovação da solução.

8.2.9 A aprovação na POC constitui condição indispensável para adjudicação do objeto e posterior contratação.

8.3 Essa escolha assegura maior autonomia institucional, redução de custos indiretos e fortalecimento da governança de segurança cibernética, eliminando a dependência técnica de infraestrutura física da CONTRATADA e permitindo que o Banco mantenha plena titularidade, controle e continuidade do uso das soluções e dos dados, inclusive em cenários de transição contratual ou encerramento do contrato.

8.4 O modelo SaaS proporciona elasticidade e escalabilidade automáticas dentro da capacidade contratada, simplifica o provisionamento de recursos e dispensa investimentos em hardware e licenças locais, garantindo alta disponibilidade, resiliência operacional, atualização tecnológica contínua e redução de riscos associados à obsolescência.

8.5 Além disso, a nova solução ampliará o período de retenção de logs e eventos de segurança, passando de 20 (vinte) dias para 12 (doze) meses em camada de armazenamento de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), assegurando integridade, rastreabilidade, imutabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória, atendendo integralmente às exigências do Banco Central do Brasil (Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025), bem como às boas práticas de governança de dados.

8.6 A retenção de 48 (quarenta e oito) meses tem finalidades regulatória, forense e de auditoria. Os dados além dos 12 meses “quentes” não precisam permanecer pesquisáveis em camada normalizada pelo SIEM, podendo as consultas ser realizadas a partir de dados brutos indexados ou em outros formatos definidos na fase de implantação.

8.7 A retenção dos 48 (quarenta e oito) meses poderá ser atendida mediante exportação automática, segura, íntegra e verificável dos logs para ambiente de armazenamento sob custódia direta do Banco da Amazônia, devendo a CONTRATADA ser responsável pela entrega, integridade, periodicidade, rastreabilidade e segurança dessa exportação.

8.8 O período de 12 (doze) meses de logs “quentes” está fundamentado em requisitos regulatórios, auditoria, investigações e governança interna. Eventuais adequações poderão ser realizadas, desde que previamente validadas e aceitas pelo Banco da Amazônia, mantida a retenção total mínima de 60 (sessenta) meses.

8.9 A solução adotada deverá permitir integração nativa, contínua, automatizada e interoperável entre múltiplas camadas de inteligência e automação, contemplando:

a) SIEM (Security Information and Event Management): coleta, correlação e análise centralizada de eventos de segurança;

b) UEBA (User and Entity Behavior Analytics): detecção comportamental baseada em análise de desvios e anomalias;

c) SOAR (Security Orchestration, Automation and Response): execução automatizada de playbooks e respostas a incidentes;

d) Threat Intelligence: integração com bases globais de indicadores de comprometimento (IOC, IP, hash e URL);

e) Inteligência Artificial Generativa: apoio a investigações, contextualização de alertas e recomendação de respostas em linguagem natural.

8.10 Essa arquitetura integrada, interoperável e orientada a dados visa aumentar a maturidade cibernética do Banco da Amazônia, reduzir o tempo médio de detecção e resposta (MTTD/MTTR), automatizar processos investigativos e de correlação avançada e proporcionar visão unificada, contextualizada e preditiva sobre ameaças e vulnerabilidades do ambiente tecnológico.

8.11 A adoção do modelo SaaS em nuvem pública ou híbrida, conforme critérios de segurança definidos neste Termo de Referência e em seus anexos, elimina a necessidade de manutenção e atualização de infraestrutura on-premise, reduz riscos de obsolescência, amplia a eficiência operacional e assegura maior flexibilidade para evolução tecnológica ao longo da vigência contratual.

8.12 O modelo contratual basear-se-á em pagamentos condicionados ao cumprimento dos Níveis Mínimos de Serviço (NMS), conforme o Anexo I-B, assegurando entregas mensuráveis, qualidade contínua, rastreabilidade das atividades executadas e governança orientada a resultados na prestação dos serviços gerenciados de segurança cibernética.

8.13 Com a implantação do SOC, no modelo de Cyber Fusion Center, o Banco da Amazônia passará a operar um modelo de defesa cibernética baseado em inteligência, correlação multidomínio, automação e resposta coordenada, elevando sua maturidade cibernética aos níveis exigidos pelas melhores práticas do Sistema Financeiro Nacional.

8.14 Deverá ser assegurada, de forma obrigatória, a atuação coordenada, integrada, contínua e sob responsabilidade única da CONTRATADA, sendo vedada qualquer descontinuidade operacional decorrente de falhas de integração entre os componentes da solução.

8.15 Com essa escolha, o Banco da Amazônia alinha-se às melhores práticas de mercado e às diretrizes de resiliência operacional, continuidade de negócios e segurança da informação estabelecidas pelo Banco Central do Brasil, pela Lei nº 13.709/2018 (LGPD) e pelas normas internacionais ABNT NBR ISO/IEC 27001:2022, ISO/IEC 27017:2026 e ISO/IEC 27018:2025, consolidando um modelo sustentável, auditável, interoperável e em conformidade com as exigências regulatórias do Sistema Financeiro Nacional.

8.16 Os parâmetros quantitativos, a volumetria contratual e os critérios de medição associados a essa arquitetura encontram-se detalhados a seguir, estabelecendo as bases técnicas e operacionais que nortearão o dimensionamento, a mensuração de desempenho, a validação das entregas e o acompanhamento contínuo dos serviços de segurança gerenciada.

8.17 A escolha da arquitetura não implica obrigatoriedade de fornecimento por um único fabricante, sendo admitida a composição da solução por diferentes tecnologias integradas, desde que garantidas, de forma mandatória, a plena integração técnica, a interoperabilidade operacional, a continuidade dos fluxos de detecção e resposta e a responsabilidade integral da CONTRATADA pela operação fim a fim da solução.

8.18 As soluções deverão, obrigatoriamente:

a) Permitir integração por meio de APIs abertas, documentadas e seguras, conectores nativos ou mecanismos equivalentes;

b) Compartilhar, de forma automatizada e em tempo real, eventos, alertas, indicadores de risco, contexto de incidentes e informações de ativos;

c) Operar com playbooks integrados e fluxos automatizados de resposta (SOAR), assegurando orquestração entre os componentes da solução;

d) Assegurar correlação multidomínio entre eventos, vulnerabilidades, identidades, ativos e incidentes em tratamento;

e) Garantir consistência, rastreabilidade, integridade e sincronização das informações entre as plataformas;

f) Não impor quaisquer restrições técnicas, contratuais ou comerciais à integração com soluções existentes no ambiente do Banco da Amazônia;

g) Permitir acionamento automático entre as camadas de detecção, análise e resposta, sem dependência de intervenção manual do Banco.

8.19 **Da Volumetria e Dimensionamento Técnico**

8.19.1 A volumetria estimada para a contratação dos Serviços Gerenciados de Segurança Operacional Cibernética foi definida com base nas necessidades operacionais do Banco da Amazônia, nos registros históricos de consumo de logs do contrato vigente e nas projeções de crescimento do ambiente tecnológico institucional, incluindo a ampliação do escopo de monitoramento de eventos de segurança, a incorporação de logs transacionais oriundos de sistemas críticos de negócio e a evolução dos serviços digitais.

8.19.2 O dimensionamento proposto tem por objetivo assegurar cobertura integral dos ambientes monitorados, desempenho operacional estável e capacidade de escalabilidade para absorver o aumento progressivo do volume de eventos, ativos, identidades e superfícies de ataque ao longo da vigência contratual, observando as características de elasticidade, alta disponibilidade, resiliência e expansão sob demanda inerentes ao modelo SaaS em nuvem.

8.19.3 Os quantitativos definidos constituem referência técnica e econômica inicial para o dimensionamento da contratação, devendo ser considerados como baseline contratual, sendo admitidos ajustes decorrentes da evolução do ambiente tecnológico, desde que previamente avaliados e formalmente aprovados pelo Banco da Amazônia, sem prejuízo da continuidade operacional, da previsibilidade contratual e da adequada precificação dos serviços.

8.19.4 O dimensionamento da solução foi estruturado de forma integrada, considerando a operação unificada dos serviços de monitoramento, detecção, análise, gestão de vulnerabilidades e resposta a incidentes, sob responsabilidade única da CONTRATADA, assegurando coerência técnica, interoperabilidade entre os componentes e alinhamento com o modelo de Cyber Fusion Center adotado pelo Banco da Amazônia.

8.19.5 A volumetria deverá contemplar, no mínimo, os seguintes parâmetros técnicos:

a) Capacidade de ingestão de logs e eventos de segurança de, no mínimo, 600 GB (seiscentos gigabytes) por dia;

b) Monitoramento de, no mínimo, 5.000 (cinco mil) ativos tecnológicos por mês, incluindo servidores, estações de trabalho, dispositivos de rede, aplicações e ativos em nuvem;

c) Proteção e monitoramento de, no mínimo, 5.000 (cinco mil) endpoints por mês, contemplando estações de trabalho, notebooks, servidores físicos e virtuais;

d) Monitoramento de aproximadamente 5.000 (cinco mil) identidades digitais ativas, considerando credenciais corporativas integradas ao ambiente de autenticação (Active Directory e serviços correlatos);

e) Cobertura de ambientes containerizados, incluindo aproximadamente 3.000 workloads em plataformas Kubernetes/OpenShift, conforme detalhamento a ser refinado na fase de Due Diligence Técnica;

f) Retenção de logs e eventos de segurança por período mínimo de 60 (sessenta) meses, sendo 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses em camada de arquivamento seguro (“cold storage”).

8.19.6 Os quantitativos definidos consideram não apenas o cenário atual do ambiente tecnológico do Banco da Amazônia, mas também projeções de crescimento orgânico, expansão de serviços digitais, aumento do volume transacional, evolução da superfície de ataque e incorporação de novas fontes de dados, evitando a necessidade de aditivos contratuais frequentes.

8.19.7 A CONTRATADA deverá garantir que a solução seja capaz de operar dentro dos limites de volumetria estabelecidos, sem degradação de desempenho, perda de dados, limitação de funcionalidades ou impacto na qualidade dos serviços prestados, sendo responsável pela adequação contínua da infraestrutura lógica e dos recursos necessários à sustentação da operação.

8.19.8 A solução deverá possuir mecanismos nativos de escalabilidade horizontal e vertical, capazes de absorver variações de carga e picos de processamento, garantindo a continuidade dos serviços, a integridade dos dados e o cumprimento dos níveis mínimos de serviço (NMS) estabelecidos.

8.19.9 Eventuais variações relevantes de volumetria, decorrentes de mudanças estruturais no ambiente do Banco da Amazônia, deverão ser tratadas no âmbito da governança contratual, com análise técnica, impacto econômico e formalização adequada, preservando o equilíbrio econômico-financeiro do contrato e a continuidade da prestação dos serviços.

8.19.10 A seguir, os componentes e respectivas especificações quantitativas e justificativas técnicas:

Componente	Descrição	Unidade de Medida	Quantidade Estimada	Justificativa Técnica
1	Solução de SIEM (Security Information and Event Management) para gerenciamento centralizado de informações e eventos de segurança	GB/dia	600	Conforme relatório de consumo de logs do SIEM atualmente em operação, o ambiente processa uma média diária de 316,69 GB de eventos. Todavia, esse volume não inclui logs transacionais provenientes dos

				principais sistemas críticos do Banco da Amazônia (Banklink, Mobile Banking, Internet Banking, NextBank, Cabine SPB e demais aplicações core), atualmente não integrados ao SIEM. Considerando a ampliação da cobertura de monitoração para esses sistemas e a inclusão de novas plataformas oriundas do Programa de Transformação Digital, estima-se a necessidade de capacidade mínima de ingestão de 600 GB/dia, garantindo margem técnica suficiente para o crescimento projetado do ambiente e evitando restrições operacionais ou contratuais à expansão do volume de logs monitorados.
2	Solução de GVUL (Gestão de Vulnerabilidades) para detecção, priorização e tratamento contínuo de vulnerabilidades	Ativo monitorado/mês	5.000/mês	O quantitativo de 5.000 (cinco mil) ativos monitorados por mês foi estabelecido considerando a quantidade total estimada de estações de trabalho, notebooks e

				servidores (físicos e virtuais) corporativos do Banco da Amazônia – abrangendo aproximadamente 3.000 estações e notebooks e 2.000 servidores distribuídos entre a matriz e as unidades regionais.
3	Solução de XDR (Extended Detection and Response) baseado em SIEM para correlação avançada de eventos e resposta automatizada a incidentes	Endpoint protegido/mês	5.000/mês	O quantitativo de 5.000 (cinco mil) endpoints protegidos por mês foi definido com base na mesma estimativa de ativos corporativos monitorados pelo GVUL, garantindo cobertura integral de estações de trabalho, notebooks e servidores (físicos e virtuais) localizados na matriz e nas unidades regionais.
4	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas (XDR baseado em SIEM), Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL) e Serviço e Solução Integrada de Resposta a	Mês	60	A alocação de 60 meses para os Serviços Gerenciados de SIEM, GVUL e XDR baseado em SIEM, em regime contínuo (24x7x365), justifica-se pela necessidade de garantir a alta disponibilidade do ecossistema de segurança cibernética do Banco da Amazônia, conforme o

	Incidentes de Segurança na Primeira Linha de Defesa (SRIS) – todos em regime contínuo (24x7x365)			modelo Cyber Fusion Center descrito neste Termo de Referência. Esses serviços constituem o núcleo técnico da defesa digital do Banco, permitindo coleta, correlação e resposta automatizada a incidentes com uso de Inteligência Artificial, automação (SOAR) e análise comportamental (UEBA). O período contratual de 60 meses assegura continuidade, maturidade processual e aderência às Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, à LGPD e às normas ISO/IEC 27035, garantindo estabilidade, evolução tecnológica e retorno estratégico do investimento, em conformidade com este Termo de Referência. A alocação de 60 meses para o Serviço e Solução

				Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) justifica-se pela natureza crítica e ininterrupta das operações do Banco da Amazônia, que demandam disponibilidade e resiliência operacional permanentes. Conforme este Termo de Referência, o serviço é responsável por identificar, conter, erradicar e recuperar incidentes cibernéticos, atuando de forma integrada e sinérgica com o SOC (Segunda Linha de Defesa) e sob supervisão técnica da Gerência Executiva de Infraestrutura e Produção. O prazo assegura continuidade institucional, estabilidade operacional e maturidade dos processos de defesa, com equipes especializadas e certificadas alinhadas às normas ISO/IEC 27035 e NIST SP 800-61 Rev. 3 (2025). Além disso, garante

				conformidade com a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e a Lei nº 13.709/2018 (LGPD), viabilizando uma atuação preventiva e coordenada frente ao aumento da complexidade das ameaças digitais e à criticidade dos serviços bancários, conforme este Termo de Referência.
5	Serviços Técnicos Especializados sob demanda (consultorias, revisões, integrações e customizações de segurança)	UST	5.000	A alocação de 5.000 Unidades de Serviço Técnico (USTs) para os Serviços Técnicos Especializados sob demanda justifica-se pela necessidade de o Banco da Amazônia dispor de capacidade técnica flexível e mensurável para execução de atividades complexas e pontuais de segurança cibernética, não cobertas pelos serviços gerenciados contínuos do SOC. As USTs abrangem

				consultorias especializadas, integrações de ferramentas, revisões de configuração, customizações de segurança, auditorias, testes de invasão e análises forenses, essenciais à adaptação contínua da arquitetura de segurança às mudanças tecnológicas, regulatórias e operacionais. As atividades serão mensuradas em UST, conforme critérios definidos no Anexo I-A – Especificações Técnicas da Solução Completa, garantindo rastreabilidade e controle quantitativo das entregas, em conformidade com este Termo de Referência.
6	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda)	Turma	3 (com 15 participantes cada)	A alocação, sob demanda, de 3 turmas de capacitação técnica, com até 15 participantes cada, justifica-se pela necessidade de assegurar a transferência efetiva de conhecimento e o fortalecimento das competências internas das equipes do Banco da

				Amazônia na operação das soluções contratadas (SIEM, GVUL e XDR baseado em SIEM), dentro do modelo Cyber Fusion Center. Conforme este Termo de Referência, os treinamentos abrangem operações de monitoramento e correlação de eventos, gestão de vulnerabilidades, resposta a incidentes, análise forense e automação de playbooks (SOAR), sendo ministrados por instrutores certificados e acompanhados de material didático e certificados de conclusão. O formato de três turmas permite distribuir o conteúdo por áreas e turnos distintos, garantindo formação prática e contextualizada de até 45 colaboradores, promovendo autonomia operacional, continuidade do conhecimento e maturidade institucional na gestão integrada da segurança cibernética,

				conforme este Termo de Referência.

8.19.11 A arquitetura de segurança definida neste Termo de Referência consolida a evolução do atual modelo de monitoramento e resposta do Banco da Amazônia para um ecossistema integrado, inteligente e colaborativo de defesa cibernética.

8.19.12 O SOC, no modelo de Cyber Fusion Center proposto, integra, sob uma governança unificada e responsabilidade única da CONTRATADA, as funções de detecção (XDR baseado em SIEM), prevenção e mitigação (Gestão de Vulnerabilidades – GVUL) e resposta a incidentes (SRIS), promovendo visão única, correlacionada e contextualizada do risco cibernético institucional.

8.19.13 Esse modelo rompe o paradigma reativo do SOC tradicional, adotando uma postura preditiva, orientada por dados, automação (SOAR), aprendizado de máquina e análise comportamental (UEBA), em alinhamento direto com as Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, a Lei nº 13.709/2018 (LGPD) e as melhores práticas internacionais de segurança e resiliência digital (ISO/IEC 27001, NIST CSF).

8.19.14 O presente Termo de Referência consolida a evolução da segurança cibernética do Banco da Amazônia para um modelo integrado, inteligente e colaborativo de defesa digital, baseado em um SOC no modelo de Cyber Fusion Center, estruturado de forma unificada e com execução end-to-end sob responsabilidade da CONTRATADA.

8.19.15 A adoção dessa arquitetura representa não apenas uma atualização tecnológica, mas uma transformação estrutural na forma como o Banco gerencia seus riscos, protege seus ativos críticos e conduz sua estratégia de resiliência cibernética.

8.19.16 Com a convergência operacional entre monitoramento, gestão de vulnerabilidades e resposta a incidentes, em uma única estrutura integrada, o Banco fortalece sua postura de resiliência operacional, conformidade regulatória e soberania informacional, em consonância com as diretrizes do Banco Central do Brasil, da LGPD e das normas internacionais de segurança.

8.19.17 A execução dos serviços deverá ocorrer de forma integrada, contínua, automatizada e interoperável, sendo obrigatória a atuação coordenada da CONTRATADA em todo o ciclo de detecção, análise e resposta, mediante:

a) Compartilhamento estruturado e contínuo de eventos, alertas, vulnerabilidades e indicadores de risco;

b) Utilização de playbooks integrados e automatizados de resposta a incidentes (SOAR);

c) Acionamento automático e coordenado entre as camadas de detecção, análise e resposta;

d) Garantia de responsabilidade integral pela execução dos serviços, vedada qualquer fragmentação operacional, transferência indevida de responsabilidade ou lacunas de atuação.

8.19.18 Todo o tratamento de dados institucionais do Banco da Amazônia deverá observar rigorosamente a Lei nº 13.709/2018 (LGPD), a Resolução CD/ANPD nº 15/2024, relativa à comunicação de incidentes de segurança e, quando caracterizada transferência internacional de dados pessoais, bem como a Resolução CD/ANPD nº 19/2024, a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e demais normativos aplicáveis, assegurando a proteção jurídica, a integridade, a confidencialidade e a rastreabilidade das informações.

8.19.19 Dessa forma, o Banco da Amazônia consolida sua maturidade cibernética e sua capacidade de gestão integrada de ameaças, garantindo a continuidade segura de seus serviços financeiros e a proteção do patrimônio tecnológico e informacional da instituição.

8.19.20 Ao integrar inteligência, tecnologia e governança sob uma arquitetura única e unificada, o Banco da Amazônia estabelece uma postura de segurança baseada em risco e resiliência, assegurando continuidade operacional, soberania dos dados e maturidade cibernética compatível com os desafios do Sistema Financeiro Nacional.

8.19.21 O Banco disponibilizará, durante a fase de planejamento e implantação, a documentação técnica consolidada dos casos de uso legados, bem como dicionários de dados, formatos de logs e demais artefatos necessários, a fim de garantir o adequado dimensionamento, integração e efetividade da solução contratada

9 REQUISITOS DA CONTRATAÇÃO

9.1 Da Implantação do Serviço

9.1.1 A implantação dos serviços está condicionada à prévia aprovação da solução na Prova de Conceito (POC), conforme estabelecido no item 8.2 e detalhado no Anexo I-C – Prova de Conceito (POC).

9.1.2 A implantação dos serviços ocorrerá em até 5 (cinco) dias úteis após a assinatura do contrato, deverá ocorrer a reunião de início (kick-off), com a participação do preposto designado, do gerente de projeto e da equipe técnica da CONTRATADA, ocasião em que serão alinhadas as etapas de implantação, cronograma, papéis e responsabilidades. Não há impedimento para a acumulação de papéis entre preposto e gerente de projeto.

9.1.3 A CONTRATADA deverá manter profissional com papel de gerente de projeto, responsável pelas atividades de planejamento, interlocução técnica, elaboração de cronograma e entrega da documentação associada à fase de implantação. O profissional deverá possuir certificação e experiência em gestão de projetos, conforme disposto no item 5.2 deste Termo de Referência.

9.1.4 Na reunião de kick-off, a CONTRATADA deverá apresentar:

a) a indicação nominal dos técnicos responsáveis pela implantação dos serviços de SOC, GVUL e XDR baseado em SIEM;

b) documentação comprobatória de certificação e experiência dos profissionais, conforme item 5.2;

c) comprovação de vínculo jurídico dos profissionais com a CONTRATADA;

d) os Termos de Confidencialidade e Sigilo, assinados por todos os profissionais envolvidos, conforme Anexo -Termo de Confidencialidade e Sigilo do Profissional;

e) os documentos do Projeto Executivo, contendo a proposta de cronograma detalhado e metodologia de execução da implantação;

f) Relatório de Aderência Arquitetural, demonstrando a compatibilidade da solução com a arquitetura tecnológica do Banco da Amazônia, abrangendo, pelo menos, integração com OpenShift, Oracle RAC e Data Lake corporativo.

9.1.5 O cronograma detalhado das atividades deverá ser apresentado em até 2 (dois) dias úteis após a reunião de kick-off, devendo conter as etapas, prazos, responsáveis e dependências técnicas.

9.1.6 O escopo da implantação deverá contemplar:

a) ativação e configuração inicial da solução de Monitoramento e Resposta a Incidentes (SOC), no modelo de Cyber Fusion Center, Gestão de Vulnerabilidades (GVUL) e Detecção e Resposta Estendidas (XDR baseado em SIEM), em ambiente seguro e segregado, em nome do Banco da Amazônia, no prazo máximo de 5 (cinco) dias corridos após a assinatura do contrato;

b) implantação e configuração do concentrador de logs no ambiente virtualizado do Banco;

c) integração dos componentes tecnológicos necessários ao funcionamento unificado das soluções SOC, GVUL e XDR baseado em SIEM;

d) migração, homologação e ativação das regras de detecção (casos de uso) a serem definidas pelo Banco, com base em planilha fornecida contendo lista, descrição e sintaxe das regras no padrão do SIEM utilizado;

e) homologação, pela CONTRATANTE, de cada regra migrada, mediante apresentação de evidência técnica de efetividade, utilizando eventos reais sempre que viável;

f) integração da solução de SIEM ao ServiceNow do Banco da Amazônia, para correlação e gerenciamento de incidentes.

9.1.7 O período de implantação e migração da solução atual para a nova arquitetura de segurança deverá ocorrer em até 90 (noventa) dias corridos, contados da assinatura do contrato – este prazo é baseado em requisitos internos de transição e continuidade, de modo que o cronograma dependerá da validação contínua das equipes do Banco.

9.1.8 Durante a fase de implantação, a CONTRATADA poderá alocar, a seu critério, profissionais especializados adicionais, distintos da equipe de operação continuada, desde que possuam qualificação técnica conforme o item 6.18, e sem custos adicionais ao Banco.

9.1.9 A CONTRATADA deverá, às suas expensas, alocar toda a equipe necessária para instalação, configuração, integração e execução dos serviços de implantação descritos neste Termo de Referência e em seus Anexos;

9.1.10 Ao final da implantação, deverá ser entregue ao Banco da Amazônia a documentação de as-built completa de cada serviço implantado, contendo, no mínimo:

a) descrição detalhada dos serviços implantados;

b) topologia lógica e física dos componentes e integrações;

c) versões, parâmetros e configurações dos softwares;

d) rotinas de operação, manutenção, atualização e verificação de funcionamento;

e) definição de responsabilidades operacionais e de suporte;

f) procedimentos para abertura e atendimento de chamados;

g) rotinas periódicas configuradas;

h) documentação dos processos de trabalho, fluxos de resposta a incidentes, prazos e responsáveis;

i) documentação dos casos de uso (regras de detecção) configurados nas ferramentas de monitoramento e detecção;

j) definição dos padrões de nomenclatura, configuração e versionamento aplicáveis.

9.1.11 A CONTRATADA deverá manter documentação atualizada de todas as atividades realizadas, incluindo planos de trabalho, atas de reunião, registros de teste, homologação, entregas e conferências, compondo um dossiê técnico completo a ser entregue ao Banco ao término da implantação.

9.1.12 A CONTRATADA será responsável por executar os procedimentos de diagnóstico e correção de falhas eventualmente identificadas durante a implantação. Caso o diagnóstico aponte causas alheias à implantação, o Banco poderá assumir o tratamento, desde que comprovado tecnicamente pela CONTRATADA e mediante aprovação da CONTRATANTE.

9.1.13 O Serviço Gerenciado de Monitoramento e Resposta a Incidentes (SOC), no modelo de Cyber Fusion Center, deverá ser iniciado no dia útil seguinte à homologação da primeira regra de monitoramento, mesmo que a integração completa com o ServiceNow ainda esteja em andamento. Nesse caso, os alertas deverão ser escalados manualmente, assegurando continuidade operacional.

9.1.14 Os serviços implantados poderão ser rejeitados total ou parcialmente caso não atendam às especificações deste Termo de Referência e seus anexos, devendo ser corrigidos, refeitos ou substituídos pela CONTRATADA no prazo determinado pelo Fiscal do Contrato, sem ônus ao Banco e sem prejuízo das penalidades aplicáveis.

9.1.15 Em caso de início parcial dos serviços previstos neste Termo, o Banco da Amazônia efetuará o pagamento proporcional aos serviços efetivamente iniciados e autorizados.

9.1.16 Os Termos de Aceite serão emitidos após a verificação da conformidade técnica, homologação das entregas e comprovação do atendimento integral dos requisitos estabelecidos neste Termo de Referência.

9.2 **Da Qualificação Técnica dos Profissionais da Contratada**

9.2.1 Os serviços contratados deverão ser executados por profissionais devidamente qualificados, com experiência e certificações compatíveis com as características e a complexidade técnica das atividades, observadas as seguintes exigências mínimas:

a) O Preposto do Contrato: profissional responsável pelo gerenciamento do contrato e pela interlocução entre a equipe da CONTRATADA e o Banco da Amazônia, deverá possuir formação superior completa, experiência profissional mínima de 72 (setenta e dois) meses em gestão de contratos de serviços técnicos e participação comprovada em pelo menos 2 (dois) contratos de porte e complexidade equivalentes ao objeto desta contratação, preferencialmente em instituições financeiras ou órgãos públicos.

b) Equipe de Implantação Técnica (Projeto Executivo, Instalação, Configuração, Testes, Ativação e Documentação): os profissionais responsáveis por essas atividades deverão possuir certificação oficial na solução de SIEM ofertada, bem como experiência comprovada em implantação de plataformas corporativas de monitoramento, correlação de eventos e integração de serviços gerenciados de segurança.

c) Equipe de Monitoramento e Resposta a Incidentes (SOC), no modelo de Cyber Fusion Center: os profissionais responsáveis pela operação do serviço deverão possuir experiência comprovada mínima de 2 (dois) anos em ambientes de Monitoramento de Segurança (SOC), no modelo de Cyber Fusion Center, e operação de soluções integradas de SIEM, XDR baseado em SIEM ou equivalentes, além de certificação técnica válida em pelo menos uma das seguintes credenciais:

   i) Profissionais de primeiro e segundo nível com certificações CompTIA Security+, CompTIA CySA+, CEH ou equivalentes;

   ii) Profissionais de terceiro nível com certificações GCIH, GCFA, CHFI, OSCP ou equivalentes, com experiência comprovada em resposta a incidentes e forense digital.

d) Gerente de Projeto: profissional responsável pelo planejamento, acompanhamento e controle das atividades de implantação e operação, devendo possuir certificação PMP (Project Management Professional) ou CompTIA Project+, emitida por instituição reconhecida internacionalmente. Esse profissional deverá atuar durante toda a execução contratual, garantindo o cumprimento de cronogramas, entregas e níveis de serviço.

e) Profissional Responsável pelos Relatórios Gerenciais e de Segurança (RMS e RSS): os relatórios técnico-operacionais mensais e semestrais deverão ser elaborados e apresentados por profissional com conhecimento comprovado do serviço e que possua ao menos uma das seguintes certificações de segurança da informação:

   CISSP (Certified Information Systems Security Professional);

   CISM (Certified Information Security Manager);

   GCIA (GIAC Certified Intrusion Analyst);

   GSEC (GIAC Security Essentials);

   GCIH (GIAC Incident Handler);

   GMON (GIAC Continuous Monitoring);

   CompTIA Security+.

9.2.2 Para comprovação das certificações e qualificações técnicas exigidas, a CONTRATADA deverá apresentar, para cada profissional envolvido:

a) cópia do certificado oficial emitido ou reconhecido pela instituição certificadora correspondente, ou comprovação eletrônica de validade da certificação;

b) documento comprobatório do vínculo jurídico com a CONTRATADA (carteira de trabalho, contrato de prestação de serviços ou declaração formal do empregador).

9.2.3 A CONTRATADA deverá demonstrar maturidade em gestão de segurança da informação, por meio da apresentação de certificações vigentes, ou comprovação documental equivalente, que evidenciem a adoção de um Sistema de Gestão de Segurança da Informação (SGSI) auditável e alinhado às melhores práticas internacionais.

9.2.4 A comprovação poderá ocorrer por:

a) Certificações de mercado, válidas de Segurança da Informação;

b) Certificação corporativa de grupo econômico;

c) Evidências formais de processos, auditorias independentes e controles equivalentes, a critério do Banco da Amazônia.

9.2.5 Todos os profissionais deverão estar formalmente designados e identificados na documentação de kick-off e poderão ser substituídos apenas mediante anuência prévia e por escrito do Banco da Amazônia, desde que o substituto atenda integralmente aos requisitos técnicos e certificações previstos neste item.

9.3 **Dos Requisitos de Segurança da Informação**

9.3.1 Todos os empregados, terceirizados e parceiros que venham a executar serviços, direta ou indiretamente, no âmbito deste contrato, deverão assinar o Termo de Confidencialidade e Sigilo, conforme Anexo – Termo de Confidencialidade e Sigilo do Profissional, que deverá ser apresentado antes do início das atividades de cada profissional, como condição para acesso a qualquer informação, sistema ou infraestrutura do Banco da Amazônia.

9.3.2 No encerramento das atividades de qualquer profissional vinculado à CONTRATADA, esta deverá proceder, imediatamente, à revogação de todas as credenciais, acessos e autorizações associadas às soluções sob sua responsabilidade, bem como solicitar ao Banco da Amazônia a revogação das credenciais eventualmente concedidas às soluções sob responsabilidade do Banco da Amazônia.

9.3.3 Essas exigências têm por finalidade assegurar a proteção do Banco da Amazônia contra o uso indevido, vazamento ou manipulação indevida de informações sob sua guarda, em conformidade com as Políticas e Normativos de Segurança da Informação e Cibernética do Banco, com a Resolução CMN nº 4.893/2021 do Banco Central do Brasil, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e com as boas práticas de governança e gestão de segurança da informação preconizadas pelas normas ABNT NBR ISO/IEC 27001, 27002 e 27035.

9.3.4 O Centro de Operações de Segurança (SOC), no modelo de Cyber Fusion Center, da CONTRATADA, bem como as infraestruturas correlatas utilizadas para a execução dos serviços gerenciados de segurança (SOC, GVUL e XDR baseado em SIEM), deverão observar os seguintes requisitos mínimos de segurança física, lógica e operacional:

a) dispor de sistema de CFTV com capacidade de rastreamento e registro contínuo de movimentações internas, cujas imagens sejam armazenadas por, no mínimo, 90 (noventa) dias e recuperáveis mediante solicitação formal do Banco da Amazônia;

b) possuir perímetro físico protegido com sensores de intrusão e alarmes contra acesso não autorizado;

c) implementar controle de acesso físico com, no mínimo, dois fatores de autenticação (ex.: cartão magnético, biometria digital, reconhecimento facial ou análise de retina);

d) operar em regime ininterrupto (24x7x365), garantindo alta disponibilidade e contingência contínua;

e) manter registro de entrada e saída de pessoas, atualizado e acessível por no mínimo 90 (noventa) dias;

f) dispor de links dedicados redundantes, com dupla abordagem (provedores distintos), assegurando continuidade das comunicações;

g) manter ambiente dedicado de laboratório isolado do SOC de produção, destinado à simulação, investigação e reprodução de incidentes, sem impacto nas operações;

h) possuir processos formalizados para as funções essenciais de segurança:

i) monitoramento e detecção de ameaças;

ii) gestão de dispositivos e ativos;

iii) gestão de vulnerabilidades;

iv) resposta e tratamento de incidentes;

v) inteligência de ameaças;

vi) investigação e forense digital;

vii) gestão de conformidade e auditoria.

i) manter console central de gerenciamento de eventos e incidentes (SIEM) instalado e operacional em seu SOC, com capacidade de integração e correlação de dados com os sistemas do Banco da Amazônia;

j) possuir plataforma de sandbox para análise de ameaças avançadas, com suporte a detecção comportamental e execução controlada de amostras;

k) dispor de infraestrutura de continuidade e contingência, incluindo mecanismos de proteção contra incêndio, redundância de energia, backup físico e plano de recuperação de desastres (DRP) documentado e testado;

l) permitir que o Banco da Amazônia realize diligências ou auditorias técnicas a qualquer tempo, para verificação das condições de segurança e conformidade das instalações e serviços, inclusive mediante visita técnica pré-agendada.

9.3.5 A CONTRATADA deverá documentar integralmente os controles e procedimentos relacionados à execução dos serviços, observando os seguintes requisitos:

a) elaborar, apresentar e manter atualizadas todas as definições, processos e procedimentos implementados durante a vigência do contrato;

b) manter a documentação técnica e operacional continuamente revisada e disponível para auditorias internas ou externas do Banco da Amazônia;

c) realizar, sempre que necessário, atualizações e manutenções dos entregáveis já executados, de forma a garantir a aderência às melhores práticas e às normas vigentes;

d) apresentar, no momento da designação da equipe, o portfólio de formação, certificações e qualificações de todos os profissionais indicados para a execução dos serviços.

9.4 **Dos Requisitos para Serviços Executados em Nuvem**

9.4.1 A CONTRATADA deverá assegurar que a legislação brasileira prevaleça integralmente sobre quaisquer disposições estrangeiras aplicáveis aos serviços prestados em nuvem, garantindo que o Banco da Amazônia mantenha plena titularidade, posse e soberania sobre seus dados, metadados e informações, sejam eles processados, armazenados ou transmitidos na infraestrutura da CONTRATADA ou de seus provedores de nuvem.

9.4.2 Todo o tratamento de dados institucionais do Banco da Amazônia deve ser com foco na aderência à LGPD, no cumprimento da Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, e na garantia de que não haja qualquer comprometimento da segurança jurídica do Banco.

9.4.3 Os serviços executados em nuvem, quando utilizados na prestação dos serviços gerenciados de segurança (SOC, GVUL e XDR baseado em SIEM), deverão atender às seguintes condições mínimas:

a) Cumprir integralmente as diretrizes da Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025, da Lei nº 13.709/2018 (LGPD), a Resolução CD/ANPD nº 15/2024, relativa à comunicação de incidentes de segurança e, quando caracterizada transferência internacional de dados pessoais, a Resolução CD/ANPD nº 19/2024, bem como as demais normas correlatas de segurança cibernética e proteção de dados;

b) Assegurar ao Banco da Amazônia acesso total, direto e seguro aos dados e informações processados ou armazenados pela CONTRATADA ou por eventuais subcontratadas;

c) Garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade de todos os dados e informações do Banco, inclusive durante transmissão, processamento, armazenamento e descarte;

d) Manter conformidade com as normas ABNT NBR ISO/IEC 27001:2022, ISO/IEC 27017:2026 e ISO/IEC 27018:2025, demonstrando, mediante evidências documentais, o atendimento aos controles e objetivos relativos à segurança e proteção de dados pessoais;

e) Permitir ao Banco da Amazônia acesso a relatórios de auditoria independentes (tais como SOC 2, ISO, ISAE 3402, entre outros), relativos aos controles de segurança, disponibilidade e confidencialidade da infraestrutura de nuvem utilizada;

f) Disponibilizar recursos de monitoramento e gestão que possibilitem o acompanhamento em tempo real da disponibilidade, desempenho e conformidade dos serviços de nuvem;

g) Assegurar segregação lógica e/ou física dos dados do Banco da Amazônia, com relatórios técnicos que comprovem os controles aplicados;

h) Implementar controles de acesso baseados em identidade federada (SSO) e autenticação multifator (MFA), utilizando preferencialmente o mecanismo corporativo do Banco da Amazônia;

i) Manter registros de logs, eventos, acessos e incidentes cibernéticos pelo período mínimo de 12 (doze) meses em camada de armazenamento de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, assegurando a integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória, disponibilizando-os ao Banco sempre que solicitado;

j) A retenção de 48 (quarenta e oito) meses tem finalidades regulatória, forense e de auditoria. Os dados além dos 12 meses "quentes" não precisam permanecer pesquisáveis em camada normalizada pelo SIEM. Portanto, consultas poderão ser realizadas a partir de dados brutos indexados ou em outros formatos definidos na fase de implantação.

k) A retenção dos 48 (quarenta e oito) meses poderá ser atendida mediante exportação automática, segura e íntegra dos logs para ambiente de armazenamento sob custódia direta do Banco da Amazônia, devendo a CONTRATADA ser responsável pela entrega, integridade, periodicidade e segurança dessa exportação;

l) Apoiar o Banco da Amazônia em atividades de investigação de incidentes de segurança, fornecendo prontamente logs, registros e demais evidências solicitadas;

m) Adotar controles de segurança aplicáveis ao ciclo de vida de sistemas e aplicações hospedados em nuvem, incluindo revisão de vulnerabilidades, homologação de versões e gestão formal de mudanças;

n) Garantir isolamento dos ambientes e proteção contra usuários não autorizados, utilizando mecanismos de criptografia de ponta a ponta, com chaves sob controle exclusivo do Banco da Amazônia, sempre que tecnicamente viável;

o) Assegurar que todas as alterações de sistema sejam homologadas e documentadas conforme processo formal de gestão de mudanças;

p) Dispor de plano de comunicação e resposta a incidentes, com dashboards atualizados e notificações imediatas ao Banco da Amazônia em casos que impactem a confidencialidade, integridade, disponibilidade ou autenticidade das informações;

q) Realizar gestão mensal de riscos de segurança da informação, incluindo mapeamento de ativos, identificação, tratamento e monitoramento de riscos, com apresentação de plano atualizado;

r) Possuir plano de continuidade e recuperação de desastres (DRP/BCP), testado regularmente, assegurando a disponibilidade e a recuperação dos serviços críticos;

s) Realizar, trimestralmente, testes de segurança da informação (análise de riscos, vulnerabilidades, testes de penetração e auditorias independentes), apresentando relatórios comprobatórios ao Banco da Amazônia;

t) Dispor de soluções técnicas de proteção, incluindo firewall de próxima geração, IDS/IPS, antivírus, antimalware, anti-DDoS, gestão de patches, gestão de logs e correlação de eventos (SIEM);

u) Assegurar a transmissão de dados por canais criptografados e garantir acesso apenas a usuários e aplicações autorizadas;

v) Realizar backups e salvaguardas das comunicações e permitir a consulta a esses dados;

w) Manter todas as cópias e backups de dados corporativos hospedados em território brasileiro, salvo exceções autorizadas pelo Banco e em conformidade com a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025;

x) Garantir a exclusividade de direitos do Banco da Amazônia sobre todas as informações tratadas durante a vigência contratual, inclusive cópias e backups;

y) Proibir expressamente o uso de informações do Banco da Amazônia para fins de propaganda, treinamento ou aprendizado de modelos de inteligência artificial, inclusive de terceiros, enriquecimento de dados ou qualquer outro uso secundário não autorizado;

z) Preservar os dados do Banco contra acessos indevidos e impedir a replicação ou o armazenamento fora do território nacional, comunicando imediatamente qualquer tentativa de acesso externo, inclusive judicial;

aa) Conceder ao Banco Central do Brasil e ao Banco da Amazônia acesso a contratos, acordos, dados, cópias de segurança e informações referentes à execução dos serviços;

bb) Manter o Banco da Amazônia permanentemente informado sobre limitações técnicas, contratuais ou regulatórias que possam comprometer a execução, segurança ou conformidade dos serviços;

cc) Fornecer informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados, sempre que solicitado;

dd) Operar o serviço dentro do uso proposto, com desempenho adequado e mínima dependência de permissões adicionais em outros sistemas do Banco;

ee) Demonstrar conformidade com a LGPD, mantendo evidências documentais sobre:

i) diretrizes e políticas de tratamento de dados;

ii) atendimento a solicitações de titulares;

iii) medidas de confidencialidade e segurança;

iv) registros de atividades de tratamento;

v) autorizações de subcontratação;

vi) devolução e descarte de dados após o término contratual.

9.4.4 Os dados, metadados e informações produzidos ou custodiados pelo Banco da Amazônia devem estar hospedados em território brasileiro, mantendo-se pelo menos uma cópia atualizada de segurança local. Informações sem restrição de acesso poderão possuir cópias fora do país, desde que em conformidade com a Resolução CMN nº 4.893/2021, e alterações posteriores, principalmente as promovidas pela Resolução CMN nº 5.274/2025.

9.4.5 O provedor de nuvem e a CONTRATADA deverão garantir que quaisquer transferências internacionais de dados ocorram somente mediante autorização formal e expressa do Banco da Amazônia, observando as exigências da LGPD e as diretrizes do Banco Central do Brasil.

9.4.6 O descumprimento de quaisquer dos requisitos deste item será considerado falha grave de execução contratual, sujeitando a CONTRATADA às penalidades previstas neste Termo de Referência e no contrato, sem prejuízo das responsabilidades civis, administrativas e regulatórias.

9.4.7 Em caso de término contratual, a CONTRATADA deverá transferir integralmente todos os dados, registros e backups ao Banco da Amazônia ou a novo prestador, garantindo a integridade e a completude das informações, e proceder à eliminação segura de quaisquer cópias remanescentes, com emissão de declaração formal de destruição.

10 PLANO DE SUSTENTAÇÃO

10.1 Da Transição Contratual

10.1.1 O período de transição contratual corresponderá aos últimos 2 (dois) meses de vigência do contrato, devendo ser conduzido de forma planejada e supervisionada, a fim de assegurar a continuidade operacional dos serviços gerenciados de segurança (SOC, GVUL e XDR baseado em SIEM) e a preservação integral das informações, dados e configurações. Sendo que todas as informações, acessos e insumos necessários serão fornecidos durante o período de transição.

10.1.2 Durante esse período, a CONTRATADA deverá elaborar e entregar a documentação técnica completa de transição contratual, destinada a subsidiar futuras contratações e assegurar a transferência ordenada do conhecimento técnico e operacional. Essa documentação deverá garantir a confidencialidade, integridade e disponibilidade dos serviços e das informações, contemplando, no mínimo:

a) documentação técnica atualizada de as-built da solução, contendo topologia, integrações, fluxos de dados, configurações e parâmetros operacionais;

b) demonstrativo histórico de crescimento e consumo de recursos durante toda a vigência contratual, incluindo métricas de alertas gerados, volume de logs ingeridos e tendências de capacidade;

c) baseline de desempenho e dados consolidados que subsidiem o planejamento de capacidade e dimensionamento de serviços futuros;

d) relatórios de efetividade dos controles e registros de incidentes tratados;

e) esclarecimento de dúvidas e suporte técnico às equipes designadas pelo Banco da Amazônia ou pela nova contratada, abrangendo aspectos de configuração, dimensionamento e operação.

10.1.3 A CONTRATADA deverá disponibilizar ao Banco da Amazônia todas as informações, relatórios e evidências técnicas relevantes relacionadas aos serviços prestados, bem como prestar apoio técnico durante o processo de transição, mediante solicitação formal.

10.1.4 A CONTRATADA deverá ainda assegurar a continuidade dos serviços, o acesso às informações necessárias e a transferência de conhecimento técnico, de forma estruturada, segura e documentada, sem ônus adicional ao Banco da Amazônia.

10.2 **Do Plano de Continuidade de Negócios**

10.2.1 A CONTRATADA deverá elaborar, manter e disponibilizar ao Banco da Amazônia um Plano de Continuidade de Negócios (PCN) aplicável à execução dos serviços gerenciados de segurança (SOC, GVUL e XDR baseado em SIEM), fundamentado em normas reconhecidas de gestão de continuidade, em especial a ABNT NBR ISO 22301:2020 – Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Requisitos, o ITIL v4, o COBIT 2019, o Good Practice Guidelines (Business Continuity Institute) e o Professional Practices (Disaster Recovery International Institute), ou equivalentes.

10.2.2 O PCN deverá contemplar políticas, procedimentos e planos de ação destinados a mitigar impactos decorrentes de riscos operacionais, falhas sistêmicas, indisponibilidades, desastres naturais ou cibernéticos que possam comprometer os Níveis Mínimos de Serviço (NMS) definidos neste Termo de Referência e no contrato.

10.2.3 O PCN e as evidências dos testes realizados deverão ser apresentados pela CONTRATADA ao Banco da Amazônia:

a) término da fase de implantação e emissão do Termo de Aceitação Definitiva;

b) anualmente, com atualização e comprovação dos testes de contingência;

c) sempre que solicitado formalmente pelo Banco da Amazônia.

10.2.4 O PCN submetido será analisado pelo Banco da Amazônia, que poderá aprová-lo, rejeitá-lo ou solicitar ajustes, de forma motivada, para garantir o atendimento aos requisitos técnicos e aos Níveis Mínimos de Serviço contratualmente estabelecidos.

10.2.5 Em caso de rejeição ou necessidade de ajustes, a CONTRATADA disporá do prazo máximo de 30 (trinta) dias corridos, contados da comunicação formal do Banco da Amazônia, para reapresentar o plano revisado e devidamente adequado às exigências técnicas.

10.2.6 O descumprimento dos prazos ou a ausência de conformidade do PCN com as normas e práticas exigidas caracterizará falha contratual grave, sujeitando a CONTRATADA às penalidades previstas no contrato e na legislação aplicável.

11 INDICAÇÃO SE O CONTRATO É COM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

Esta contratação não possui dedicação exclusiva de mão de Obra.

12 MODELO DE GESTÃO DO CONTRATO

12.1 Da Execução Contratual

12.1.1 O contrato deverá ser executado fielmente pelas partes, em conformidade com as cláusulas avençadas e com as normas da Lei nº 13.303/2016, respondendo cada uma pelas consequências de sua inexecução total ou parcial.

12.1.2 Em caso de impedimento, ordem de paralisação ou suspensão da execução, o cronograma contratual será automaticamente prorrogado pelo período correspondente, devendo tais circunstâncias ser registradas mediante apostila formal.

12.2 Das Comunicações e Reuniões

12.2.1 Todas as comunicações entre o Banco da Amazônia e a CONTRATADA deverão ser realizadas por escrito, preferencialmente por meio eletrônico institucional, sempre que o ato exigir formalidade.

12.2.2 O Banco da Amazônia poderá, a qualquer momento, convocar representantes da CONTRATADA para adoção imediata de providências relativas à execução contratual.

12.2.3 Após a assinatura do contrato, o Banco da Amazônia promoverá reunião inicial de alinhamento para apresentação do Plano de Fiscalização, contendo as obrigações contratuais, mecanismos de controle, estratégias de execução, critérios de aferição de resultados e penalidades aplicáveis.

12.3 Da Fiscalização Contratual

12.3.1 A execução do contrato será acompanhada e fiscalizada por fiscais designados formalmente pelo Banco da Amazônia, que atuarão conforme suas respectivas competências técnicas e administrativas.

12.3.2 A ausência, omissão ou tolerância da fiscalização não eximirá a CONTRATADA de suas responsabilidades contratuais, legais e regulatórias.

12.4 Da Fiscalização Técnica

a) O Fiscal Técnico acompanhará permanentemente a execução do objeto, assegurando que os serviços sejam prestados conforme as especificações técnicas e os níveis mínimos de serviço contratados;

b) Todas as ocorrências deverão ser registradas no Histórico de Gerenciamento do Contrato, inclusive recomendações, falhas e medidas corretivas;

c) Verificada qualquer irregularidade ou descumprimento, o fiscal técnico emitirá notificação formal com prazo para correção;

d) Situações que extrapolem a competência técnica do fiscal deverão ser imediatamente comunicadas ao Gestor do Serviço, para adoção das providências cabíveis;

e) Em caso de risco à continuidade contratual, o fiscal técnico deverá notificar o gestor e a autoridade superior, indicando a gravidade e as ações mitigatórias;

f) O fiscal técnico comunicará ao gestor o término do contrato com antecedência mínima necessária à renovação ou prorrogação, quando aplicável.

12.5 **Da Fiscalização Administrativa**

a) O Fiscal Administrativo verificará a manutenção das condições de habilitação e qualificação da CONTRATADA durante toda a execução contratual;

b) Identificado descumprimento de obrigações administrativas, o fiscal atuará tempestivamente na correção ou reporte ao Gestor do Serviço, conforme o nível de competência;

c) Caberá ao fiscal administrativo manter atualizados os registros sobre documentação fiscal, trabalhista e previdenciária da CONTRATADA.

12.6 **Da Gestão do Contrato**

a) O Gestor do Serviço coordenará o processo de acompanhamento e fiscalização, assegurando a integração entre os fiscais técnico e administrativo e a manutenção do histórico contratual completo;

b) Caberá ao gestor consolidar as informações sobre ordens de serviço, prorrogações, alterações contratuais e relatórios de desempenho;

c) O gestor emitirá relatórios periódicos de conformidade e desempenho, baseados em indicadores mensuráveis e nas avaliações realizadas pelos fiscais;

d) O gestor será responsável por instaurar processos de responsabilização e propor sanções administrativas;

e) Ao final da vigência contratual, o gestor elaborará relatório conclusivo contendo a análise da execução, o cumprimento dos objetivos e as recomendações de aprimoramento;

f) Caberá ao gestor encaminhar à área de contratos toda a documentação comprobatória necessária à liquidação e pagamento, com base nas medições e atestos emitidos pelos fiscais.

12.7 **Da Designação da Unidade Responsável**

12.7.1 A Gerência Executiva de Segurança Corporativa (GESEC) será responsável pela fiscalização da entrega e desempenho dos serviços contratados, designando formalmente representante para o gerenciamento das obrigações técnicas e administrativas.

12.8 **Dos Critérios de Avaliação**

12.8.1 A verificação da conformidade e adequação dos serviços será realizada com base nos critérios, indicadores e métricas definidos neste Termo de Referência, nos anexos contratuais e na proposta técnica da CONTRATADA.

13 ESTIMATIVAS DOS PREÇOS E ORÇAMENTO DETALHADO DO VALOR

13.1. Esta Licitação será mantida sobre sigilo até a fase final dos lances.

14 RUBRICA ORÇAMENTÁRIA

14.1 Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto desta contratação estão previstos no orçamento do Banco da Amazônia, nas rubricas:

ITEM	DESCRIÇÃO	RUBRICA
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	82.559-0
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	82.543-3
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	82.559-0
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	82.548-4
Obs.:	** Regime contínuo de 24x7x365.*	
	*** Sob demanda, a critério do Banco, mediante Ordem de Serviço.*	

15 PRAZO DE VIGÊNCIA

15.1 Do Prazo de Vigência Contratual

15.1.1 O contrato decorrente deste Termo de Referência terá vigência de 60 (sessenta) meses, contados a partir da data de sua assinatura, incluindo todas as fases de implantação, operação, suporte e manutenção, conforme o cronograma físico-financeiro aprovado, nos termos do Art. 71 da Lei 13.303/2016 c/c Art. 92 do Regulamento Interno de Licitações e Contratos.

15.2 Do Encerramento e Transição

15.2.1 Encerrado o prazo contratual, a CONTRATADA deverá assegurar a transição ordenada e sem descontinuidade dos serviços, conforme previsto no Plano de Sustentação e Transição Contratual, garantindo:

a) a transferência integral de conhecimento técnico e documentação atualizada;

b) o apoio à transição para eventual nova contratada; e

c) a preservação da integridade, confidencialidade e disponibilidade das informações e dados do Banco da Amazônia.

16 CONDIÇÕES DE REAJUSTE DE PREÇOS

16.1 Os preços serão reajustados com o intervalo mínimo de um ano, a contar da data limite para a apresentação da proposta ou da data do orçamento a que a proposta se referir, pelo ICTI/IPEA apurado no período.

16.2 Os reajustes subsequentes observarão o interregno mínimo de um ano a contar da data base de reajuste do ano anterior.

16.3 O reajuste incidirá sobre os preços unitários vigentes dos itens que compõem a contratação, inclusive:

a) serviços continuados de XDR baseado em SIEM;
b) Gestão de Vulnerabilidades – GVUL;
c) SRIS;
d) preço unitário da UST; e
e) preço unitário das turmas de capacitação.

16.4 Para os itens executados sob demanda, especialmente UST e capacitação técnica, o reajuste incidirá sobre o preço unitário contratual vigente, aplicando-se apenas às Ordens de Serviço emitidas após a data de início dos efeitos financeiros do reajuste.

16.5 O reajuste não implicará alteração dos quantitativos estimados ou dos limites máximos contratados, permanecendo inalterados, salvo modificação contratual regularmente autorizada:

a) o limite de 5.000 UST;
b) o quantitativo de 3 turmas de capacitação;
c) as capacidades mínimas contratadas de XDR baseado em SIEM, GVUL e demais serviços; e
d) os quantitativos e parâmetros técnicos estabelecidos no Termo de Referência.

16.6 Os custos relativos a licenças, subscrições, serviços de fabricantes, infraestrutura em nuvem, armazenamento, processamento, suporte, mão de obra e demais componentes necessários à execução do serviço deverão ser considerados pela CONTRATADA na formação dos preços ofertados, não sendo admitida sua transferência automática ao Banco em razão de variações ordinárias desses componentes.

16.7 Eventual variação cambial relacionada à aquisição, pela CONTRATADA, de licenças, subscrições, tecnologias ou serviços de fornecedores estrangeiros constitui, em regra, risco ordinário da atividade empresarial e não ensejará reajuste específico ou automático dos preços contratados.

16.8 Situações excepcionais e devidamente comprovadas que provoquem alteração extraordinária e imprevisível, ou de consequências incalculáveis, das condições econômicas originalmente pactuadas serão analisadas segundo as regras aplicáveis à recomposição do equilíbrio econômico-financeiro, não se confundindo com o reajuste anual previsto neste item.

16.9 O pedido de recomposição extraordinária deverá ser acompanhado de documentação suficiente para demonstrar o evento, sua excepcionalidade, o nexo causal com a execução contratual e o impacto econômico efetivamente suportado pela parte interessada.

16.10 Alterações de tributos, encargos ou obrigações legais serão tratadas conforme sua natureza e a legislação aplicável, não sendo automaticamente incorporadas aos preços sem demonstração de efetivo impacto sobre o equilíbrio econômico-financeiro do contrato.

16.11 Na hipótese de extinção, suspensão, alteração substancial ou impossibilidade de utilização do índice de reajuste adotado, será utilizado índice oficial substituto previsto na legislação ou definido pelo Banco de forma tecnicamente fundamentada, preservada a finalidade de recomposição da variação ordinária dos preços.

16.12 Caso o índice acumulado no período apresente variação negativa, deverá ser observada a disciplina estabelecida no Edital, no contrato e nos normativos internos do Banco quanto à aplicação da redução correspondente.

16.13 A concessão do reajuste deverá ser formalizada na forma prevista no Regulamento de Licitações e Contratos do Banco da Amazônia e no instrumento contratual, com atualização das respectivas planilhas e preços unitários aplicáveis.

16.14 O reajuste dos preços não modificará o escopo, os requisitos técnicos, os Níveis Mínimos de Serviço – NMS, os indicadores de desempenho, os prazos, os critérios de aceite ou quaisquer outras obrigações assumidas pela CONTRATADA.

16.15 Não será admitida a utilização do reajuste como fundamento para alteração da composição econômica relativa entre os itens, redistribuição de preços, compensação entre componentes contratados ou modificação da estrutura originalmente adjudicada.

17 ALTERAÇÃO DO CONTRATO

17.1 As alterações incidentes sobre o objeto do contrato deverão ser formalmente justificadas, aprovadas pelas instâncias competentes do Banco da Amazônia e consensuais entre as partes, observando-se o disposto no artigo 81 da Lei nº 13.303/2016 e as normas internas do Banco.

17.2 As alterações poderão ser:

a) Quantitativas, quando implicarem acréscimo ou diminuição do objeto contratado; ou

b) Qualitativas, quando disserem respeito à modificação das características técnicas ou especificações do objeto contratado.

17.3 **Das Alterações Quantitativas**

17.3.1 As alterações quantitativas sujeitam-se aos limites previstos nos §§ 1º e 2º do artigo 81 da Lei nº 13.303/2016, observando-se que:

a) os limites de acréscimo e supressão deverão ser aplicados de forma independente, não sendo admitida compensação entre eles;

b) deve ser preservada a proporção percentual entre o valor global do contrato e o valor originalmente orçado pelo Banco da Amazônia;

c) qualquer variação quantitativa deverá manter a coerência técnica e financeira com o escopo contratual e com o planejamento de segurança da informação do Banco.

17.4 **Das Alterações Qualitativas**

17.4.1 Excepcionalmente, a alteração qualitativa poderá ultrapassar os limites dos §§ 1º e 2º do artigo 81 da Lei nº 13.303/2016, desde que observados os seguintes pressupostos técnicos e jurídicos:

a) os encargos decorrentes da continuidade do contrato sejam inferiores aos de uma eventual rescisão e nova licitação;

b) a rescisão seguida de novo certame represente prejuízo relevante ao interesse institucional ou à continuidade dos serviços críticos de segurança cibernética;

c) a modificação seja necessária para o alcance dos objetivos originais da contratação, otimização de cronogramas ou adequação tecnológica de soluções SOC, GVUL e XDR baseado em SIEM;

d) a capacidade técnica e econômico-financeira da CONTRATADA seja compatível com a nova dimensão do objeto;

e) a motivação decorra de fatores supervenientes, devidamente documentados, que não caracterizem burla ao processo licitatório;

f) a alteração não resulte em mudança de natureza, finalidade ou escopo essencial do contrato.

17.5 **Dos Procedimentos e Instruções Processuais**

17.5.1 Toda alteração contratual deverá ser instruída com:

a) memória de cálculo, parecer técnico e justificativa fundamentada dos fiscais técnico e administrativo do Banco da Amazônia, contendo a avaliação dos pressupostos, impactos e limites aplicáveis;

b) ratificação pelo gestor do contrato;

c) manifestação jurídica e financeira do Banco, quando aplicável;

d) análise de conformidade pela unidade de governança ou controle interno, conforme normativos corporativos.

17.6 **Da Formalização**

17.6.1 As alterações contratuais incidentes sobre o objeto ou decorrentes de revisão de preços deverão ser formalizadas por termo aditivo, assinado pela mesma autoridade que firmou o contrato, devendo seu extrato ser publicado no sítio eletrônico do Banco da Amazônia.

17.7 **Dos Apostilamentos**

17.7.1 Não caracterizam alteração contratual e poderão ser formalizadas por termo de apostilamento, dispensando-se termo aditivo, as seguintes situações:

a) variação do valor contratual em razão de reajuste de preços previsto contratualmente;

b) atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento;

c) correção de erros materiais identificados no instrumento contratual;

d) alterações na razão social, CNPJ ou denominação da CONTRATADA, sem modificação da estrutura jurídica ou operacional da empresa.

17.8 **Da Fusão, Cisão ou Incorporação**

17.8.1 Será admissível a fusão, cisão ou incorporação da CONTRATADA com outra pessoa jurídica, desde que:

a) a nova pessoa jurídica comprove o atendimento a todos os requisitos de habilitação exigidos no Termo de Referência;

b) sejam mantidas integralmente as cláusulas, obrigações e garantias do contrato;

c) não haja interrupção ou prejuízo à execução dos serviços de segurança cibernética contratados; e

d) haja anuência expressa do Banco da Amazônia quanto à continuidade contratual.

18 PAGAMENTO AO FORNECEDOR

18.1 O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados a partir da validação do Relatório de Serviços Prestados (RSP) pela fiscalização do contrato, conforme modelo e parâmetros definidos no Anexo I-B – Níveis Mínimos de Serviço (NMS).

18.2 A CONTRATADA somente deverá emitir a Nota Fiscal após a aprovação formal do RSP pelos fiscais designados, sendo esta aprovação condição indispensável para a liquidação e o pagamento do valor correspondente.

18.3 As Notas Fiscais emitidas após o 25º (vigésimo quinto) dia do mês subsequente à prestação dos serviços não serão aceitas. A emissão deverá ocorrer a partir do primeiro dia útil do mês seguinte, observando os prazos e procedimentos internos do Banco da Amazônia.

18.4 Em caso de atraso de pagamento por parte do Banco da Amazônia, os valores devidos à CONTRATADA serão atualizados monetariamente desde o termo final do prazo contratual até a data efetiva do pagamento, aplicando-se o índice IPCA/IBGE.

18.5 **Da Forma de Pagamento**

18.5.1 O pagamento será realizado por ordem bancária, mediante crédito em conta corrente vinculada ao CNPJ do contrato, informada previamente pela CONTRATADA.

18.5.2 Considerar-se-á como data do pagamento o dia da emissão da ordem bancária pelo Banco da Amazônia.

18.5.3 No ato do pagamento, serão efetuadas as retenções tributárias previstas na legislação vigente, independentemente dos percentuais indicados na planilha de custos e formação de preços.

18.5.4 A CONTRATADA optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, ficará dispensada das retenções tributárias relativas aos tributos abrangidos por aquele regime, desde que comprove formalmente essa condição mediante documento fiscal ou certidão específica emitida por órgão competente.

18.5.5 Para fins de pagamento a contratada deverá apresentar a **regularidade fiscal**, previdenciária, trabalhista e fundiária da contratada, conforme disposto no item 9.9 deste termo. Caso seja constada a irregularidade fiscal da contratada esta ficará sujeita a aplicação das sanções administrativas previstas neste edital, mas não autoriza, por si só, a retenção dos pagamentos pelos serviços já prestados e recebidos formalmente pelo Banco da Amazônia..

18.6 **Da Liquidação da Despesa**

18.6.1 Recebida a Nota Fiscal ou documento equivalente, iniciar-se-á o prazo de 30 (trinta) dias úteis para a liquidação e pagamento, prorrogável uma única vez por igual período mediante justificativa formal.

18.6.2 Para fins de liquidação, o fiscal técnico verificará se o documento de cobrança contém, no mínimo:

a) prazo de validade;

b) data de emissão;

c) identificação do contrato e do Banco da Amazônia;

d) período de execução a que se refere o pagamento;

e) valor líquido a pagar;

f) destaque das retenções tributárias aplicáveis.

18.6.3 Caso haja erros formais, inconsistências ou pendências que impeçam a liquidação, o pagamento ficará suspenso até a regularização da situação, reiniciando-se o prazo de liquidação após o saneamento, sem ônus ao Banco da Amazônia.

18.7 **Da Execução e Regularidade Durante o Contrato**

18.7.1 Havendo efetiva execução dos serviços e manutenção dos níveis de desempenho contratualmente previstos, os pagamentos poderão ser realizados normalmente até a conclusão do processo administrativo que decida sobre eventual irregularidade ou rescisão contratual, desde que não haja impedimento legal específico.

18.8 **Da Comprovação de Regularidade Fiscal e Trabalhista**

18.8.1 O Banco da Amazônia deverá realizar consulta ao SICAF (Sistema de Cadastramento Unificado de Fornecedores) antes da liquidação de cada pagamento, com o objetivo de verificar a manutenção das condições de habilitação exigidas neste Termo de Referência, e de identificar eventuais proibições de contratar com o Poder Público ou restrições cadastrais.

18.8.2 Constatada irregularidade cadastral, fiscal, previdenciária, trabalhista ou fundiária, o fiscal técnico notificará a CONTRATADA para que regularize sua situação no prazo de 5 (cinco) dias úteis, prorrogáveis uma única vez, a critério do Banco da Amazônia.

18.8.3 Não havendo regularização, ou sendo a defesa considerada improcedente, o Banco da Amazônia comunicará a situação aos órgãos fiscalizadores competentes, informando eventual crédito pendente, de modo a resguardar o interesse público e o erário.

18.8.4 Persistindo a irregularidade, o Banco da Amazônia poderá adotar as medidas administrativas cabíveis, inclusive rescisão contratual motivada, assegurando à CONTRATADA o direito à ampla defesa e ao contraditório, nos termos da legislação vigente.

18.8.5 Enquanto pendente de regularização, a CONTRATADA não fará jus a novos pagamentos relativos às etapas subsequentes de execução contratual, ressalvados os valores referentes a serviços já comprovadamente executados e aceitos pelo Banco da Amazônia.

19 GARANTIAS CONTRATUAIS

19.1 A CONTRATADA deverá manter, durante toda a vigência contratual, garantia de execução em favor do Banco da Amazônia, em uma das modalidades previstas no art. 70 da Lei nº 13.303/2016:

19.2 Caução em dinheiro;

19.3 Fiança bancária; ou

19.4 Seguro-garantia.

19.5 O valor da garantia será correspondente a 5% (cinco por cento) do valor global do contrato.

19.6 A garantia deverá assegurar o cumprimento integral do objeto contratado, incluindo obrigações acessórias, trabalhistas, fiscais e previdenciárias.

19.7 A CONTRATADA deverá apresentar a garantia no prazo máximo de 10 (dez) dias úteis contados da data de assinatura do contrato.

19.8 Em caso de caução em dinheiro, o valor será depositado em conta específica administrada pelo Banco da Amazônia e restituído à CONTRATADA após o encerramento do contrato e a comprovação da inexistência de pendências contratuais ou financeiras.

19.9 O Banco da Amazônia reserva-se o direito de utilizar total ou parcialmente o valor da caução para cobrir eventuais prejuízos decorrentes do descumprimento contratual, inclusive por falhas na execução dos serviços ou paralisações motivadas por atos da CONTRATADA.

19.10 Caso a caução seja utilizada, a CONTRATADA deverá recompor o valor integral da garantia no prazo de 5 (cinco) dias úteis a partir da notificação formal do Banco da Amazônia, sob pena de rescisão contratual.

19.11 A devolução da caução ocorrerá em até 30 (trinta) dias após o término ou rescisão do contrato, desde que comprovada a inexistência de débitos pendentes.

19.12 O Banco da Amazônia deverá constar como beneficiário da apólice, a qual deverá ter validade mínima de 3 (três) meses após o término do contrato.

19.13 A apólice deverá assegurar o pagamento de todas as obrigações contratuais, principais e acessórias.

19.14 A CONTRATADA deverá apresentar nova apólice até 5 (cinco) dias úteis antes do vencimento da anterior e comprovar o pagamento do prêmio no prazo máximo de 2 (dois) dias úteis após seu vencimento.

19.15 No caso de fiança bancária, o instrumento deverá conter, no mínimo:

a) Prazo de validade igual à vigência do contrato acrescido de 3 (três) meses;

b) Declaração expressa do fiador de que atuará como devedor solidário e principal pagador, comprometendo-se ao pagamento de eventuais prejuízos ao Banco da Amazônia independentemente de interpelação judicial;

c) Cláusula de atualização monetária do valor afiançado até o efetivo pagamento.

19.16 Mediante prévia comunicação ao Banco da Amazônia, poderá ser admitida a substituição da modalidade de garantia, desde que dentro das hipóteses legais e sem prejuízo à continuidade das coberturas.

19.17 A garantia deverá ser atualizada sempre que houver reajuste contratual, redimensionamento de volumes ou revisão de preços, de forma a manter-se equivalente a 5% (cinco por cento) do valor global atualizado do contrato.

19.18 A garantia será liberada pelo Banco da Amazônia em até 30 (trinta) dias após o encerramento do contrato, desde que comprovado o cumprimento integral das obrigações contratuais e a inexistência de débitos trabalhistas, fiscais ou previdenciários relacionados ao objeto.

19.19 Nos casos de seguro-garantia ou fiança bancária, o documento deverá conter cláusula que condicione a liberação à comprovação dessas regularidades.

20 DILIGÊNCIAS E VERIFICAÇÕES

20.1 O Banco da Amazônia poderá, a qualquer tempo e sem necessidade de aviso prévio, realizar diligências, inspeções, auditorias técnicas ou vistorias nas dependências da CONTRATADA ou em ambientes de terceiros utilizados na execução dos serviços

gerenciados de segurança (SOC, GVUL e XDR baseado em SIEM), com o objetivo de verificar a conformidade técnica, operacional e de segurança da informação.

20.2 A CONTRATADA deverá assegurar livre acesso às áreas, sistemas, registros e documentos relacionados à execução contratual, prestando todas as informações requeridas e adotando, tempestivamente, as medidas corretivas decorrentes das recomendações emitidas.

20.3 O Banco da Amazônia poderá, igualmente, realizar testes de segurança, varreduras de vulnerabilidade, simulações de intrusão (penetration tests) ou outras avaliações técnicas, com o intuito de verificar a robustez, a conformidade e a resiliência dos ambientes tecnológicos sob responsabilidade da CONTRATADA.

20.4 A CONTRATADA deverá colaborar integralmente com tais verificações, garantindo a integridade das informações e a continuidade dos serviços durante a execução dos testes, responsabilizando-se pela implementação das correções e recomendações identificadas.

20.5 Caso a CONTRATADA mantenha rotina própria de verificação ou escaneamento de vulnerabilidades em seus ambientes de TI, deverá disponibilizar ao Banco da Amazônia, sempre que solicitado, relatórios técnicos atualizados contendo:

a) descrição das vulnerabilidades identificadas e classificadas por criticidade;

b) planos de mitigação e prazos de correção;

c) evidências de tratamento ou justificativas técnicas para vulnerabilidades não corrigidas.

20.6 A CONTRATADA compromete-se a implementar as melhorias recomendadas pelo Banco da Amazônia, pelos auditores internos ou por órgãos de controle, dentro dos prazos formalmente estabelecidos, sob pena de aplicação das penalidades contratuais cabíveis.

20.7 O descumprimento das recomendações técnicas, a recusa de acesso às dependências, sistemas ou registros, ou a obstrução de auditorias e diligências constituirão falha grave de execução contratual, sujeitando a CONTRATADA às sanções previstas neste Termo de Referência, no contrato e na legislação vigente.

21 RELATÓRIO DE SERVIÇOS PRESTADOS (RSP)

21.1 Da Periodicidade e Apresentação

21.1.1 A CONTRATADA deverá apresentar, até o 5º (quinto) dia útil de cada mês, o Relatório de Serviços Prestados (RSP) referente ao mês imediatamente anterior.

21.1.2 O relatório deverá ser submetido à validação da fiscalização técnica e administrativa do Banco da Amazônia, que avaliará no prazo de 5 dias úteis os serviços prestados, e ainda servirá de base para a apuração dos indicadores de desempenho e dos Níveis Mínimos de Serviço (NMS), conforme estabelecido no Anexo I-B.

21.2 Das Reuniões de Acompanhamento

21.2.1 O Banco da Amazônia poderá realizar reunião mensal de acompanhamento, preferencialmente em formato remoto, até 10 (dez) dias após o recebimento do relatório da CONTRATADA, com o objetivo de analisar o desempenho e a conformidade dos serviços executados.

21.2.2 Na reunião, deverão estar presentes, obrigatoriamente, o preposto técnico e o preposto administrativo da CONTRATADA, podendo o Banco da Amazônia solicitar a participação de outros profissionais envolvidos na execução do contrato, quando julgar necessário.

21.2.3 A CONTRATADA será responsável pela elaboração da ata da reunião, devendo encaminhá-la ao Banco da Amazônia por e-mail, no prazo máximo de 5 (cinco) dias úteis após sua realização, para eventuais considerações ou ajustes.

21.3 **Da Verificação e Ajustes do Relatório**

21.3.1 O Banco da Amazônia verificará a conformidade e a consistência dos dados apresentados no RSP, por meio de amostragem técnica e análise cruzada das informações provenientes das ferramentas de monitoramento e gestão.

21.3.2 Identificadas inconformidades ou divergências, a CONTRATADA deverá corrigir e reenviar o relatório ajustado no prazo máximo de 3 (três) dias úteis, contados a partir da solicitação formal do Banco.

21.4 **Da Apuração de Indicadores e Níveis de Serviço**

21.4.1 A apuração dos indicadores e dos Níveis de Serviço será realizada mensalmente, considerando o período de 1º (primeiro) a último dia do mês de referência da execução contratual.

21.4.2 Os resultados apurados no RSP serão utilizados para compor a Nota de Avaliação Mensal (NAM), calculada com base no desempenho da CONTRATADA em relação aos Níveis Mínimos de Serviço definidos no Anexo I-B – Níveis Mínimos de Serviço (NMS).

21.5 **Da Avaliação de Desempenho e Ajuste de Pagamento**

21.5.1 O valor mensal a ser pago à CONTRATADA poderá sofrer ajustes financeiros, positivos ou negativos, em função do desempenho verificado no período.

21.5.2 O cálculo do valor a pagar seguirá a seguinte fórmula:

Valor Mensal = (Valor Total Mensal) × (Fator de Correção Mensal)

onde:

a) Valor Total Mensal representa o custo mensal previsto no contrato;

b) Fator de Correção Mensal é obtido a partir da Nota de Avaliação Mensal (NAM), considerando as penalidades ou bonificações associadas ao cumprimento (ou descumprimento) dos níveis de serviço definidos.

21.5.3 Os ajustes financeiros decorrentes do desempenho da CONTRATADA serão aplicados na fatura do mês imediatamente subsequente ao período de apuração, salvo impossibilidade técnica ou operacional, hipótese em que o desconto será aplicado na fatura posterior, mediante justificativa formal do Banco da Amazônia.

21.5.4 Na fatura referente ao último mês de vigência do contrato, eventuais descontos deverão obrigatoriamente ser aplicados no próprio mês da ocorrência da violação ou do descumprimento dos níveis de serviço.

21.6 **Da Documentação e Rastreabilidade**

21.6.1 O RSP deverá conter, no mínimo:

a) descrição detalhada das atividades realizadas no período;

b) indicadores de desempenho e respectivos resultados;

c) registro de incidentes e vulnerabilidades identificadas e tratadas;

d) quantitativos de logs processados, alertas tratados e ações executadas;

e) ocorrências críticas e respectivas medidas corretivas adotadas;

f) análise de tendências e recomendações de melhoria contínua.

21.6.2 Todos os dados, relatórios e evidências técnicas que fundamentarem o RSP deverão permanecer disponíveis para auditoria e verificação pelo Banco da Amazônia durante toda a vigência contratual e pelo período de 5 (cinco) anos após o término do contrato, nos termos da legislação aplicável.

22 OBRIGAÇÕES DA CONTRATADA

22.1 Da Execução e Conformidade Contratual

22.1.1 Executar o objeto do contrato em estrita conformidade com todas as condições, prazos, níveis de serviço e especificações técnicas estabelecidos neste Termo de Referência, seus anexos e demais documentos que fundamentam a contratação.

22.1.2 Cumprir rigorosamente os prazos contratuais e níveis mínimos de serviço (NMS) definidos, assegurando a plena operacionalidade das soluções e serviços prestados.

22.1.3 Prestar prontamente todos os esclarecimentos e informações solicitados pelo Banco da Amazônia, atendendo tempestivamente às eventuais reclamações, inconformidades ou determinações decorrentes da fiscalização contratual.

22.1.4 Submeter-se integralmente à fiscalização técnica e administrativa exercida pelo Banco da Amazônia, fornecendo toda a documentação, evidências e acesso necessários à verificação da execução contratual.

22.1.5 Providenciar, às suas expensas, todos os meios, recursos humanos, técnicos e logísticos necessários à execução eficiente do objeto contratado.

22.2 Da Responsabilidade Técnica e Operacional

22.2.1 Planejar, desenvolver, implantar, executar, manter e operar os serviços objeto do contrato em conformidade com os acordos de níveis mínimos de serviço (NMS) estabelecidos.

22.2.2 Comunicar imediatamente e por escrito ao Banco da Amazônia qualquer anormalidade, incidente ou situação que comprometa a execução do contrato, propondo medidas corretivas e colaborando na busca de soluções.

22.2.3 Responder pelos danos, prejuízos ou perdas comprovadamente causados ao Banco da Amazônia ou a terceiros, por ação ou omissão, culpa ou dolo de seus empregados, prepostos, representantes ou subcontratados autorizados.

22.2.4 A fiscalização exercida pelo Banco da Amazônia não exime nem atenua a responsabilidade da CONTRATADA pelos danos decorrentes da execução do contrato.

22.2.5 Manter, durante toda a vigência contratual, profissionais qualificados, certificados e em número suficiente para o cumprimento das atividades contratadas, conforme exigências técnicas previstas neste Termo de Referência.

22.3 Da Segurança da Informação e Confidencialidade

22.3.1 Cumprir integralmente as Políticas e os Normativos internos de Segurança da Informação e Cibernética do Banco da Amazônia e adotar boas práticas de segurança em todas as fases do ciclo de vida dos serviços e sistemas.

22.3.2 Assinar, por ocasião da assinatura do contrato, o Termo de Confidencialidade e Sigilo, comprometendo-se a garantir total confidencialidade sobre as informações acessadas, que deverão ser utilizadas exclusivamente para a execução do contrato.

22.3.3 Providenciar, antes do início da prestação dos serviços, a assinatura do Termo de Confidencialidade e Sigilo do Profissional por cada colaborador envolvido na execução do contrato.

22.3.4 Responder, de forma integral e incondicional, por quebra de sigilo, uso indevido de informações, vazamento de dados ou qualquer violação à confidencialidade das informações sob sua guarda.

22.3.5 Concluir a prestação dos serviços com a devolução e eliminação segura de todas as informações e documentos fornecidos pelo Banco da Amazônia, devendo comprovar a destruição segura dos dados conforme metodologias reconhecidas (NIST SP 800-88 Rev. 2).

22.3.6 Responder civil, criminal e administrativamente por qualquer uso indevido, ilegal ou não autorizado de informações, dados ou sistemas do Banco da Amazônia, ainda que praticado por seus empregados ou prepostos, desde que devidamente comprovado.

22.4 **Da Responsabilidades Trabalhistas, Fiscais e Legais**

22.4.1 Assumir integralmente os encargos previdenciários, trabalhistas, fiscais e comerciais decorrentes da execução do contrato, inexistindo qualquer vínculo empregatício entre os empregados da CONTRATADA e o Banco da Amazônia.

22.4.2 Responder por eventuais ações, demandas, custos e despesas judiciais ou administrativas, de natureza trabalhista, cível ou penal, relacionadas à execução dos serviços, eximindo o Banco da Amazônia de qualquer responsabilidade solidária ou subsidiária.

22.4.3 Manter, durante toda a vigência contratual, as condições de habilitação e qualificação técnica e jurídica exigidas na licitação, apresentando sempre que solicitado os comprovantes de regularidade fiscal, trabalhista e previdenciária.

22.4.4 Assumir inteira responsabilidade técnica, operacional e administrativa pela execução do objeto contratado, sendo vedada a transferência ou repasse a terceiros sem prévia autorização formal do Banco da Amazônia.

22.5 **Da Integridade e Cooperação Institucional**

22.5.1 Manter postura ética, transparente e colaborativa em todas as interações com o Banco da Amazônia, comunicando imediatamente quaisquer situações que possam configurar conflito de interesses ou comprometer a integridade da execução contratual.

22.5.2 Indicar formalmente um preposto técnico-administrativo, devidamente qualificado, como responsável pela representação da CONTRATADA perante o Banco da Amazônia e pela interlocução com os fiscais do contrato.

22.5.3 Cooperar com o Banco da Amazônia em auditorias, inspeções e verificações realizadas por órgãos de controle interno ou externo, inclusive o Banco Central do Brasil, nos termos do §1º do art. 33 da Resolução CMN nº 4.557/2017, garantindo acesso às dependências, documentos e registros relacionados ao contrato.

22.5.4 Não repassar a terceiros, em hipótese alguma, dados, informações técnicas, documentação, arquitetura, logs, metadados, produtos desenvolvidos ou quaisquer informações sigilosas obtidas durante a execução do contrato.

22.5.5 Aceitar integralmente a fiscalização permanente exercida pelo Banco da Amazônia quanto ao cumprimento das obrigações contratuais, padrões de segurança, níveis de serviço e resultados de desempenho.

23 OBRIGAÇÕES DO BANCO DA AMAZÔNIA

23.1 Da Gestão e Fiscalização Contratual

23.1.1 Exigir o integral cumprimento das obrigações assumidas pela CONTRATADA, conforme as cláusulas contratuais, o Termo de Referência e sua proposta técnica-comercial.

23.1.2 Exercer a fiscalização técnica, administrativa e operacional dos serviços, por empregados especialmente designados, nos termos da Lei nº 13.303/2016, do Decreto nº 8.945/2016 e do Art. 99 do Regulamento Interno do Banco da Amazônia.

23.1.3 Atestar, por intermédio do Fiscal Técnico do Contrato, as Notas Fiscais/Faturas de Serviços correspondentes às etapas executadas, após a verificação da conformidade e desempenho dos serviços, para fins de liquidação e pagamento.

23.1.4 Rejeitar, no todo ou em parte, os serviços executados em desacordo com as especificações técnicas, níveis mínimos de serviço (NMS) ou demais condições contratuais.

23.1.5 Registrar formalmente as não-conformidades identificadas, determinando prazo para correção e acompanhando a execução das medidas corretivas.

23.2 Da Gestão Financeira e Processual

23.2.1 Efetuar o pagamento das Notas Fiscais/Faturas devidamente aprovadas, observando os prazos e condições previstos neste Termo de Referência e nos documentos contratuais correlatos.

23.2.2 Comunicar tempestivamente à CONTRATADA qualquer irregularidade que impeça o processamento do pagamento, indicando as providências necessárias para saneamento.

23.2.3 Zelar pela observância das normas fiscais, trabalhistas e de integridade, adotando os procedimentos de verificação de regularidade previstos no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

23.3 Da Infraestrutura e Apoio Operacional

23.3.1 Disponibilizar, quando aplicável, infraestrutura adequada para o desempenho das atividades contratadas, incluindo áreas de trabalho, instalações sanitárias, vestiários, rede elétrica e lógica, além de espaço para guarda de materiais, equipamentos e ferramentas utilizados na execução dos serviços.

23.3.2 Garantir o acesso controlado e seguro dos profissionais designados pela CONTRATADA às dependências do Banco da Amazônia – localizado na Avenida Presidente Vargas, nº 800, no bairro da Campina – em Belém do Pará, mediante prévia identificação e autorização, de forma a permitir a execução das atividades previstas.

23.3.3 Assegurar que as ordens de serviço e instruções operacionais sejam direcionadas exclusivamente ao preposto formalmente designado pela CONTRATADA, evitando interferência direta sobre os empregados da contratada.

23.4 **Da Comunicação, Governança e Integridade**

23.4.1 Promover reuniões de acompanhamento e governança contratual, de forma periódica ou sempre que necessário, para avaliação dos resultados, indicadores e relatórios de desempenho (RSP e NAM).

23.4.2 Notificar a CONTRATADA, por escrito, sobre a aplicação de penalidades, descumprimentos contratuais ou falhas na execução dos serviços, fixando prazos para saneamento ou apresentação de defesa.

23.4.3 Fornecer à CONTRATADA cópia atualizada dos normativos internos, políticas e padrões técnicos relacionados à execução dos serviços, especialmente aqueles que tratem de segurança da informação, privacidade e continuidade de negócios.

23.4.4 Assegurar, quando aplicável, o apoio logístico e técnico das áreas internas envolvidas, a fim de viabilizar a integração e a execução coordenada das atividades contratadas.

24 SANÇÕES ADMINISTRATIVAS

24.1 **Da Aplicação das Penalidades**

24.1.1 Pela inexecução total ou parcial do objeto contratual, o Banco da Amazônia poderá aplicar à CONTRATADA, garantido o contraditório e a ampla defesa, as penalidades previstas na Lei nº 13.303/2016, no Decreto nº 8.945/2016 e neste Termo de Referência, sem prejuízo das demais medidas legais cabíveis.

24.1.2 As sanções poderão compreender:

a) Advertência, quando constatadas falhas de execução que não resultem em prejuízo relevante ao Banco;

b) Multa de 10% (dez por cento) sobre o valor global do contrato, em caso de inexecução total do objeto;

c) Multa diária de 0,2% (dois décimos por cento), calculada sobre o valor da respectiva fatura mensal, enquanto perdurar o atraso ou inadimplemento parcial;

d) Suspensão temporária do direito de licitar e contratar com o Banco da Amazônia pelo prazo de até 2 (dois) anos, nos casos de reincidência ou descumprimento grave das obrigações contratuais.

24.2 **Da Rescisão e Consequências Financeiras**

24.2.1 O atraso na execução do objeto por período superior a 30 (trinta) dias consecutivos poderá ensejar, a exclusivo critério do Banco da Amazônia, a rescisão unilateral do contrato, sem prejuízo da aplicação das sanções cabíveis.

24.2.2 A rescisão contratual motivada pela CONTRATADA implicará, de pleno direito, a cobrança de multa compensatória de 10% (dez por cento) sobre o valor total contratado, além da responsabilidade por perdas e danos eventualmente apurados.

24.3 **Do Procedimento Administrativo**

24.3.1 Nenhuma penalidade será aplicada sem a prévia instauração de processo administrativo, assegurados o contraditório e a ampla defesa, com prazo mínimo de 5 (cinco) dias úteis para manifestação da CONTRATADA.

24.3.2 As penalidades poderão ser aplicadas cumulativamente, conforme a gravidade da infração e seus efeitos, observado o princípio da proporcionalidade.

24.3.3 A aplicação de multa não possui caráter compensatório, sendo sua cobrança independente da obrigação da CONTRATADA de reparar eventuais danos materiais ou morais causados ao Banco da Amazônia.

24.4 **Da Cobrança e Execução das Multas**

24.4.1 O valor das multas aplicadas será descontado dos pagamentos devidos à CONTRATADA, após conclusão do processo administrativo.

24.4.2 Na inexistência de saldo a pagar, ou caso este seja insuficiente, a CONTRATADA deverá efetuar o recolhimento do valor devido no prazo máximo de 10 (dez) dias consecutivos, contados da notificação oficial do Banco da Amazônia, mediante depósito identificado em conta específica da instituição.

24.4.3 O não pagamento no prazo estipulado ensejará a cobrança judicial do valor devido, acrescido de correção monetária, juros e demais encargos legais.

25 PREPOSTO DO CONTRATO

25.1 **Da Indicação e Dados de Contato**

25.1.1 No momento da assinatura do contrato, a CONTRATADA deverá informar o nome, telefone e endereço de correio eletrônico corporativo dos profissionais responsáveis pelos seguintes níveis de representação, devendo manter esses dados sempre atualizados durante toda a vigência contratual:

Nível	Cargo
1	Diretor de Vendas e/ou Diretor de Operações
2	Gerente de Vendas Nacional
3	Gerente de Conta
4	Preposto (Representante Administrativo)

25.1.2 Esses profissionais poderão ser acionados pelo Banco da Amazônia sempre que necessário, especialmente para solução de pendências, divergências contratuais ou questões de gestão técnica e operacional.

25.2 **Da Designação do Preposto e Substituto**

25.2.1 A CONTRATADA deverá designar formalmente, no ato da assinatura do contrato, um Preposto (Representante Administrativo) e um substituto eventual, devidamente habilitados para representar a empresa perante o Banco da Amazônia na gestão e acompanhamento da execução contratual.

25.2.2 O substituto atuará exclusivamente nas ausências do titular, sem prejuízo da continuidade dos serviços.

25.2.3 O Banco da Amazônia poderá, a qualquer tempo e mediante justificativa formal, requerer a substituição do Preposto ou de seu substituto, sem ônus adicional à Administração.

25.2.4 A remuneração e encargos trabalhistas dos profissionais indicados constituem encargo exclusivo da CONTRATADA.

25.3 **Da Disponibilidade e Forma de Atuação**

25.3.1 Não se exige do Preposto dedicação exclusiva ou presença diária nas dependências do Banco da Amazônia – localizado na Avenida Presidente Vargas, nº 800, no bairro da Campina – em Belém do Pará, desde que assegurada acessibilidade plena e resposta tempestiva durante o horário comercial do Banco.

25.3.2 O Preposto deverá estar disponível por telefone e e-mail corporativo em dias úteis e participar prontamente de reuniões presenciais ou virtuais, sempre que solicitado pelo Banco da Amazônia.

25.4 **Das Responsabilidades Gerais**

25.4.1 O Preposto será o responsável direto pela gestão administrativa e operacional do contrato, devendo zelar pela execução adequada dos serviços, pela conformidade técnica e pela atuação dos profissionais da CONTRATADA.

25.4.2 Compete ao Preposto:

a) Acompanhar a execução dos serviços, garantindo conformidade com as especificações e níveis mínimos de serviço estabelecidos;

b) Ser o representante oficial da CONTRATADA para recebimento de comunicações, notificações e intimações do Banco da Amazônia;

c) Gerir e supervisionar a equipe alocada, controlando horários, férias, faltas e conduta profissional;

d) Coordenar as providências de acesso físico e lógico dos profissionais às dependências e sistemas do Banco da Amazônia;

e) Comunicar imediatamente o desligamento ou substituição de profissionais, solicitando a revogação de credenciais e acessos;

f) Garantir a capacitação contínua dos profissionais alocados e disseminar internamente as determinações do Banco da Amazônia;

g) Informar tempestivamente qualquer ocorrência que possa comprometer a execução ou a qualidade dos serviços;

h) Elaborar relatórios gerenciais e técnicos, conforme periodicidade e formato estabelecidos pelo Banco da Amazônia;

i) Participar das reuniões periódicas de acompanhamento contratual, discutindo resultados, incidentes e melhorias;

j) Avaliar, em conjunto com o Banco da Amazônia, os níveis de serviço (NAM) e propor medidas corretivas quando necessário;

k) Zelar pela qualidade geral e pela aderência técnica das entregas, assegurando o cumprimento dos prazos e padrões estabelecidos;

l) Supervisionar tecnicamente a equipe da CONTRATADA, garantindo alinhamento com as especificações técnicas deste Termo de Referência;

m) Apresentar e negociar planos de ação corretiva em casos de não conformidade ou impacto nos serviços;

n) Certificar-se da execução das medidas acordadas com o Banco da Amazônia;

o) Garantir a correta aplicação dos fluxos operacionais e procedimentos internos definidos para execução dos serviços;

p) Responder integralmente pelo controle de qualidade das entregas e pela integridade das informações e dados tratados no âmbito do contrato.

26 PROPOSTAS DE PREÇO

26.1 As LICITANTES deverão apresentar propostas contendo os valores unitários, totais e globais, em conformidade com as exigências estabelecidas neste Termo de Referência e demais documentos do processo licitatório.

26.2 Nos preços propostos deverão estar incluídos todos os custos diretos e indiretos necessários ao cumprimento integral do objeto, tais como: salários, softwares, encargos sociais, fiscais e comerciais, impostos, taxas, tributos e quaisquer outras despesas aplicáveis.

26.3 Deverão estar contemplados, ainda, os custos marginais relativos aos profissionais designados para a execução dos serviços, incluindo deslocamentos, hospedagens, treinamentos e demais despesas acessórias.

26.4 Todos os softwares, componentes e equipamentos ofertados deverão corresponder às versões mais recentes disponíveis comercialmente na data de abertura das propostas, assegurando atualização tecnológica e suporte oficial do fabricante.

26.5 A LICITANTE deverá informar o modelo, fabricante, versão e principais características técnicas de cada item de software e hardware ofertado, de forma a garantir a rastreabilidade e a conformidade com as especificações exigidas.

26.6 A LICITANTE deverá apresentar declaração formal de concordância com todos os termos e condições deste Termo de Referência e do Edital correspondente.

26.7 A proposta técnico-comercial deverá ser apresentada:

a) Em papel timbrado da empresa;

b) Assinada pelo responsável legal ou representante devidamente constituído;

c) Redigida em língua portuguesa, com valores expressos em reais (R$).

26.8 A proposta de preços deverá conter, no mínimo:

a) Razão social da empresa LICITANTE, endereço completo e número de inscrição no CNPJ;

b) Declaração expressa de que todos os custos, encargos e despesas de qualquer natureza estão incluídos nos preços propostos. Na ausência dessa declaração, considerar-se-á implícita tal inclusão;

c) Prazo de validade não inferior a 60 (sessenta) dias, contados da data de abertura da sessão pública estabelecida no Edital. Na ausência de menção expressa, aplicar-se-á automaticamente o referido prazo;

d) Dados bancários (instituição financeira, agência e conta corrente) para efeito de pagamento, os quais poderão ser solicitados em momento posterior pela Administração;

e) Telefones, endereço eletrônico corporativo e contatos para comunicações durante o período de vigência contratual;

f) Observância obrigatória ao modelo de proposta de preços constante do Anexo II – Modelo de Proposta de Preço deste Termo de Referência.

27 DOS CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA

27.1 A licitante mais bem classificada deverá encaminhar a proposta de preço adequada ao último lance, no prazo de 2 (duas) horas, prorrogável por igual período, contado da convocação efetuada pelo Pregoeiro.

27.2 prorrogação de prazo de envio da proposta somente poderá ocorrer por solicitação da licitante, mediante justificativa aceita pelo Pregoeiro; ou de ofício, a critério do Pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade.

27.3 O Pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor estimado e à compatibilidade da proposta com as especificações técnicas do objeto, inclusive no que tange aos preços unitários cotados pelo Banco da Amazônia.

27.4 O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Banco da Amazônia ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

27.5 Não se considerará qualquer oferta de vantagem não prevista no edital, inclusive financiamentos subsidiados ou a fundo perdido.

27.6 Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

27.7 Não serão aceitas propostas com valor unitário ou global superior ao estimado.

27.8 Os critérios de aceitabilidade são cumulativos, verificando-se tanto o valor global quanto os valores unitários estimativos da contratação.

27.9 Será desclassificada a proposta que:

27.9.1 Contiver vícios insanáveis;

27.9.2 Não obedecer às especificações técnicas pormenorizadas no edital;

27.9.2.1 Apresentar preços inexequíveis ou permanecer acima do orçamento estimado para a contratação;

27.10 Não tiver sua exequibilidade demonstrada, quando exigido pelo Pregoeiro;

27.11 Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão.

27.12 Apresentar desconformidade com quaisquer outras exigências do edital, desde que insanável;

27.13 Não corrigir ou não justificar eventuais falhas apontadas pelo Pregoeiro. A licitante que abandonar o certame, deixando de enviar a documentação indicada no edital, será desclassificada e sujeitar-se-á às sanções previstas no instrumento convocatório.

27.14 Se a proposta não for aceitável, ou se a licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda ao edital.

28 AVALIAÇÃO DO FORNECEDOR

28.1 Da Finalidade e Periodicidade

28.1.1 Com o objetivo de promover a melhoria contínua da gestão contratual, o Banco da Amazônia realizará, no início de cada semestre, a Avaliação de Desempenho da CONTRATADA, contemplando aspectos técnicos, operacionais e comportamentais relacionados à execução do contrato.

28.1.2 Os resultados obtidos subsidiarão ações corretivas, revisões de processo e aprimoramentos no modelo de atendimento, assegurando maior eficiência, transparência e governança na relação contratual.

28.2 Dos Critérios de Avaliação

28.2.1 A avaliação semestral contemplará, no mínimo, os seguintes critérios qualitativos:

a) Comunicação: clareza e precisão das informações transmitidas; adequação da linguagem técnica; tempestividade nas respostas; cordialidade, urbanidade e nível de formalidade no relacionamento com as equipes do Banco da Amazônia.

b) Confiabilidade: qualidade e exatidão dos serviços prestados, ausência de erros recorrentes, aderência às especificações contratuais e eficácia das medidas corretivas e preventivas adotadas.

c) Organização e Gestão: evidência de planejamento, integração e controle das atividades; cumprimento de prazos; domínio técnico dos profissionais designados; e regularidade na entrega dos relatórios e indicadores de desempenho (RSP e NAM).

28.3 Da Escala de Avaliação e Conceitos

28.3.1 Cada critério será avaliado com nota de 0 (zero) a 10 (dez), conforme desempenho observado.

28.3.2 A média aritmética das notas resultará no conceito global de desempenho, conforme escala a seguir:

a) Péssimo: 0,0 a 4,9

b) Regular: 5,0 a 7,4

c) Bom: 7,5 a 8,9

d) Ótimo: 9,0 a 10,0

28.3.3 A avaliação será conduzida pelos fiscais técnico e administrativo do contrato, com base em evidências documentais, relatórios mensais e registros de desempenho operacional.

28.4 Da Comunicação dos Resultados e Ações Corretivas

28.4.1 A CONTRATADA será formalmente comunicada sobre o conceito médio obtido, o qual será registrado nos sistemas de controle e histórico de desempenho de fornecedores do Banco da Amazônia.

28.4.2 Quando a avaliação resultar em conceito inferior a “Bom”, o Banco da Amazônia poderá determinar a elaboração de plano de ação corretivo, com prazos e metas específicas para melhoria do desempenho.

28.4.3 A reincidência em desempenho “Regular” ou “Péssimo” poderá ensejar a aplicação de advertência formal e será considerada fator negativo em eventuais renovações, prorrogações ou novas contratações futuras com o Banco da Amazônia.

29 RESCISÃO CONTRATUAL

29.1 A rescisão contratual poderá ocorrer de forma consensual, administrativa ou judicial, observadas as disposições da Lei nº 13.303/2016, deste Termo de Referência e do respectivo instrumento contratual.

29.2 São modalidades de rescisão:

a) Distrato – pela inexecução total ou parcial das cláusulas contratuais, devidamente formalizado;

b) Acordo entre as partes, reduzido a termo no processo de contratação, quando houver conveniência para o Banco da Amazônia, mediante autorização escrita e fundamentada, precedida de aviso prévio mínimo de 30 (trinta) dias;

c) Judicial, nos termos da legislação aplicável.

29.3 **Dos Motivos para Rescisão**

29.3.1 Constituem motivos para rescisão do contrato, sem prejuízo das demais sanções legais e contratuais:

a) paralisação injustificada ou atraso reiterado na execução dos serviços;

b) não cumprimento de cláusulas contratuais, especificações técnicas ou prazos;

c) cessão, subcontratação ou transferência total ou parcial do contrato, não previstas neste termo de referência e sem autorização expressa do Banco da Amazônia;

d) desatendimento às determinações formais da fiscalização contratual;

e) cometimento reiterado de faltas ou falhas operacionais na execução dos serviços;

f) decretação de falência, pedido de recuperação judicial ou extrajudicial;

g) dissolução da sociedade contratada;

h) alteração societária que modifique o controle acionário, a finalidade ou a estrutura da CONTRATADA, de modo a comprometer a execução contratual;

i) prática de fraude fiscal, trabalhista ou previdenciária;

j) descumprimento de obrigações legais, regulatórias ou de conformidade;

k) utilização de mão de obra em desacordo com o art. 7º, XXXIII, da Constituição Federal;

l) comprovação de ato que afete a idoneidade, reputação ou capacidade técnica da CONTRATADA;

m) razões de interesse público devidamente justificadas;

n) ocorrência de caso fortuito ou força maior, comprovadamente impeditiva da execução;

o) perda da regularidade fiscal, trabalhista, previdenciária ou do FGTS;

p) uso indevido, divulgação ou apropriação de informações sigilosas do Banco da Amazônia.

29.4 **Da Rescisão por Denúncia**

29.4.1 O Banco da Amazônia poderá, a qualquer tempo, mediante aviso com antecedência mínima de 30 (trinta) dias, denunciar o contrato, por razões de conveniência e oportunidade administrativa, sem que caiba à CONTRATADA qualquer indenização, multa ou compensação, ressalvadas as hipóteses previstas em lei.

29.5 **Das Hipóteses Adicionais**

29.5.1 Também constituem motivos para rescisão imediata:

a) não apresentação ou insuficiência da garantia contratual;

b) declaração de inidoneidade por qualquer órgão da Administração Pública;

c) protesto de títulos, execução fiscal ou outras evidências de comprometimento da capacidade econômico-financeira;

d) reincidência em falhas graves ou inexecuções parciais do contrato;

e) descumprimento de obrigações de confidencialidade ou segurança da informação;

f) constatação de irregularidades graves em auditorias, diligências ou fiscalizações.

29.6 **Dos Efeitos da Rescisão**

a) A rescisão acarretará a execução imediata da garantia contratual, quando existente, para ressarcimento ao Banco da Amazônia de multas, indenizações e demais valores devidos;

b) Havendo créditos pendentes da CONTRATADA, o Banco poderá reter valores até o limite dos prejuízos apurados;

c) As penalidades e responsabilidades da CONTRATADA por danos, perdas ou ilícitos permanecem vigentes mesmo após a rescisão do contrato;

d) A rescisão deverá ser formalmente motivada nos autos do processo administrativo, assegurando-se o contraditório e a ampla defesa à CONTRATADA;

e) O Banco da Amazônia poderá assumir diretamente a execução ou contratar terceiros para conclusão dos serviços, sem prejuízo das penalidades aplicáveis à CONTRATADA.

30 DOS CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL, SOCIAL E TRABALHISTA E ECONÔMICA FINANCEIRA

30.1 A fase de habilitação sucederá às fases de apresentação de propostas, lances e julgamento, observando-se o disposto na Lei nº 13.303/2016, no Regulamento de Licitações e Contratos do Banco da Amazônia e nas demais normas aplicáveis.

30.2 **Da Habilitação Jurídica**

30.2.1 Para comprovar a capacidade jurídica de exercer direitos e assumir obrigações, a LICITANTE deverá apresentar:

a) Contrato social, estatuto ou ato constitutivo atualizado, devidamente registrado no órgão competente;

b) Documentos que comprovem os poderes de representação de seus administradores ou procuradores, inclusive instrumentos de mandato, quando for o caso;

c) Decreto de autorização para funcionamento no País, no caso de empresas estrangeiras, conforme legislação aplicável;

d) Cópias do CPF e do RG ou CNH dos representantes legais e/ou procuradores habilitados para assinatura do contrato.

30.3 **Da Habilitação Fiscal, Social e Trabalhista**

30.3.1 A LICITANTE deverá apresentar documentação comprobatória de regularidade fiscal e trabalhista, conforme exigências do Sistema de Cadastramento Unificado de Fornecedores – SICAF ou, alternativamente, mediante as seguintes certidões:

a) Cartão de inscrição no CNPJ ou CPF, conforme o caso;

b) Comprovante de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativo à sede da LICITANTE e pertinente ao ramo de atividade;

c) Certidão de regularidade fiscal perante as Fazendas Federal, Estadual e Municipal ou Distrital, negativas ou positivas com efeito de negativa;

d) Certidão Negativa ou Positiva com efeito de Negativa de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União;

e) Certidão de Regularidade do FGTS (CRF);

f) Certidão Negativa ou Positiva com efeito de Negativa de Débitos Trabalhistas (CNDT);

g) Declaração de não empregar menor, conforme art. 7º, inciso XXXIII, da Constituição Federal;

h) Declaração de conhecimento e observância do Decreto nº 7.203/2010, que dispõe sobre a vedação ao nepotismo no âmbito da administração pública.

30.3.2 Os documentos acima poderão ser substituídos por meios eletrônicos idôneos e legalmente válidos que comprovem a regularidade da LICITANTE, desde que emitidos por órgãos oficiais competentes.

30.4 **Da Habilitação Econômico-Financeira**

30.4.1 A LICITANTE deverá apresentar Balanço Patrimonial e Demonstrações Contábeis do último exercício social, devidamente registrados, que comprovem sua boa situação financeira, demonstrada por meio dos seguintes índices, todos com valores superiores a 1 (um):

a) Liquidez Geral (LG)

$$LG = \frac{Ativo\ Circulante\ +\ Realiza\acute{}vel\ a\ Longo\ Prazo}{Passivo\ Circulante\ +\ Passivo\ Não\ Circulante}$$

b) Liquidez Corrente (LC)

$$LC = \frac{Ativo\ Circulante}{Passivo\ Circulante}$$

c) Solvência Geral (SG)

$$SG = \frac{Ativo\ Total}{Passivo\ Circulante\ +\ Passivo\ Não\ Circulante}$$

30.4.2 Apresentar Certidão Negativa de Falência ou Recuperação Judicial, emitida pelo distribuidor da sede da empresa.

30.4.3 A LICITANTE que obtiver índice igual ou inferior a 1 (um) em qualquer dos parâmetros deverá comprovar patrimônio líquido mínimo equivalente a 10% (dez por cento) do valor total estimado da contratação.

30.4.4 Empresas com menos de um ano de constituição deverão apresentar Balanço de Abertura e, quando aplicável, Balanço Intermediário, devidamente assinados pelo administrador e contador, com registro no órgão competente.

30.4.5 Empresas inativas no exercício anterior deverão apresentar as demonstrações contábeis do último exercício ativo, Certidão de Inatividade e Balanço de Reabertura.

30.4.6 Empresas em recuperação judicial ou extrajudicial poderão participar da licitação, desde que comprovem o atendimento integral às condições econômico-financeiras exigidas neste Termo.

30.4.7 Microempresas (ME) e Empresas de Pequeno Porte (EPP) deverão cumprir integralmente as exigências de habilitação, observadas as prerrogativas legais da Lei Complementar nº 123/2006.

30.5 **Das Outras Condições de Habilitação**

30.5.1 A LICITANTE deverá apresentar, nos modelos definidos pelo Banco da Amazônia, as seguintes declarações:

a) Declaração de conhecimento do Art. 38 da Lei nº 13.303/2016;

b) Declaração de Inexistência de Fato Impeditivo ou Superveniente;

c) Declaração de Inexistência de Empregado do Banco da Amazônia em seu quadro funcional;

d) Declaração de Conhecimento da Lei de Improbidade Administrativa (Lei nº 8.429/1992);

e) Declaração de enquadramento como ME ou EPP, quando aplicável.

30.6 **Da Verificação em Listas Restritivas**

30.6.1 O Banco da Amazônia realizará consultas às listas de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT).

30.6.2 A LICITANTE que apresentar restrições nessas listas será desclassificada, salvo decisão expressa e fundamentada do comitê competente do Banco.

30.7 **Da Manutenção das Condições de Habilitação**

30.7.1 A CONTRATADA obriga-se a manter, durante toda a vigência contratual, todas as condições de habilitação e qualificação exigidas neste Termo de Referência, compatíveis com as obrigações assumidas, sob pena de aplicação das sanções previstas.

30.8 **Da Participação de consórcios**

30.8.1 Será admitida a participação de agentes econômicos reunidos em consórcio.

31 CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA

31.1 **Da Comprovação da Capacidade Técnico-Operacional**

31.1.1 A propensa **CONTRATADA** deverão apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove a aptidão da licitante para o desempenho de atividade pertinente e compatível em características e quantidade equivalentes com o objeto da presente contratação.

31.1.2 A comprovação a que se refere o item anterior deverá abranger 50% (cinquenta por cento) dos grupos de requisitos funcionais previstos no item 1.2 deste Termo de Referência, percentual fixado com fundamento no art. 79, itens 2 e 3, do Regulamento de Licitações e Contratos do Banco da Amazônia.

31.1.3 As LICITANTES deverão comprovar aptidão técnico-operacional para a execução de serviços pertinentes e compatíveis, em características, complexidade e porte, com as parcelas de maior relevância do objeto desta contratação, mediante apresentação de um ou mais Atestados de Capacidade Técnica, emitidos por pessoa jurídica de direito público ou privado.

31.1.4 Para fins de qualificação técnica, serão consideradas pertinentes as experiências relacionadas à prestação de Serviços Gerenciados de Segurança Cibernética, compreendendo atividades de SOC, monitoramento e correlação de eventos, XDR baseado em SIEM, Gestão de Vulnerabilidades – GVUL, resposta a incidentes e capacidades correlatas compatíveis com o objeto.

31.1.5 Os atestados poderão ser apresentados em documento físico ou eletrônico, desde que permitam identificar o emitente, o objeto executado e as informações necessárias à aferição da experiência declarada, não sendo exigida forma documental específica que restrinja injustificadamente sua aceitação.

31.2 **Do Somatório de Atestados**

31.2.1 Serão aceitos quantos atestados forem necessários para a comprovação dos quantitativos através de sua soma.

31.2.2 Será admitida a apresentação de mais de um atestado de capacidade técnica, podendo suas experiências ser consideradas em conjunto para comprovação das parcelas relevantes do objeto, desde que os serviços comprovados sejam tecnicamente compatíveis e permitam aferir a capacidade operacional necessária à execução da contratação.

31.2.3 O somatório de atestados não estará condicionado, como regra geral, à concomitância dos respectivos períodos de execução, quando a natureza, a complexidade e a técnica empregadas nos serviços não variarem em razão da dimensão quantitativa.

31.2.4 Exclusivamente quando o somatório for utilizado para comprovar capacidade operacional simultânea relacionada à volumetria mínima de 150 GB/dia de ingestão de logs e eventos, os períodos de execução considerados deverão ser concomitantes, de modo a demonstrar que a LICITANTE efetivamente possuía capacidade para operar, em um mesmo período, volume equivalente ao mínimo exigido.

31.2.5 Não será admitida a soma meramente aritmética de volumes executados em períodos sucessivos para atendimento do requisito de capacidade simultânea previsto no item 31.2.3.

31.2.6 Esse ajuste mantém a concomitância somente onde existe justificativa técnica objetiva: demonstrar capacidade simultânea de processamento.

31.3 **Do Período de Experiência**

31.3.1 Os atestados deverão referir-se a contratos concluídos ou que tenham alcançado, no mínimo, 12 (doze) meses de execução contínua, de forma a demonstrar experiência na prestação sustentada de serviços de segurança cibernética.

31.3.2 Quando o contrato que fundamenta o atestado possuir prazo total inferior a 12 (doze) meses, poderá ser aceita a comprovação de sua execução integral, mediante apresentação do respectivo instrumento contratual ou de documentação equivalente.

31.3.3 O período mínimo estabelecido neste item destina-se à comprovação da capacidade de prestação continuada dos serviços, considerando a natureza ininterrupta e crítica da operação prevista para o Cyber Fusion Center.

31.4 **Da Verificação da Autenticidade e das Diligências**

31.4.1 As LICITANTES deverão disponibilizar informações suficientes para permitir a verificação da autenticidade e legitimidade dos atestados apresentados.

31.4.2 O Banco da Amazônia poderá promover diligências junto aos emitentes dos atestados, solicitar esclarecimentos e requerer documentação complementar destinada a confirmar ou esclarecer as informações apresentadas.

31.4.3 Poderão ser utilizados como documentação complementar, entre outros:

a) contratos e respectivos aditivos;
b) Ordens de Serviço;
c) relatórios de execução;
d) termos de aceite;
e) notas fiscais;
f) declarações complementares emitidas pelo contratante anterior;
g) documentos de medição; e
h) outros documentos idôneos capazes de demonstrar a natureza, o porte ou a execução dos serviços.

31.4.4 A diligência poderá ser utilizada para esclarecer, complementar ou confirmar informações constantes da documentação apresentada, observadas as regras aplicáveis ao procedimento licitatório.

31.5 **Da Comprovação Técnico-Operacional das Parcelas Relevantes**

31.5.1 A LICITANTE deverá comprovar experiência na prestação de Serviço Gerenciado de Monitoramento e Resposta a Incidentes – SOC, Cyber Fusion Center ou serviço gerenciado de segurança cibernética de natureza equivalente, contemplando capacidade de ingestão de, no mínimo, 150 GB/dia de logs e eventos de segurança, correspondente a 25% (vinte e cinco por cento) da capacidade mínima de 600 GB/dia prevista para esta contratação.

31.5.2 A comprovação da volumetria mínima poderá constar diretamente do atestado ou ser demonstrada por documentação complementar emitida ou validada pelo contratante anterior, desde que seja possível aferir objetivamente a capacidade executada.

31.5.3 Deverá ser comprovada experiência em operação contínua 24x7x365, envolvendo concomitantemente, em um mesmo ambiente de serviços gerenciados, pelo menos duas das seguintes capacidades:

a) monitoramento, correlação e resposta a incidentes por meio de SIEM ou tecnologia equivalente;

b) Detecção e Resposta Estendida – XDR baseado em SIEM ou capacidade equivalente;

c) Gestão de Vulnerabilidades – GVUL;

d) resposta operacional a incidentes de segurança cibernética; ou

e) serviços equivalentes que demonstrem integração entre detecção, análise, vulnerabilidades e resposta a incidentes.

31.5.4 Não será exigido que a experiência anterior tenha sido denominada formalmente “Cyber Fusion Center”, desde que as atividades comprovadas demonstrem complexidade, integração e características compatíveis com as parcelas relevantes desta contratação.

31.6 **Do Conteúdo dos Atestados**

31.6.1 Os atestados de capacidade técnica deverão conter informações suficientes para permitir a identificação e avaliação da experiência comprovada, incluindo, no mínimo:

a) identificação da pessoa jurídica emitente;

b) identificação ou forma de contato com o responsável pela emissão ou validação das informações;

c) descrição do objeto ou dos serviços executados, em nível suficiente para demonstrar sua pertinência e compatibilidade com a contratação;

d) período de execução;

e) informação relativa à operação contínua 24x7x365, quando utilizada para atendimento do requisito correspondente;

f) volumetria ou capacidade executada, quando necessária à comprovação do requisito previsto no item 7.5.1; e

g) indicação de que os serviços foram executados satisfatoriamente.

31.6.2 Não será exigido que o próprio atestado contenha, obrigatoriamente, informações detalhadas sobre fabricante, módulos, versões, quantidade de usuários ou outros elementos técnicos específicos que não sejam normalmente registrados em documentos dessa natureza.

31.6.3 Quando as informações do atestado forem insuficientes para aferição de determinado requisito, o Banco poderá solicitar documentação complementar ou realizar diligência, nos termos do item 7.4.

31.7 **Da Pertinência e Compatibilidade Técnica**

31.7.1 Serão considerados pertinentes e compatíveis os serviços que demonstrem experiência na execução de atividades de segurança cibernética gerenciada de natureza, complexidade e porte compatíveis com as parcelas relevantes da contratação, independentemente do fabricante ou da plataforma tecnológica utilizada na experiência anterior.

31.7.2 A comprovação de capacidade técnico-operacional não dependerá de experiência prévia com a mesma solução, fabricante, produto ou arquitetura tecnológica que venha a ser ofertada ao Banco da Amazônia.

31.7.3 Serão admitidas experiências obtidas mediante utilização de tecnologias distintas, desde que comprovem a execução de serviços funcional e operacionalmente equivalentes aos requisitos de qualificação estabelecidos.

31.7.4 O domínio, a aderência funcional, a capacidade de integração, o desempenho e as demais características da solução efetivamente ofertada na licitação serão avaliados por meio da Prova de Conceito – POC, conforme o Anexo I C, não constituindo requisito de experiência pretérita vinculado a fabricante específico.

31.8 **Da Verificação e Diligência Técnica**

31.8.1 O Banco da Amazônia poderá realizar diligências destinadas à confirmação da experiência técnico-operacional apresentada, inclusive mediante contato com os emitentes dos atestados, entrevistas técnicas ou, quando devidamente justificado, visitas às organizações que tenham contratado os serviços declarados.

31.8.2 Durante a diligência poderão ser solicitados contratos, Ordens de Serviço, relatórios, termos de aceite, notas fiscais, documentos de medição ou outros elementos relacionados à execução dos serviços.

31.8.3 As diligências terão por finalidade verificar a autenticidade, esclarecer informações e confirmar a efetiva compatibilidade da experiência apresentada com os requisitos de qualificação técnica.

31.9 **Da Declaração de Capacidade Técnica**

31.9.1 A comprovação da capacidade técnico-operacional será realizada primordialmente por meio dos atestados emitidos por contratantes anteriores, nos termos dos itens precedentes, não podendo declaração unilateral da própria LICITANTE substituí-los.

31.9.2 A LICITANTE deverá apresentar, adicionalmente, a Declaração Complementar de Capacidade e Compromisso Técnico, conforme modelo constante do Anexo I-E, declarando:

a) ciência integral dos requisitos técnicos e operacionais da contratação;

b) capacidade de mobilizar estrutura técnica e operacional compatível com os serviços;

c) compromisso de disponibilizar, na fase de implantação, equipe técnica dimensionada e qualificada nos termos deste Termo de Referência;

d) compromisso de manter a operação 24x7x365 e cumprir os Níveis Mínimos de Serviço;

e) ciência dos requisitos de integração, segurança, continuidade e governança; e

f) compromisso de apresentar, no momento contratualmente previsto, os documentos comprobatórios relativos aos profissionais que efetivamente atuarão na execução.

31.9.3 A declaração prevista neste item possui natureza complementar e não substitui os Atestados de Capacidade Técnica exigidos para comprovação da experiência técnico-operacional.

31.10 **Da Equipe Técnica e do Momento de sua Comprovação**

31.10.1 A qualificação técnico-operacional exigida na fase de habilitação refere-se à capacidade e à experiência da LICITANTE, não sendo exigida, como condição de habilitação, a indicação nominativa, comprovação de vínculo empregatício ou apresentação das certificações de todos os profissionais que integrarão a equipe de execução contratual.

31.10.2 A CONTRATADA deverá apresentar, durante a fase de implantação e nos prazos estabelecidos neste Termo de Referência, a composição efetiva da equipe técnica, acompanhada da documentação necessária à comprovação da formação, experiência, certificações e demais qualificações aplicáveis aos respectivos perfis.

31.10.3 Quando determinada certificação estiver prevista como requisito para perfil profissional específico, serão admitidas certificações equivalentes, desde que possuam escopo, nível de conhecimento e complexidade compatíveis com a atividade exercida.

31.10.4 O dimensionamento quantitativo da equipe será de responsabilidade da CONTRATADA, devendo ser suficiente para assegurar, objetivamente:

a) operação contínua 24x7x365;

b) cumprimento integral dos Níveis Mínimos de Serviço;

c) atendimento simultâneo a eventos e incidentes compatível com a criticidade do ambiente;

d) cobertura dos níveis operacionais e especialidades previstos;

e) supervisão técnica contínua;

f) continuidade durante férias, afastamentos, substituições ou indisponibilidades;

g) handover adequado entre turnos;

h) atendimento a situações críticas e aumentos excepcionais de demanda; e

i) execução das atividades sob demanda sem prejuízo dos serviços continuados.

31.10.5 A aprovação pelo Banco do dimensionamento da equipe estará vinculada exclusivamente à demonstração do atendimento aos critérios objetivos estabelecidos no item 31.10.4. e às demais exigências técnicas do Termo de Referência, não podendo ser baseada em juízo discricionário desvinculado desses parâmetros.

31.10.6 Caso a equipe apresentada ou mantida pela CONTRATADA se mostre insuficiente para cumprimento dos NMS, cobertura operacional, simultaneidade de atendimento ou continuidade dos serviços, caberá à CONTRATADA promover, sem ônus adicional ao Banco, os ajustes de dimensionamento necessários.

32 VEDAÇÕES

32.1 Da Cessão e Transferência

32.1.1 É vedada a cessão, transferência ou subcontratação, total ou parcial, dos direitos e obrigações decorrentes deste contrato, salvo nas hipóteses expressamente previstas neste termo de referência, sem autorização expressa e prévia do Banco da Amazônia, desde que observadas as condições estabelecidas neste Termo de Referência e mantidas todas as garantias e obrigações contratuais.

32.2 Das Restrições de Divulgação e Uso

32.2.1 É expressamente vedado à CONTRATADA, salvo autorização formal e expressa do Banco da Amazônia:

a) Veicular publicidade, campanhas ou materiais de divulgação que utilizem o nome, marca, logotipo, imagem institucional ou menção à relação contratual com o Banco da Amazônia como apelo mercadológico ou promocional;

b) Utilizar este contrato como garantia financeira, objeto de cessão de crédito ou lastro em operações de desconto bancário perante terceiros;

c) Usar, reproduzir, copiar ou reter quaisquer informações, dados, documentos, sistemas, imagens, relatórios, códigos, bancos de dados ou quaisquer outros ativos de propriedade do Banco da Amazônia, fora dos limites estritamente necessários à execução contratual;

d) Divulgar ou compartilhar com terceiros quaisquer informações classificadas como sigilosas, estratégicas ou restritas, sob pena de responsabilização civil, administrativa e penal.

32.3 Da Vedação de Nepotismo

32.3.1 Nos termos do artigo 7º do Decreto nº 7.203/2010, que dispõe sobre a vedação ao nepotismo no âmbito da administração pública federal, é proibido à CONTRATADA, durante toda a vigência contratual, empregar ou manter vínculo profissional com cônjuge, companheiro ou parente, em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, de empregado do Banco da Amazônia que exerça cargo em comissão ou função de confiança.

32.4 A inobservância destas disposições sujeitará a CONTRATADA às penalidades cabíveis e poderá ensejar a rescisão imediata do contrato, sem ônus para o Banco da Amazônia.

33 DOS CRITÉRIOS DE SUSTENTABILIDADE

33.1 Do Compromisso com as Políticas Institucionais do Banco da Amazônia

33.1.1 A CONTRATADA se compromete a atender integralmente às diretrizes da Política de Responsabilidade Socioambiental do Banco da Amazônia – PRSAC (disponível em:https://www.bancoamazonia.com.br/component/edocman/prsac/viewdocument/5204) e da Política Geral de Contratações (disponível em: https://www.bancoamazonia.com.br/component/edocman/politica-geral-de-contratacoes/viewdocument/5727), observando os requisitos mínimos descritos a seguir.

33.2 Das Condições de Trabalho e Direitos Humanos

a) Não permitir a prática de trabalho análogo ao escravo, infantil ou qualquer outra forma de trabalho ilegal;

b) Empenhar esforços para que seus fornecedores, parceiros e subcontratados também adotem as mesmas práticas de respeito aos direitos humanos e trabalhistas;

c) Não empregar menores de 18 (dezoito) anos em atividades noturnas, perigosas ou insalubres, nem menores de 16 (dezesseis) anos em qualquer atividade laboral, exceto na condição de aprendiz a partir dos 14 (quatorze) anos, conforme legislação vigente;

d) Não permitir discriminação no acesso ou permanência no emprego em razão de sexo, gênero, raça, cor, origem, condição física, religião, estado civil, idade, orientação sexual, condição familiar, estado gravídico ou qualquer outra forma de preconceito;

e) Respeitar o direito de sindicalização, de negociação coletiva e de organização dos trabalhadores, vedadas quaisquer represálias.

33.3 Da Saúde, Segurança e Meio Ambiente

a) Cumprir rigorosamente a legislação ambiental, fiscal, trabalhista, previdenciária e de segurança e saúde ocupacional aplicáveis;

b) Adotar práticas preventivas que evitem danos ambientais e implementar ações corretivas sempre que houver impacto decorrente de suas atividades;

c) Observar a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), promovendo o descarte adequado, reutilização e reciclagem de materiais de forma ecologicamente correta;

d) Evitar a exposição de colaboradores a condições ultrajantes, sub-humanas ou degradantes, definidas nos subitens a seguir:

i) Condições ultrajantes: aquelas que exponham o indivíduo de forma ofensiva, imoral ou humilhante;

ii) Condições sub-humanas: situações de degradação abaixo dos limites mínimos de dignidade humana;

iii) Condições degradantes: condições que privem o trabalhador de direitos fundamentais ou o submetam a tratamento semelhante à escravidão.

33.4 **Das Integridade, Ética e Conformidade Legal**

a) Atender integralmente à legislação e aos regulamentos que tratam da prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT);

b) Não possuir registro ativo de sanções impeditivas de contratar com a Administração Pública, tampouco constar no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);

c) Adotar controles internos compatíveis com as boas práticas de governança, integridade e compliance, conforme diretrizes anticorrupção do Banco da Amazônia e legislação correlata;

d) Adotar medidas e controles técnicos voltados à proteção da confidencialidade, integridade e disponibilidade das informações, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD);

e) Manter registro e comprovação documental da conformidade de seus processos com os dispositivos legais, disponibilizando-os ao Banco da Amazônia sempre que solicitado.

33.5 **Das Sanções por Descumprimento**

33.5.1 O Banco da Amazônia poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir o contrato de forma imediata e unilateral, sem ônus ou penalidades, garantido o direito de defesa, caso seja comprovado que a CONTRATADA, seus subcontratados ou fornecedores:

a) utilizem trabalho em desconformidade com as condições legais e éticas previstas neste Termo de Referência;

b) pratiquem atos lesivos à integridade humana, ao meio ambiente ou aos direitos trabalhistas;

c) incorram em violação das políticas institucionais do Banco da Amazônia ou da legislação vigente.

34 INTEGRIDADE, DA CONDUTA ÉTICA E DOS PROCEDIMENTOS ANTICORRUPÇÃO

34.1 **Dos Compromissos Gerais**

34.1.1 O contrato oriundo desta contratação deverá conter cláusula expressa pela qual as partes declaram conhecer e cumprir integralmente as normas de prevenção e combate à corrupção previstas na legislação brasileira, em especial a Lei de Improbidade Administrativa (Lei nº 8.429, de 02 de junho de 1992), a Lei Anticorrupção Empresarial (Lei nº 12.846, de 01 de agosto de 2013) e seus regulamentos e demais dispositivos legais aplicáveis às empresas públicas e sociedades de economia mista.

34.1.2 As partes comprometem-se a cumprir fielmente tais normas, por si, por seus sócios, administradores, empregados, prepostos e terceiros contratados, mantendo e observando, durante toda a vigência contratual, um Código de Ética e Conduta próprio, que estabeleça padrões compatíveis com a legislação e com os princípios de integridade corporativa.

34.2 **Das Proibições e Condutas Vedadas**

34.2.1 Fica expressamente vedado às partes, seus representantes e contratados:

a) Prometer, oferecer, conceder, solicitar ou receber, direta ou indiretamente, vantagem indevida de qualquer natureza, em favor próprio ou de terceiros, com o intuito de influenciar ato ou decisão administrativa, direcionar negócios ou obter benefício ilícito;

b) Financiar, custear, patrocinar ou de qualquer modo subvencionar atos ilícitos ou práticas corruptas, inclusive fraudes licitatórias ou contratuais;

c) Utilizar intermediários, consultores ou parceiros para dissimular a oferta ou recebimento de vantagens indevidas;

d) Praticar atos de corrupção, suborno, extorsão, fraude, tráfico de influência ou lavagem de dinheiro, em qualquer esfera da relação contratual.

34.3 **Da Prevenção e Monitoramento**

34.3.1 A CONTRATADA deverá adotar mecanismos de integridade, auditoria e controle interno, incluindo políticas de prevenção, detecção e resposta a riscos de corrupção, fraude e lavagem de dinheiro, bem como procedimentos de verificação e due diligence aplicáveis a seus administradores, colaboradores e fornecedores.

34.3.2 Deverá ainda colaborar com o Banco da Amazônia em eventuais auditorias, fiscalizações ou diligências voltadas à apuração de fatos relacionados à integridade contratual.

34.4 **Da Aderência ao Código de Conduta Ética do Banco da Amazônia**

34.4.1 A CONTRATADA deverá respeitar e assegurar que seus empregados e representantes respeitem, no que couber, os princípios e valores éticos previstos no Código de Conduta Ética do Banco da Amazônia, disponível em: https://www.bancoamazonia.com.br/component/edocman/relacoes-investidores/governanca-corporativa/codigo-etica

34.5 **Das Sanções e Consequências**

34.5.1 A comprovação de violação às obrigações previstas neste item, inclusive mediante dolo, fraude ou corrupção, constituirá causa de rescisão unilateral e imediata do contrato pelo Banco da Amazônia, sem ônus para a Administração, e ensejará a aplicação das penalidades cabíveis, sem prejuízo do ressarcimento por eventuais perdas e danos.

34.6 **Da Responsabilização Independente**

34.6.1 A aplicação das penalidades previstas na Lei nº 12.846/2013 não exclui ou substitui os demais processos de responsabilização civil, administrativa e penal decorrentes de ilícitos praticados no âmbito do contrato.

35 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

35.1 A CONTRATADA, por si, por seus colaboradores e por eventuais subcontratados, deverá:

a) observar as determinações de órgãos reguladores e fiscalizadores sobre a matéria, inclusive as emanadas da Autoridade Nacional de Proteção de Dados (ANPD); e

b) atuar em conformidade com toda a legislação vigente sobre proteção de dados pessoais, em especial a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), a Resolução CD/ANPD nº 15/2024, relativa à comunicação de incidentes de

segurança e, quando caracterizada transferência internacional de dados pessoais, a Resolução CD/ANPD nº 19/2024;

c) atender às normas e políticas de proteção de dados de cada país onde haja qualquer tratamento de dados do Banco da Amazônia, incluindo os dados de seus clientes e colaboradores.

35.2 **Diretrizes para o Tratamento de Dados Pessoais**

35.2.1 **Da Relação de Controladoria e Operação**

a) O Banco da Amazônia será o Controlador dos Dados Pessoais, cabendo-lhe as decisões referentes ao tratamento.

b) A CONTRATADA atuará como Operadora, realizando o tratamento exclusivamente sob as instruções formais do Controlador e conforme as normas legais e contratuais aplicáveis, respondendo civil, administrativa e criminalmente por quaisquer danos decorrentes de descumprimento.

35.2.2 **Da Correção e Atualização**

a) A CONTRATADA deverá corrigir, completar, bloquear ou excluir Dados Pessoais sempre que solicitado pelo Banco da Amazônia, mediante comunicação formal.

35.2.3 **Das Solicitações de Titulares**

a) Qualquer solicitação ou reclamação de titular de Dados Pessoais recebida pela CONTRATADA deverá ser comunicada ao Banco da Amazônia em até 24 (vinte e quatro) horas, para tratamento adequado.

35.2.4 **Da Confidencialidade**

a) Todos os Dados Pessoais tratados em decorrência deste contrato são estritamente confidenciais, permanecendo sob sigilo mesmo após a rescisão contratual, independentemente da causa de extinção.

35.2.5 **Da Governança e Segurança da Informação**

a) A CONTRATADA deverá adotar medidas técnicas e organizacionais adequadas para garantir a confidencialidade, integridade, disponibilidade e resiliência dos Dados, utilizando tecnologias seguras e atualizadas conforme as melhores práticas de mercado.

35.2.6 **Das Medidas Técnicas e Organizacionais**

a) Devem ser implementadas medidas como pseudonimização, criptografia, controle de acesso, segregação de ambientes, registro de logs, backup seguro e gestão de vulnerabilidades, além de políticas e procedimentos de segurança da informação formalmente instituídos.

35.2.7 **Da Transmissão Segura**

a) Toda comunicação ou compartilhamento de Dados Pessoais deverá ocorrer por meio de canais criptografados e protocolos seguros de transmissão de dados, conforme padrões técnicos reconhecidos.

35.2.8 **Do Registro de Operações e Ambientes Seguros**

a) A CONTRATADA deverá manter registros detalhados das operações de tratamento, garantindo que seus ambientes físicos e lógicos estejam em conformidade com as

exigências de segurança, boas práticas e governança previstas na LGPD e nas normas complementares.

35.2.9 **Da Rastreabilidade**

a) Deverá ser mantido registro de todas as atividades realizadas nos sistemas que envolvam Dados Pessoais, permitindo identificar o responsável, o tipo de operação e o respectivo momento de execução.

35.2.10 **Do Monitoramento de Conformidade**

a) A CONTRATADA deverá monitorar periodicamente sua conformidade e a de seus empregados e subcontratados quanto às obrigações de proteção de dados, apresentando relatórios de controle e auditoria ao Banco da Amazônia sempre que solicitado.

b) Os relatórios deverão conter, no mínimo:

i) status dos sistemas e operações de tratamento;

ii) medidas e controles de segurança implantados;

iii) períodos de indisponibilidade ou falhas detectadas;

iv) conformidade com políticas e requisitos organizacionais;

v) incidentes ou violações de dados;

vi) ameaças e riscos identificados;

vii) planos de correção e melhorias aplicadas.

35.2.11 **Da Fiscalização**

a) O Banco da Amazônia poderá auditar, monitorar e fiscalizar, a qualquer tempo, o cumprimento das obrigações de proteção de dados, sem prejuízo da responsabilidade integral da CONTRATADA perante a lei e o contrato.

35.2.12 **Das Notificações**

a) A CONTRATADA deverá notificar o Banco da Amazônia em até 24 (vinte e quatro) horas após a identificação de qualquer:

i) violação, incidente ou suspeita de incidente de segurança;

ii) descumprimento legal ou contratual relativo à proteção de dados;

iii) exposição, vazamento ou ameaça à integridade dos Dados Pessoais;

iv) solicitação ou ordem de autoridade judicial ou administrativa que envolva dados do Banco.

35.2.13 **Da Cooperação**

a) A CONTRATADA deverá cooperar integralmente com o Banco da Amazônia:

i) na resposta a incidentes de segurança e comunicações à ANPD e aos titulares, conforme arts. 48 e 49 da LGPD;

ii) no atendimento às solicitações judiciais, administrativas e regulatórias;

iii) no cumprimento dos direitos dos titulares, prestando suporte técnico e operacional.

35.2.14 **Da Propriedade dos Dados**

a) Os Dados, metadados e quaisquer informações tratadas ou geradas em decorrência deste contrato são e permanecerão de propriedade exclusiva do Banco da Amazônia, sendo vedada sua utilização, compartilhamento, reprodução ou comercialização pela CONTRATADA.

35.2.15 **Do Tratamento Internacional**

a) Qualquer tratamento de Dados Pessoais fora do território nacional dependerá de autorização prévia e expressa do Banco da Amazônia, devendo observar o disposto nos arts. 33 a 36 da LGPD.

35.2.16 **Da Retenção e Eliminação**

a) A CONTRATADA não poderá armazenar ou reter Dados além do prazo legal ou contratual necessário. Ao término do contrato ou quando solicitado, deverá devolver integralmente os Dados e proceder à sua eliminação segura no prazo máximo de 30 (trinta) dias.

b) Caso os dados estejam em banco estruturado, a CONTRATADA deverá fornecer também o dicionário de dados e metadados, em até 10 (dez) dias, permitindo a plena compreensão e reuso das informações pela CONTRATANTE.

35.2.17 **Das Solicitações e Entregas de Dados**

a) Sempre que solicitada pelo Banco da Amazônia, a CONTRATADA deverá disponibilizar os Dados ou Registros solicitados em até 48 (quarenta e oito) horas, ou em prazo inferior, quando houver determinação judicial ou legal.

35.2.18 **Da Adequação Legislativa**

a) Eventuais alterações legais ou regulamentares que impactem a execução contratual deverão ser imediatamente comunicadas ao Banco da Amazônia.

b) Caso tais alterações inviabilizem a continuidade da execução nos moldes acordados, o Banco poderá rescindir o contrato sem ônus, mediante apuração proporcional dos valores devidos até a data da rescisão.

35.2.19 **Da Responsabilidade e Direito de Regresso**

a) A CONTRATADA será responsável, de forma ilimitada, por todos os danos diretos ou indiretos decorrentes de tratamento irregular de Dados Pessoais.

b) Fica assegurado ao Banco o direito de regresso integral contra a CONTRATADA, inclusive no caso de penalidades administrativas, civis ou judiciais impostas à CONTRATANTE por falhas, omissões ou atos ilícitos da CONTRATADA.

36 MATRIZ DE RISCO

36.1 Em atendimento ao disposto no artigo 42, §3º, da Lei nº 13.303/2016, e às boas práticas de gestão e governança aplicáveis às empresas públicas e sociedades de economia mista, fica consignado que esta contratação observará a Matriz de Riscos constante do Anexo X -deste Termo de Referência.

36.2 A Matriz de Riscos estabelece a repartição objetiva e equilibrada dos riscos entre o Banco da Amazônia e a CONTRATADA, especificando os eventos que poderão impactar o equilíbrio econômico-financeiro do contrato, bem como os mecanismos de mitigação e recomposição aplicáveis.

36.3 A Matriz de Riscos tem por finalidade:

a) identificar e classificar os riscos previsíveis relacionados à execução contratual;

b) definir a parte responsável pela gestão, mitigação e absorção de cada risco;

c) disciplinar as condições em que caberá a revisão contratual, reequilíbrio econômico-financeiro ou adoção de medidas corretivas; e

d) assegurar a transparência, a previsibilidade e a segurança jurídica na execução do contrato.

36.4 A Matriz de Riscos integra o presente Termo de Referência e o contrato que dele resultar, tendo força obrigatória entre as partes, devendo ser observada em todos os atos de gestão, execução e fiscalização contratual.

37 FORO

37.1 Fica eleito o Foro da Comarca de Belém, capital do Estado do Pará, com renúncia expressa a qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas, litígios ou controvérsias oriundas da interpretação ou execução desta contratação.

37.2 As partes reconhecem e concordam expressamente que a utilização de assinatura eletrônica, incluindo o uso de senhas pessoais, certificados digitais, biometria ou plataformas de assinatura eletrônica – como, por exemplo, a “DocuSign” – constitui forma legítima, válida e suficiente para:

a) comprovar a identidade dos signatários;

b) confirmar a autenticidade e integridade do documento; e

c) demonstrar a manifestação inequívoca de vontade para fins de celebração e execução do presente contrato, conforme o disposto na legislação aplicável, especialmente a Medida Provisória nº 2.200-2/2001, que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), e demais normas correlatas.

PREGÃO ELETRÔNICO N. 90029/2026
ANEXO I-A
ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO COMPLETA

1. DESCRIÇÃO GERAL

1.1 O presente Anexo tem por objetivo definir as especificações técnicas mínimas para a implementação dos Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, contemplando licenciamento, operação e suporte das soluções integradas de Segurança da Informação e Cibernética a serem contratadas pelo Banco da Amazônia, compreendendo:

a) SIEM (Security Information and Event Management): Gerenciamento centralizado de informações e eventos de segurança;

b) GVUL (Gestão de Vulnerabilidades): Identificação, priorização e tratamento contínuo de vulnerabilidades;

c) XDR (Extended Detection and Response) baseado em SIEM: Correlação avançada de eventos e resposta automatizada a incidentes.

1.2 As soluções e serviços deverão operar de forma integrada e orquestrada, assegurando monitoramento contínuo (24x7x365), resposta tempestiva a incidentes, tratamento de vulnerabilidades, detecção avançada de ameaças e suporte especializado, conforme os requisitos descritos neste Anexo.

1.3 As soluções deverão observar as diretrizes técnicas, os padrões de interoperabilidade e as tecnologias estabelecidas pelo Banco da Amazônia, assegurando plena compatibilidade com o ecossistema tecnológico institucional, que contempla arquitetura de microsserviços, containers e APIs REST em ambiente Red Hat OpenShift Container Platform.

1.4 As soluções hospedadas em nuvem deverão integrar-se às ferramentas de observabilidade, métricas e logs corporativos (tais como Prometheus, Grafana, Elastic Search e equivalentes), garantindo interoperabilidade com o ambiente tecnológico do Banco, sendo obrigatória a compatibilidade com o ambiente Red Hat OpenShift Container Platform, incluindo o suporte a agentes ou APIs nativas para coleta e correlação de dados em clusters.

2. ESCOPO TÉCNICO E SOLUÇÕES INTEGRADAS

2.1 Como parte integrante do escopo técnico do Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center, deverá ser considerada a implementação, o licenciamento e a operação contínua e integrada das soluções integradas de SIEM, GVUL e XDR, bem como a prestação dos serviços correlatos de monitoramento, resposta, consultoria técnica e capacitação, conforme descrito a seguir:

componentes	Descrição	Unidade	Quantidade

1	Serviços gerenciados de Monitoramento e Resposta a Incidentes (SIEM), Gestão de Vulnerabilidades (GVUL), Detecção e Resposta Estendida (XDR) e de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), em regime contínuo (24x7x365)	Mês	60
2	Solução de SIEM (Security Information and Event Management) para gerenciamento centralizado de informações e eventos de segurança	GB/dia	600
3	Solução de GVUL (Gestão de Vulnerabilidades) para detecção, priorização e tratamento contínuo de vulnerabilidades	Ativo monitorado/mês	5.000/mês
4	Solução de XDR (Extended Detection and Response) baseado em SIEM para correlação avançada de eventos e resposta automatizada a incidentes	Endpoint protegido/mês	5.000/mês

2.2 Os Serviços Gerenciados de Monitoramento e Resposta a Incidentes (SIEM), Gestão de Vulnerabilidades (GVUL), Detecção e Resposta Estendida (XDR baseada em SIEM) e de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), deverão ser prestados em regime contínuo (24x7x365), pelo período de 60 (sessenta) meses, assegurando operação ininterrupta, acompanhamento proativo, correlação de alertas, emissão de relatórios técnicos e mitigação tempestiva de incidentes.

2.3 O Serviço de SOC, no modelo de Cyber Fusion Center, será responsável por monitorar continuamente o ambiente tecnológico do Banco da Amazônia, detectar ameaças, responder a incidentes, apoiar ações de mitigação de riscos cibernéticos e garantir a integração operacional entre as soluções contratadas.

2.3.1 Solução de SIEM (Security Information and Event Management):

a) Responsável pelo gerenciamento centralizado de informações e eventos de segurança, com ingestão, correlação e análise de logs em tempo real, permitindo a detecção precoce de ameaças e o apoio à resposta a incidentes.

b) O licenciamento da Solução de SIEM deverá contemplar o processamento de, no mínimo, 600 GB/dia de logs e eventos, abrangendo todas as fontes de dados corporativos – infraestrutura, servidores, aplicações, endpoints, dispositivos de segurança, serviços em nuvem e sistemas de negócio críticos – assegurando armazenamento dos logs por período mínimo de 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), garantindo integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória.

c) A Solução de SIEM deverá operar de forma integrada ao SOC e à camada de resposta (XDR), incorporando mecanismos de detecção comportamental (UEBA), correlação entre múltiplas fontes e geração automatizada de alertas priorizados por severidade.

2.3.2 Solução de GVUL (Gestão de Vulnerabilidades):

a) Destinada à detecção, priorização e tratamento contínuo de vulnerabilidades, com mecanismos automatizados de varredura, análise de risco, classificação de criticidade e emissão de relatórios técnicos consolidados.

b) O licenciamento da Solução de GVUL deverá abranger, no mínimo, 5.000 (cinco mil) ativos monitorados por mês, incluindo servidores físicos e virtuais, estações de trabalho, equipamentos de rede, appliances de segurança e ativos em ambiente de nuvem sob responsabilidade do Banco da Amazônia.

c) O Serviço de GVUL deverá compreender o ciclo completo de gestão de vulnerabilidades, incluindo identificação, análise, priorização e acompanhamento das ações corretivas até sua resolução, promovendo o tratamento contínuo e a mitigação tempestiva de riscos cibernéticos.

d) O provedor de GVUL deverá dispor de plataforma dedicada e de acesso seguro via web, que possibilite a visualização dos resultados, priorização de riscos, acompanhamento das ações corretivas e geração de painéis executivos e técnicos para gestão do processo.

e) As varreduras de vulnerabilidade deverão ser compatíveis e incluir ambientes containerizados, pipelines CI/CD e imagens Docker executadas no OpenShift Container Platform, bem como suportar integração com o Cofre de Senhas corporativo (BeyoundTrust) e com bancos Oracle 19c RAC.

f) O quantitativo de 5.000 (cinco mil) ativos monitorados por mês foi definido com base na estimativa atual e projetada do parque tecnológico do Banco da Amazônia, considerando aproximadamente 2.000 (dois mil) servidores físicos e virtuais e 3.000 (três mil) estações de trabalho corporativas, além de equipamentos de rede, appliances de segurança, dispositivos de infraestrutura e recursos hospedados em ambiente de nuvem.

g) A adoção desse volume visa garantir a cobertura integral da superfície de ataque da instituição, assegurando que todos os ativos críticos, endpoints e componentes de rede estejam contemplados nas rotinas automatizadas de varredura, análise e tratamento de vulnerabilidades, em conformidade com as boas práticas de segurança cibernética e de gestão de riscos tecnológicos.

h) O quantitativo proposto contempla margem de crescimento orgânico durante a vigência contratual de 60 (sessenta) meses, de modo a evitar a necessidade de aditivos contratuais decorrentes de expansões futuras do parque computacional.

2.3.3 Solução de XDR (Extended Detection and Response):

a) Voltada à correlação avançada de eventos e resposta automatizada a incidentes de segurança, correlacionando informações provenientes de múltiplas camadas do ambiente tecnológico – incluindo endpoints, redes, aplicações, identidades e nuvem – e promovendo integração nativa com o SIEM e o SOC.

b) A solução de XDR deverá ser compatível e abranger workloads e containers executados em OpenShift, correlacionando eventos provenientes de aplicações distribuídas, Bancos de Dados Oracle RAC e APIs REST, dispondo de conectores compatíveis com os middlewares institucionais (Red Hat Fuse, AMQ, JBoss EAP) e possibilitar integração com os serviços de observabilidade do Banco.

c) A solução de XDR deverá dispor de Monitoramento de Identidades (IDR), integrado à própria solução, abrangendo a análise de credenciais, autenticações e privilégios, com correlação de eventos de identidade e foco na detecção de acessos indevidos, elevação de privilégios e movimentações laterais anômalas.

d) O escopo de monitoramento deverá contemplar, pelo menos, 5.000 (cinco mil) credenciais ativas do Active Directory (AD) do Banco da Amazônia, assegurando

visibilidade completa dos acessos, detecção de comportamentos anômalos e correlação com os eventos de segurança registrados pelo SIEM e pelo XDR, em conformidade com as boas práticas de segurança cibernética.

e) O licenciamento da Solução de XDR deverá cobrir, no mínimo, 5.000 (cinco mil) endpoints protegidos por mês, com funcionalidades de detecção comportamental, isolamento, contenção e remediação de ameaças, atuando de forma integrada ao ecossistema de monitoramento e resposta do Banco.

f) O quantitativo de 5.000 (cinco mil) endpoints protegidos por mês foi estabelecido considerando a quantidade total estimada de estações de trabalho, notebooks e servidores corporativos do Banco da Amazônia, abrangendo aproximadamente 3.000 (três mil) estações de trabalho e notebooks e 2.000 (dois mil) servidores físicos e virtuais distribuídos entre a matriz e as unidades regionais.

g) A definição desse volume tem como objetivo assegurar a cobertura completa de todos os ativos computacionais efetivamente conectados à rede corporativa, bem como dos ativos móveis e ambientes híbridos ou em nuvem, garantindo visibilidade, correlação e resposta automatizada a incidentes em todas as camadas do ambiente tecnológico.

h) O dimensionamento proposto também considera a integração nativa da Solução de XDR com o SIEM e o SOC, permitindo que todos os endpoints licenciados sejam monitorados de forma contínua e participem dos fluxos de detecção comportamental, contenção, isolamento e remediação automática de ameaças.

i) O quantitativo de 5.000 (cinco mil) endpoints contempla margem de crescimento projetada para os 60 (sessenta) meses de vigência contratual, levando em conta possíveis expansões de parque, substituições tecnológicas e adoção gradual de novos serviços digitais.

I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SIEM

1. DESCRIÇÃO

1.1 A Solução de SIEM (Security Information and Event Management) será responsável pelo gerenciamento centralizado de informações e eventos de segurança, com ingestão, correlação e análise de logs em tempo real, permitindo a detecção precoce de ameaças e o apoio à resposta a incidentes.

1.2 O licenciamento da Solução deverá contemplar o processamento de, no mínimo, 600 GB/dia de logs e eventos, abrangendo todas as fontes de dados corporativos – infraestrutura, servidores, aplicações, endpoints, dispositivos de segurança, serviços em nuvem e sistemas de negócio críticos – e assegurando armazenamento dos logs por período mínimo de 12 (doze) meses em camada de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), garantindo integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória.

1.3 A Solução deverá operar de forma integrada ao SOC e à camada de resposta (XDR), incorporando mecanismos de detecção comportamental (UEBA), correlação entre múltiplas fontes e geração automatizada de alertas priorizados por severidade.

2. REQUISITOS GERAIS

2.1 A Solução deverá ser fornecida integralmente no modelo Software como Serviço (SaaS), em arquitetura cloud native e multi-tenant, operada diretamente pelo fabricante ou parceiro

autorizado, garantindo suporte técnico contínuo, atualizações automáticas e conformidade com as políticas de segurança do Banco da Amazônia durante toda a vigência contratual.

2.2 A Solução deverá contar com suporte técnico contínuo, atualizações automáticas de versão e correções, sem necessidade de intervenção do Banco, garantindo conformidade com as políticas de segurança da informação do Banco da Amazônia durante toda a vigência contratual.

2.3 O licenciamento da Solução de SIEM deverá ser contratado diretamente em nome do Banco da Amazônia, sendo fornecida na última versão estável disponível no momento da contratação e abrangendo todos os módulos, conectores, APIs, componentes técnicos e funcionalidades indispensáveis ao pleno funcionamento da Solução, sem custos adicionais, incluindo:

a) garantia, manutenção corretiva e evolutiva;

b) suporte técnico multilíngue (português e inglês) 24×7×365;

c) atualizações automáticas de versões, correções de segurança e melhorias funcionais;

d) direito de uso integral e contínuo durante todo o período contratual;

e) vedação ao uso de softwares ou componentes open-source genéricos ou soluções experimentais não suportadas oficialmente pelo fabricante.

2.4 O serviço de suporte técnico deverá assegurar ao Banco:

a) aplicação contínua e automática de atualizações e melhorias na solução, inclusive correções de segurança e incrementos funcionais;

b) correção de falhas identificadas e reportadas, priorizando estabilidade e integridade dos dados;

c) acesso irrestrito à base de conhecimento, documentação técnica e notas de versão do fabricante;

d) Service Desk multilíngue (português e inglês) 24×7×365, acessível por portal web, e-mail e telefone;

e) suporte técnico especializado fornecido diretamente pelo fabricante.

2.5 A Solução deverá garantir:

a) confidencialidade, integridade e autenticidade dos dados, registros e resultados das varreduras;

b) segregação lógica entre o ambiente do Banco da Amazônia e os demais clientes da plataforma, com controle de acesso por credenciais individuais e autenticação multifator (MFA);

c) conformidade com a Lei nº 13.709/2018 (LGPD) e aderência às normas ISO/IEC 27001, 27002, 27017 e 27018;

d) trilhas de auditoria imutáveis de todas as ações executadas na plataforma, com retenção mínima de 12 (doze) meses em camada de armazenamento de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), assegurando integridade, rastreabilidade, disponibilidade e consulta sob controle direto do Banco, inclusive para fins de auditoria, investigação forense e conformidade regulatória;

e) integração nativa com o Active Directory para autenticação multifator (MFA) e controle de perfis de acesso;

f) disponibilidade 24×7×365, assegurada por infraestrutura redundante em nuvem e geograficamente distribuída, garantindo continuidade e resiliência operacional.

2.6 A Solução deverá implementar controle de acesso baseado em papéis (RBAC), usuários e funções, permitindo atribuição de privilégios conforme perfil e área de atuação.

2.7 O acesso ao ambiente deverá ocorrer exclusivamente por navegador web compatível com HTML5, mediante protocolo HTTPS/TLS 1.2 ou superior, sendo vedado o uso de componentes locais ou protocolos obsoletos.

2.8 A Solução deverá ser plenamente compatível, no mínimo, com os navegadores Google Chrome (v. 110+), Microsoft Edge (v. 110+) e Mozilla Firefox (v. 100+), executados em sistemas operacionais Windows 10 ou superior.

2.9 O protocolo HTTPS deverá utilizar TLS 1.2 ou superior, sendo recomendável suporte à versão 1.3, vedada a utilização de versões obsoletas ou inseguras.

2.10 A Solução deverá permitir integração direta com o ServiceNow (módulo SIR) e com o sistema de Governança, Risco e Conformidade (GRC) do Banco da Amazônia para registro, acompanhamento e fechamento de incidentes e relatórios de auditoria.

3. ARQUITETURA E COMPONENTES ESSENCIAIS

3.1 A Solução deverá ser capaz de coletar, normalizar e correlacionar eventos de segurança provenientes de múltiplas fontes (infraestrutura, aplicações, endpoints, identidades e transações), detectando atividades anômalas e fraudes eletrônicas.

3.2 A Solução deverá ser capaz de coletar, interpretar, normalizar e correlacionar eventos oriundos de logs técnicos, operacionais e transacionais, independentemente da origem ou fabricante, garantindo detecção de atividades anômalas, ameaças cibernéticas e fraudes eletrônicas.

3.3 A arquitetura mínima deverá contemplar:

a) Console Web Unificado para administração, monitoramento e investigação;

b) Mecanismo de Coleta compatível com Syslog, APIs, conectores cloud, CSV/JSON etc.;

c) Motor de Correlação capaz de aplicar regras customizadas e detecção avançada de ameaças (YARA-L ou linguagem equivalente);

d) Armazenamento e Indexação em Nuvem, com busca em larga escala e retenção mínima de 12 (doze) meses em camada de armazenamento de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), assegurando a integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória;

e) Módulo UEBA (User and Entity Behavior Analytics) integrado nativamente;

f) Módulo SOAR (Security Orchestration, Automation and Response) para automação de respostas.

3.4 Todos os componentes deverão operar de forma nativamente integrada, sem necessidade de customizações específicas, em infraestrutura redundante geograficamente segregada,

constituindo um ambiente unificado de monitoração, análise, investigação, inteligência e resposta a incidentes.

4. CAPACIDADE OPERACIONAL E RETENÇÃO

4.1. A Solução deverá ingerir e processar, de forma contínua e sustentada, mínimo de 600 GB/dia de eventos de segurança.

4.2. A infraestrutura deverá escalar automaticamente conforme o volume de dados, sem perda de eventos ou necessidade de intervenção manual.

4.3. A Solução deverá processar volumes superiores à média diária contratada em situações de pico temporário, sem descartar eventos nem impor bloqueios ao recebimento de logs, restabelecendo o fluxo normal sem intervenção manual ou custo adicional.

4.4. Todos os logs deverão permanecer imutáveis por 12 meses, em armazenamento de acesso imediato (“logs quentes”), com opção posterior de arquivamento (“cold storage”) ou exportação, mantendo consulta sob controle direto do Banco para fins de auditoria e investigação.

4.5. A Solução deverá disponibilizar painel de status ou meio equivalente que permita ao Banco acompanhar a disponibilidade do serviço em tempo real.

4.6. A Solução deverá manter desempenho estável e não impactar o funcionamento dos sistemas do Banco, mesmo durante picos prolongados de envio de logs.

4.7. Todas as comunicações entre sensores, conectores e A Solução SIEM deverão ocorrer mediante criptografia TLS 1.2+, garantindo confidencialidade e integridade.

5. CORRELAÇÃO, ANÁLISE E DETECÇÃO

5.1. A Solução deverá normalizar eventos e aplicar técnicas de correlação temporal, espacial, de conteúdo e comportamental.

5.2. As técnicas deverão permitir análises temporais, espaciais, de conteúdo e de comportamento anômalo, correlacionando eventos provenientes de múltiplas fontes para identificar incidentes de segurança de forma contextual.

5.3. A Solução deverá detectar ameaças conhecidas e desconhecidas por meio de:

a) assinaturas e regras de detecção;

b) análise de anomalias;

c) aprendizado de máquina (machine learning).

5.4. A Solução deverá oferecer ferramentas avançadas de investigação, permitindo busca, visualização cronológica e análise detalhada de incidentes.

5.5. Todas as novas regras de detecção e correlação deverão ser submetidas à homologação formal e validação técnica do Banco da Amazônia antes de ativação em ambiente produtivo.

5.6. A Solução deverá disponibilizar recursos de visualização cronológica (timeline), busca parametrizada e análise contextual de eventos, possibilitando identificação de causas e impactos de incidentes.

6. ENRIQUECIMENTO E CLASSIFICAÇÃO DE EVENTOS

6.1. Deverá ser possível classificar eventos por zonas lógicas, unidades organizacionais e atributos personalizados.

6.2. A coleta abrangerá dispositivos de segurança, rede, servidores Windows/Linux, bancos de dados, aplicações e serviços em nuvem.

6.3. A Solução deverá exportar logs brutos ou normalizados em CSV, JSON, XML ou PDF.

6.4. Todos os eventos deverão ser automaticamente enriquecidos com informações geográficas e feeds de inteligência de ameaças.

7. THREAT INTELLIGENCE

7.1. A plataforma deverá possuir feeds nativos de Threat Intelligence mantidos pelo fabricante, cobrindo IPs, domínios, hashes e campanhas APT.

7.2. Deverá permitir integração via API com fontes externas (MISP, VirusTotal, Anomali etc.) e correlação automática dos IOCs com os eventos coletados.

7.3. A gestão dos feeds deverá ser centralizada, permitindo ativar, desativar ou priorizar fontes conforme estratégia do Banco.

7.4. A Solução deverá permitir consulta manual e importação de IOCs (IPs, domínios, hashes, URLs) para criação de regras específicas e casos de uso, possibilitando investigações contextuais e personalizadas.

7.5. A gestão dos feeds de Threat Intelligence, internos ou externos, deverá ser centralizada, permitindo ativar, desativar ou priorizar fontes conforme a estratégia do Banco.

8. RELATÓRIOS E DASHBOARDS

8.1. A Solução deverá gerar relatórios técnicos e executivos com:

a) eventos coletados e incidentes detectados;

b) tendências e padrões comportamentais;

c) níveis de conformidade e auditoria.

8.2. Todos os relatórios deverão ser acessíveis via web e exportáveis em PDF e CSV, com personalização por usuário.

9. INTELIGÊNCIA ARTIFICIAL E UEBA

9.1. A Solução deverá empregar IA Generativa com Processamento de Linguagem Natural (PLN) para:

a) consultas em linguagem natural;

b) explicação de incidentes;

c) geração de relatórios assistidos;

d) sugestão de novas regras de detecção;

e) triagem automática de alertas apontando o resultado como falso positivo, verdadeiro positivo ou inconclusivo com o auxílio de IA.

9.2. A funcionalidade de IA Generativa deverá ser nativa ou oficialmente integrada pelo fabricante, sem necessidade de licenciamento adicional.

9.3. A Solução deverá apoiar a criação de novas regras de detecção, hipóteses investigativas e relatórios técnicos, por meio de interação em linguagem natural.

9.4. O módulo UEBA deverá analisar padrões de login, acessos, movimentações de rede e comportamento de entidades, detectando ameaças internas ou anomalias.

10. SEGURANÇA E CONFORMIDADE

10.1. A Solução deverá manter trilha de auditoria completa, compatível com as normas ISO/IEC 27001 e 27002.

10.2. A Solução deverá possuir mecanismos de segregação, anonimização e rastreabilidade de dados pessoais, em conformidade com a LGPD.

10.3. O Banco da Amazônia deverá ter acesso a todas as trilhas, relatórios e logs de auditoria, inclusive para fins de auditoria interna e regulatória.

10.4. A Solução deverá registrar todas as ações dos usuários – acessos, pesquisas, exportações e alterações de configuração – em trilhas de auditoria completas, imutáveis e rastreáveis, disponíveis para auditoria interna e externa.

11. SUPORTE TÉCNICO E GOVERNANÇA

11.1. A Solução deverá manter canal de suporte 24×7×365 em português, por portal web, e-mail e telefone.

11.2. Deverá garantir níveis mínimos de serviço (NMS) conforme Anexo I-B – Níveis Mínimos de Serviço.

11.3. A governança técnica compreenderá reuniões mensais com a área de Segurança da Informação do Banco para validação de indicadores, regras de detecção e melhorias contínuas.

11.4. As reuniões mensais deverão incluir a homologação de novas regras de detecção, ajustes de casos de uso e acompanhamento dos indicadores de desempenho definidos no Anexo I-B – NMS.

II – ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE GVUL

1. DESCRIÇÃO

1.1 A Solução de GVUL (Gestão de Vulnerabilidades) será destinada à detecção, priorização e tratamento contínuo de vulnerabilidades, com mecanismos automatizados de varredura, análise de risco, classificação de criticidade e emissão de relatórios técnicos consolidados.

1.2 O licenciamento da Solução deverá abranger, no mínimo, 5.000 ativos monitorados por mês, incluindo servidores físicos e virtuais, estações de trabalho, equipamentos de rede, appliances de segurança e ativos em ambiente de nuvem sob responsabilidade do Banco da Amazônia.

1.3 O Serviço de GVUL deverá compreender o ciclo completo de gestão de vulnerabilidades, incluindo identificação, análise, priorização e acompanhamento das ações corretivas até sua resolução.

1.4 O provedor deverá dispor de plataforma dedicada e de acesso seguro via web, que possibilite a visualização dos resultados, priorização de riscos, acompanhamento das ações corretivas e geração de painéis executivos e técnicos.

2. REQUISITOS GERAIS

2.1. A Solução deverá ser fornecida integralmente no modelo Software como Serviço (SaaS), em ambiente cloud native, operado diretamente pelo fabricante ou parceiro autorizado, garantindo suporte técnico contínuo, atualizações automáticas e conformidade com as políticas de segurança do Banco da Amazônia durante toda a vigência contratual.

2.2. A Solução deverá contar com suporte técnico contínuo, atualizações automáticas de versão e correções, sem necessidade de intervenção do Banco, garantindo conformidade com as políticas de segurança da informação do Banco da Amazônia durante toda a vigência contratual.

2.3. O licenciamento da Solução de GVUL deverá ser contratado diretamente em nome do Banco da Amazônia, sendo fornecida na última versão estável disponível no momento da contratação e abrangendo todos os módulos, conectores, APIs, componentes técnicos e funcionalidades indispensáveis ao pleno funcionamento da Solução, sem custos adicionais, incluindo:

a) garantia, manutenção corretiva e evolutiva;

b) suporte técnico multilíngue (português e inglês) 24×7×365;

c) atualizações automáticas de versões, correções de segurança e melhorias funcionais;

d) direito de uso integral e contínuo durante todo o período contratual;

e) vedação ao uso de softwares ou componentes open-source genéricos ou soluções experimentais não suportadas oficialmente pelo fabricante.

2.4. O serviço de suporte técnico deverá assegurar ao Banco:

a) aplicação contínua e automática de atualizações e melhorias na solução, inclusive correções de segurança e incrementos funcionais;

b) correção de falhas identificadas e reportadas, priorizando estabilidade e integridade dos dados;

c) acesso irrestrito à base de conhecimento, documentação técnica e notas de versão do fabricante;

d) Service Desk multilíngue (português e inglês) 24×7×365, acessível por portal web, e-mail e telefone;

e) suporte técnico especializado fornecido diretamente pelo fabricante.

2.5. A Solução deverá garantir:

a) confidencialidade, integridade e autenticidade dos dados, registros e resultados das varreduras;

b) segregação lógica entre o ambiente do Banco da Amazônia e os demais clientes da plataforma, com controle de acesso por credenciais individuais e autenticação multifator (MFA);

c) conformidade com a Lei nº 13.709/2018 (LGPD) e aderência às normas ISO/IEC 27001, 27002, 27017 e 27018;

d) trilhas de auditoria imutáveis de todas as ações executadas na plataforma, com retenção mínima de 12 (doze) meses em camada de armazenamento de consulta imediata ("logs quentes") e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro ("cold storage"), assegurando integridade, rastreabilidade, disponibilidade e consulta sob controle direto do Banco, inclusive para fins de auditoria, investigação forense e conformidade regulatória;

e) integração nativa com o Active Directory para autenticação multifator (MFA) e controle de perfis de acesso;

f) disponibilidade 24×7×365, assegurada por infraestrutura redundante em nuvem e geograficamente distribuída, garantindo continuidade e resiliência operacional.

2.6. A Solução deverá implementar controle de acesso baseado em papéis (RBAC), usuários e funções, permitindo atribuição de privilégios conforme perfil e área de atuação.

2.7. O acesso ao ambiente deverá ocorrer exclusivamente por navegador web compatível com HTML5, mediante protocolo HTTPS/TLS 1.2 ou superior, sendo vedado o uso de componentes locais ou protocolos obsoletos.

2.8. A Solução deverá ser plenamente compatível, no mínimo, com os navegadores Google Chrome (v. 110+), Microsoft Edge (v. 110+) e Mozilla Firefox (v. 100+), executados em sistemas operacionais Windows 10 ou superior.

2.9. O protocolo HTTPS deverá utilizar TLS 1.2 ou superior, sendo recomendável suporte à versão 1.3, vedada a utilização de versões obsoletas ou inseguras.

2.10. A Solução deverá permitir integração direta com o ServiceNow (módulo SIR) e com o sistema de Governança, Risco e Conformidade (GRC) do Banco da Amazônia para registro, acompanhamento e fechamento de incidentes e relatórios de auditoria.

3. ARQUITETURA E ESCOPO FUNCIONAL

3.1. A Solução deverá identificar, analisar, classificar, priorizar e acompanhar o ciclo de tratamento de vulnerabilidades em todos os ativos tecnológicos do Banco da Amazônia – servidores, estações, dispositivos de rede, aplicações, bancos de dados, sistemas operacionais e serviços em nuvem.

3.2. A Solução deverá operar de forma automática e contínua, com mecanismos de descoberta de ativos, varredura autenticada e não autenticada, detecção de falhas conhecidas (CVEs) e exposição a riscos, integrando-se ao SOC e ao XDR para correlação de eventos.

3.3. A Solução deverá ser fornecida plataforma web segura, com autenticação SSO via Active Directory e MFA, permitindo aos usuários designados:

a) visualizar resultados de varreduras;

b) classificar vulnerabilidades por severidade (CVSS, CWE, NVD);

c) monitorar ativos e níveis de exposição;

d) gerar relatórios e dashboards em tempo real;

e) acompanhar o tratamento e fechamento das vulnerabilidades.

4. FUNCIONALIDADES MÍNIMAS

4.1. A Solução deverá contemplar:

a) Descoberta Automática de Ativos por meio de scans de rede e integrações com inventários corporativos;

b) Varreduras Internas e Externas com periodicidade mínima semanal, podendo ser intensificadas conforme necessidade ou política do Banco;

c) Classificação Automática por Risco e Criticidade baseada em impacto, exploitabilidade e exposição;

d) Correlação de Riscos com ativos e priorização automática de correção;

e) Relatórios Técnicos e Gerenciais, incluindo tendências e métricas de tratamento;

f) Integração com SIEM e XDR para enriquecimento de eventos de segurança e acionamento automático de alertas correlacionados.

4.2. A Solução deverá gerar alertas automáticos para vulnerabilidades críticas com exploit ativo ou uso em campanhas APT, permitindo resposta imediata.

4.3. Os resultados deverão ser armazenados por no mínimo de 12 (doze) meses em camada de armazenamento de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, assegurando a integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória, com opção de exportação em CSV, JSON ou PDF.

5. PROCESSO DE GESTÃO DE VULNERABILIDADES

5.1. A Solução deverá executar as seguintes etapas automatizadas.

a) Descoberta de Ativos: mapeamento completo e dinâmico do ambiente de TI;

b) Varredura e Identificação: análise contínua autenticada e não autenticada;

c) Classificação e Prioridade: avaliação de risco baseada em contexto e impacto;

d) Correção e Mitigação: encaminhamento automático das falhas para as áreas responsáveis;

e) Validação e Verificação: reteste após correção;

f) Relatórios e Indicadores: emissão de relatórios técnicos e executivos.

5.2. A Solução deverá manter histórico completo do ciclo de vida de cada vulnerabilidade detectada, incluindo data de descoberta, responsável, status de tratamento, data de correção e resultado de validação.

5.3. Todos os processos deverão ser compatíveis com as melhores práticas de mercado (ISO/IEC 27002, NIST SP 800-40, CIS Controls).

5.4. O Banco da Amazônia deverá possuir acesso direto e integral à base de dados e trilhas de auditoria da solução, incluindo evidências de varreduras e histórico de tratamento, para fins de fiscalização, conformidade e auditoria.

6. INTEGRAÇÃO E CORRELAÇÃO

6.1. A Solução deverá integrar-se ao SIEM e ao XDR para permitir a correlação de vulnerabilidades com eventos de segurança e incidentes em andamento.

6.2. A integração deverá suportar APIs rest ou conectores nativos, permitindo sincronização de dados e alertas em tempo real.

6.3. Os dados correlacionados deverão ser armazenados de modo centralizado e acessíveis pelo SOC para análises e investigações, mantendo a correlação e acionamento de alertas automáticos entre SOC e GVUL.

7. RELATÓRIOS E INDICADORES

7.1. A Solução deverá fornecer relatórios mensais contendo:

a) listagem de vulnerabilidades por criticidade;

b) tendências de exposição ao longo do tempo;

c) indicadores de tratamento (MTTR, percentual corrigido e nível de risco residual);

d) vulnerabilidades reincidentes ou não tratadas;

e) recomendações técnicas de mitigação.

7.2. Relatórios e dashboards deverão ser personalizáveis e exportáveis em PDF ou CSV.

7.3. Todos os dados deverão estar disponíveis em língua portuguesa e armazenados em ambiente seguro na nuvem.

8. INTELIGÊNCIA DE AMEAÇAS E PRIORIZAÇÃO

8.1. A Solução deverá incorporar mecanismos de Threat Intelligence para identificar vulnerabilidades ativas exploradas em ataques reais, ajustando automaticamente a prioridade de tratamento.

8.2. Deverá ser possível cruzar informações de vulnerabilidades com indicadores de ameaças (IoCs) provenientes de bases como MISP ou VirusTotal.

9. CONFORMIDADE E SEGURANÇA

9.1. A Solução deverá estar em conformidade com as normas ISO/IEC 27001 e LGPD, assegurando tratamento adequado de dados sensíveis.

9.2. Os registros de acesso e operações deverão ser auditáveis e armazenados por no mínimo de 12 meses 12 (doze) meses em camada de armazenamento de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, assegurando a integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória.

9.3. A Solução deverá permitir a análise forense das atividades realizadas em caso de auditoria ou investigação.

10. SUPORTE E GOVERNANÇA

10.1. A Solução deverá dispor de suporte técnico 24×7×365 em português, via portal web, e-mail ou telefone.

19.2. Os níveis mínimos de serviço (NMS) serão os definidos no Anexo I-B – Níveis Mínimos de Serviço.

10.3. Deverão ocorrer reuniões mensais de governança técnica com a área de Segurança da Informação para validação de indicadores, análise de tendências e melhoria contínua dos processos.

11. RETENÇÃO, LICENCIAMENTO E ATUALIZAÇÕES

11.1. Os dados de vulnerabilidades identificados deverão ser mantidos armazenados por no mínimo 12 (doze) meses em camada de armazenamento de consulta imediata e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro, assegurando a integridade, rastreabilidade e disponibilidade para fins de auditoria, investigação forense e conformidade regulatória, com possibilidade de exportação e auditoria a qualquer tempo.

11.2. O licenciamento da Solução deverá incluir todas as ferramentas de scanning, dashboards, mecanismos de priorização e integrações necessárias para seu pleno funcionamento.

11.3. As atualizações de base de vulnerabilidades e plugins de varredura deverão ocorrer automaticamente, sem intervenção manual ou custo adicional para o Banco da Amazônia.

11.4. O fabricante da Solução deverá assegurar o suporte oficial e a manutenção contínua do produto durante toda a vigência contratual.

III - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE XDR

1. DESCRIÇÃO

1.1 Solução de XDR (Extended Detection and Response) será voltada à correlação avançada de eventos e à resposta automatizada a incidentes de segurança, correlacionando informações provenientes de múltiplas camadas do ambiente tecnológico – incluindo endpoints, redes, aplicações, identidades e nuvem.

1.2 O licenciamento da Solução deverá cobrir, no mínimo, 5.000 (cinco mil) endpoints protegidos por mês, com funcionalidades de detecção comportamental, isolamento, contenção e remediação automatizada de ameaças.

1.3 A Solução deverá operar integrada ao SIEM e ao SOC, possibilitando correlação inteligente de eventos, priorização automatizada de alertas e execução de ações orquestradas de resposta, visando reduzir o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR) a incidentes.

2. REQUISITOS GERAIS

2.1. A Solução deverá ser fornecida integralmente no modelo Software como Serviço (SaaS), em ambiente cloud native, operado diretamente pelo fabricante ou parceiro

autorizado, garantindo suporte técnico contínuo, atualizações automáticas e conformidade com as políticas de segurança do Banco da Amazônia durante toda a vigência contratual.

2.2. A Solução deverá contar com suporte técnico contínuo, atualizações automáticas de versão e correções, sem necessidade de intervenção do Banco, garantindo conformidade com as políticas de segurança da informação do Banco da Amazônia durante toda a vigência contratual.

2.3. O licenciamento da Solução de XDR deverá ser contratado diretamente em nome do Banco da Amazônia, sendo fornecida na última versão estável disponível no momento da contratação e abrangendo todos os módulos, conectores, APIs, componentes técnicos e funcionalidades indispensáveis ao pleno funcionamento da Solução, sem custos adicionais, incluindo:

a) garantia, manutenção corretiva e evolutiva;

b) suporte técnico multilíngue (português e inglês) 24×7×365;

c) atualizações automáticas de versões, correções de segurança e melhorias funcionais;

d) direito de uso integral e contínuo durante todo o período contratual;

e) vedação ao uso de softwares ou componentes open-source genéricos ou soluções experimentais não suportadas oficialmente pelo fabricante.

2.4. O serviço de suporte técnico deverá assegurar ao Banco:

a) aplicação contínua e automática de atualizações e melhorias na solução, inclusive correções de segurança e incrementos funcionais;

b) correção de falhas identificadas e reportadas, priorizando estabilidade e integridade dos dados;

c) acesso irrestrito à base de conhecimento, documentação técnica e notas de versão do fabricante;

d) Service Desk multilíngue (português e inglês) 24×7×365, acessível por portal web, e-mail e telefone;

e) suporte técnico especializado fornecido diretamente pelo fabricante.

2.5. A Solução deverá garantir:

a) confidencialidade, integridade e autenticidade dos dados, registros e resultados das varreduras;

b) segregação lógica entre o ambiente do Banco da Amazônia e os demais clientes da plataforma, com controle de acesso por credenciais individuais e autenticação multifator (MFA);

c) conformidade com a Lei nº 13.709/2018 (LGPD) e aderência às normas ISO/IEC 27001, 27002, 27017 e 27018;

d) trilhas de auditoria imutáveis de todas as ações executadas na plataforma, com retenção mínima de 12 (doze) meses em camada de armazenamento de consulta imediata (“logs quentes”) e 48 (quarenta e oito) meses adicionais em camada de arquivamento seguro (“cold storage”), assegurando integridade, rastreabilidade, disponibilidade e consulta

sob controle direto do Banco, inclusive para fins de auditoria, investigação forense e conformidade regulatória;

e) integração nativa com o Active Directory para autenticação multifator (MFA) e controle de perfis de acesso;

f) disponibilidade 24×7×365, assegurada por infraestrutura redundante em nuvem e geograficamente distribuída, garantindo continuidade e resiliência operacional.

2.6. A Solução deverá implementar controle de acesso baseado em papéis (RBAC), usuários e funções, permitindo atribuição de privilégios conforme perfil e área de atuação.

2.7. O acesso ao ambiente deverá ocorrer exclusivamente por navegador web compatível com HTML5, mediante protocolo HTTPS/TLS 1.2 ou superior, sendo vedado o uso de componentes locais ou protocolos obsoletos.

2.8. A Solução deverá ser plenamente compatível, no mínimo, com os navegadores Google Chrome (v. 110+), Microsoft Edge (v. 110+) e Mozilla Firefox (v. 100+), executados em sistemas operacionais Windows 10 ou superior.

2.9. O protocolo HTTPS deverá utilizar TLS 1.2 ou superior, sendo recomendável suporte à versão 1.3, vedada a utilização de versões obsoletas ou inseguras.

2.10. A Solução deverá permitir integração direta com o ServiceNow (módulo SIR) e com o sistema de Governança, Risco e Conformidade (GRC) do Banco da Amazônia para registro, acompanhamento e fechamento de incidentes e relatórios de auditoria.

3. OBJETIVO E ESCOPO FUNCIONAL

3.1. A Solução deverá ampliar a capacidade do Banco da Amazônia na identificação, análise, correlação e resposta a incidentes de segurança cibernética, integrando e correlacionando eventos provenientes de múltiplas camadas do ambiente tecnológico – endpoints, redes, aplicações, identidades, sistemas em nuvem e dispositivos de segurança, incluindo detecção e resposta a incidentes de fraude eletrônica e transacional.

3.2. A Solução deverá operar de forma integrada ao Centro de Operações de Segurança (SOC), no modelo de Cyber Fusion Center, à plataforma de Gestão de Vulnerabilidades (GVUL) e ao SIEM, compondo uma arquitetura unificada de segurança gerenciada, com visão correlacionada e resposta orquestrada em tempo real.

4. ARQUITETURA E COMPONENTES ESSENCIAIS

4.1. A Solução deverá incluir, no mínimo, os seguintes componentes nativos e integrados:

a) Monitoramento de Endpoints (EDR): coleta e análise de eventos de estações, notebooks, servidores e dispositivos móveis, com detecção de malware, ransomware, exploits e anomalias;

b) Monitoramento de Rede (NDR): inspeção de tráfego em tempo real, detecção de comunicações maliciosas e tentativas de exfiltração de dados;

c) Monitoramento de Identidades (IDR): análise de credenciais, autenticações e privilégios, com foco em acessos indevidos, contemplando aproximadamente 5.000 (cinco mil)

credenciais ativas do Active Directory (AD) do Banco da Amazônia, assegurando visibilidade completa dos acessos, detecção de comportamentos anômalos e correlação com os eventos de segurança registrados pelo SIEM e pelo XDR, em conformidade com as boas práticas de segurança cibernética;

d) Monitoramento de Aplicações e Nuvem: integração com plataformas SaaS, PaaS e IaaS (Microsoft 365, Azure, AWS, Google Cloud etc.);

e) Mecanismo de Correlação e Orquestração (SOAR): automação de respostas, execução de playbooks e enriquecimento de alertas;

f) Módulo de Inteligência Comportamental (UEBA): análise preditiva e detecção de desvios de comportamento;

g) Análise Forense e Investigação: consolidação de evidências e reconstrução detalhada de incidentes.

3.1 Todos os módulos deverão operar em ambiente unificado, com console web centralizado, interface em português e acesso autenticado via SSO e MFA.

5. FUNCIONALIDADES MÍNIMAS

5.1. A Solução deverá permitir a coleta, análise e correlação inteligente de dados de múltiplas fontes, empregando inteligência artificial, aprendizado de máquina e análise comportamental para detecção de anomalias e ameaças desconhecidas.

5.2. A Solução deverá possibilitar:

a) detecção automática de incidentes complexos em múltiplas camadas (endpoint, rede, identidade, nuvem);

b) resposta automatizada via playbooks configuráveis, os quais deverão ser submetidos à homologação formal e registro no ITSM do Banco antes da execução em produção;

c) integração bidirecional com o SIEM, alimentando e recebendo eventos correlacionados;

d) redução de falsos positivos por aprendizado contínuo e calibração de regras;

e) execução remota de ações corretivas (isolamento, bloqueio, quarentena ou reversão).

5.3. A Solução deverá incluir mecanismos de Threat Intelligence nativos e externos, permitindo correlação automática de IOCs (IPs, URLs, hashes, domínios) com os eventos coletados.

6. PROCESSO DE RESPOSTA A INCIDENTES

6.1. O processo de resposta deverá contemplar as etapas:

a) Identificação: detecção inicial do incidente e análise preliminar;

b) Contenção: isolamento automático ou manual dos ativos comprometidos;

c) Erradicação: remoção de artefatos e restauração da integridade do ambiente;

d) Recuperação: restabelecimento seguro dos serviços impactados;

e) Lições Aprendidas: geração de relatório pós-incidente com causa raiz, tempo de resposta (MTTR) e recomendações de endurecimento.

6.2. A Solução deverá permitir a criação e execução de playbooks de resposta personalizados, homologados pelo Banco da Amazônia, de acordo com o tipo e criticidade do incidente.

6.3. As atividades de resposta deverão ser registradas automaticamente na plataforma ServiceNow do Banco, com identificação do incidente, medidas executadas e resultados obtidos.

7. CORRELAÇÃO E INTEGRAÇÃO

7.1. A Solução deverá operar de forma nativamente integrada ao SIEM, SOC e GVUL, garantindo correlação cruzada entre alertas, vulnerabilidades e eventos de segurança.

7.2. A integração deverá permitir:

a) ingestão e envio bidirecional de eventos;

b) sincronização de alertas e incidentes;

c) uso unificado de indicadores de ameaça e inteligência comportamental;

d) visualização consolidada de riscos em dashboards únicos.

7.3. A Solução deverá possuir conectores nativos para plataformas corporativas do Banco da Amazônia, incluindo Active Directory, ServiceNow, Microsoft 365, Azure Defender e Google Workspace, entre outras.

8. INVESTIGAÇÃO E THREAT HUNTING

8.1. A Solução deverá permitir a realização de investigações avançadas e proativas (Threat Hunting), com periodicidade mínima semanal, visando à identificação de ameaças persistentes ou anomalias não detectadas automaticamente.

8.2. As atividades deverão incluir:

a) correlação manual e automatizada de logs e evidências;

b) consultas em linguagem natural suportadas por IA Generativa;

c) criação de hipóteses e regras customizadas de detecção;

d) exportação de evidências e relatórios técnicos para o SOC.

9. RELATÓRIOS, DASHBOARDS E INDICADORES

9.1. A Solução deverá disponibilizar relatórios técnicos e gerenciais, incluindo:

a) incidentes detectados e tratados, classificados por severidade;

b) indicadores de tempo médio de detecção e resposta (MTTD, MTTR e MTRI);

c) ameaças emergentes e tendências observadas;

d) recomendações de mitigação e endurecimento;

e) métricas de eficácia dos playbooks e das regras de detecção.

9.2. Relatórios deverão ser acessíveis via interface web, exportáveis em PDF e CSV, e apresentados em língua portuguesa.

9.3. A Solução deverá manter retrospectiva mínima de 12 (doze) meses de incidentes e alertas para auditoria e investigação forense.

10. SEGURANÇA, CONFORMIDADE E AUDITORIA

10.1. A Solução deverá observar integralmente os requisitos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e normas internacionais ISO/IEC 27001 e 27018, assegurando confidencialidade, integridade e disponibilidade das informações.

10.2. Todos os acessos e ações deverão ser registrados em trilhas de auditoria imutáveis, armazenadas por mínimo de 12 meses, acessíveis ao Banco para fins de auditoria interna e externa.

10.3. A Solução deverá manter logs de configuração, execução e resposta a incidentes, permitindo reconstrução detalhada dos eventos.

11. SUPORTE, LICENCIAMENTO E GOVERNANÇA

11.1. O licenciamento da Solução deverá incluir todos os componentes técnicos, módulos analíticos, conectores e APIs necessários para operação completa, sem custos adicionais para o Banco da Amazônia.

11.2. O suporte técnico deverá operar em regime 24×7×365, com atendimento em português, via portal web, e-mail e telefone, assegurando prazos de resposta compatíveis com os níveis mínimos de serviço (NMS).

11.3. A governança técnica deverá incluir reuniões mensais com a equipe de Segurança da Informação do Banco da Amazônia para revisão de indicadores, incidentes e melhorias contínuas.

11.4. O fabricante da Solução deverá assegurar a manutenção e evolução contínua do produto, incluindo atualizações automáticas de inteligência, detecção e correlação durante toda a vigência contratual.

1. DISPOSIÇÕES GERAIS

1.1 Este Anexo estabelece os Níveis Mínimos de Serviço (NMS) aplicáveis aos serviços continuados de que tratam os Itens 1 (XDR baseado em SIEM), 2 (GVUL) e 3 (SRIS), prestados em regime 24x7x365, conforme o Termo de Referência e o Anexo I-A — Especificações Técnicas.

1.2 Os NMS são organizados em 3 (três) trilhas de aferição independentes, correspondentes a cada um dos itens continuados, cada qual composta por indicadores agrupados por natureza de risco. A apuração mensal de cada trilha resulta em uma Nota de Desempenho (0 a 100), convertida em eventual glosa sobre o valor individual do respectivo item.

1.3 Fatura única: os Itens 1, 2 e 3 são faturados conjuntamente em fatura mensal única. A glosa apurada em cada trilha incide sobre a parcela do valor mensal correspondente ao respectivo item, conforme o Mapa de Composição de Preços, sendo o desconto total aplicado à fatura a soma das glosas apuradas nas 3 (três) trilhas.

1.4 Os indicadores, prazos, metas e pesos estabelecidos neste Anexo poderão ser revistos periodicamente pelo Banco da Amazônia, mediante justificativa técnica, observado o período de amadurecimento previsto no item 5.4.

2. TRILHA 1 — XDR BASEADO EM SIEM (ITEM 1)

2.1 Grupo A — Escalação de Alertas por Severidade

ID	Indicador	Severidade	Prazo	Unidade de aferição
NMS-01	Escalação de alerta	Crítica	30 minutos	Por alerta
NMS-02	Escalação de alerta	Alta	1 hora	Por alerta
NMS-03	Escalação de alerta	Média	2 horas	Por alerta
NMS-04	Escalação de alerta	Baixa	6 horas	Por alerta

2.1.1 [NMS-05] MTTD (Tempo Médio de Detecção): tempo decorrido entre a geração do alerta no SIEM e o escalonamento do respectivo ticket no ITSM/ServiceNow, apurado mensalmente como métrica complementar deste grupo, sem prejuízo da aferição individual do prazo de escalação por alerta. O indicador MTTR (Tempo Médio de Resposta), por abranger as fases de análise, contenção, erradicação e recuperação sob responsabilidade do time de SRIS, é definido e apurado no âmbito da Trilha 3 (item 4.4).

2.2 Grupo B — Gestão de Regras, Integrações e Correlação Multidomínio

ID	Indicador	Prazo	Unidade de aferição
NMS-06	Gestão de Regras de Correlação — criação	3 dias úteis	Por solicitação
NMS-07	Gestão de Regras de Correlação — alteração	1 dia útil	Por solicitação

ID	Indicador	Prazo	Unidade de aferição
NMS-08	Gestão de Fontes de Log — nova integração	7 dias úteis	Por fonte
NMS-09	Gestão de Fontes de Log — ajuste de integração existente	2 dias úteis	Por solicitação
NMS-10	Teste de Efetividade das Regras de Detecção	30 dias	Ciclo

2.2.1 [NMS-11] FIC — Fusion Intelligence Coverage Rate: percentual de incidentes tratados com base em correlação multidomínio (SIEM, GVUL, XDR baseado em SIEM, plataforma de Digital Risk Protection — DRP já contratada pelo Banco, e indicadores de risco operacional mantidos na plataforma corporativa de GRC do Banco, incluindo o módulo de Gestão Integrada de Riscos — IRM em implantação), apurado mensalmente.

2.2.2 Um incidente conta para o FIC quando, além dos dados nativos de SIEM/XDR, há evidência de enriquecimento por pelo menos um dos seguintes: (i) dado de vulnerabilidade do GVUL associado ao ativo afetado; (ii) indicador de ameaça ou risco digital da plataforma DRP; (iii) indicador de risco operacional da plataforma de GRC/IRM.

2.2.3 Meta do FIC: 80% (oitenta por cento), com período de amadurecimento de 60 (sessenta) dias corridos contados do Go-Live, conforme item 5.4, durante o qual o indicador será apurado e reportado sem impacto na Nota de Desempenho ou na glosa.

2.3 Grupo C — Ciclo de Relatórios e Governança

ID	Indicador	Prazo
NMS-12	Relatório Semanal	Toda segunda-feira, até as 20h
NMS-13	Relatório Mensal (entrega)	5 dias úteis do mês subsequente
NMS-14	Apresentação do Relatório Mensal	10 dias úteis do mês subsequente
NMS-15	Relatório Semestral	Conforme cronograma acordado com o Banco
NMS-16	Relatório de Investigação (sob demanda)	Conforme item 7 (Atividades Sob Demanda)

2.4 Grupo D — Atendimento Administrativo

ID	Indicador	Prazo
NMS-17	Atendimento a Solicitações e Dúvidas Diversas	2 dias úteis
NMS-18	Concessão de Acesso	1 dia útil

2.4.1 O indicador NMS-17 abrange solicitações, dúvidas ou pedidos de informação não enquadráveis em outro indicador deste Anexo. Pedidos de informação urgentes formulados no contexto de um incidente em andamento seguem os prazos aplicáveis à Trilha SRIS (item 4), não se sujeitando ao prazo deste item.

2.5 Grupo E — Falhas de Qualidade

ID	Falha	Descrição resumida	Tratamento	Pontos / Ocorrência
F-01	Indisponibilidade do SIEM	Indisponibilidade da plataforma central de correlação	Peso reforçado — falha grave	10 pontos, + 1 ponto por hora adicional, até 25 pontos
F-02	Ausência de tratamento de alerta	Alerta gerado e não tratado/escalado	Peso reforçado — falha grave	8 pontos
F-03	Alteração indevida de regra	Modificação não autorizada em regra de detecção	Peso reforçado — falha grave	8 pontos
F-04	Falha em Alerta	Classificação incorreta de severidade ou falha no processo de escalação	Peso padrão	3 pontos
F-05	Ajuste incorreto de regra	Erro técnico em alteração solicitada	Peso padrão	2 pontos
F-06	Não conformidade de licenciamento	Descumprimento de obrigação contratual de licenciamento	Peso padrão	3 pontos
F-07	Falha de Qualidade Geral	Entregas incompletas ou inconsistentes, ausência de evidências, erros de registro, negligência, imprudência ou imperícia	Peso padrão — catch-all	1 ponto

2.5.1 Os pontos indicados na tabela acima são cumulativos e correspondem a dedução direta na Nota de Desempenho da Trilha XDR baseado em SIEM (item 5.2), observado teto mensal de 30 (trinta) pontos para o conjunto das falhas deste Grupo, ainda que a soma das ocorrências no mês ultrapasse esse valor.

3. TRILHA 2 — GVUL (ITEM 2)

3.1 O ciclo de gestão de vulnerabilidades compreende as etapas de Descoberta, Varredura, Identificação, Classificação, Priorização, Encaminhamento, Tratamento, Reteste, Validação e Encerramento, nos termos do Anexo I-A. A responsabilidade da CONTRATADA abrange as etapas até o Encaminhamento e a posterior Validação/Reteste, não compreendendo a execução da correção em si, de responsabilidade da área de TI/negócio do Banco.

ID	Indicador	Prazo / Meta	Responsável pela aferição
NMS-19	Execução de varredura conforme calendário	Semanal (mínimo)	CONTRATADA
NMS-20	Identificação, classificação e encaminhamento — Crítica	24 horas após confirmação	CONTRATADA
NMS-21	Identificação, classificação e encaminhamento — Alta	48 horas após confirmação	CONTRATADA
NMS-22	Acompanhamento e escalonamento de pendências além do prazo interno do Banco	Reforço semanal à área responsável	CONTRATADA

ID	Indicador	Prazo / Meta	Responsável pela aferição
NMS-23	Validação pós-correção (reteste)	5 dias úteis após comunicação de correção	CONTRATADA

3.2 [NMS-24] Indicador informativo (sem incidência de glosa): tempo até a correção efetiva da vulnerabilidade pela área responsável do Banco, reportado no RSP e no Relatório Técnico Mensal para fins de gestão de risco, não sendo imputável à CONTRATADA.

3.3 Evidências: as etapas indicadas no item 3.1 serão registradas e mantidas na própria plataforma de Gestão de Vulnerabilidades da CONTRATADA, complementadas pelo ticket de Encaminhamento gerado automaticamente no ITSM/ServiceNow do Banco, conforme itens 5.4 e 5.5 do Anexo I-A.

3.4 Falhas de Qualidade

ID	Falha	Descrição	Pontos / Ocorrência
F-08	Falso negativo relevante	Vulnerabilidade crítica ou alta não identificada pela varredura, comprovadamente presente no ativo	8 pontos — falha grave
F-09	Varredura incompleta ou corrompida	Execução que não cobriu o escopo mínimo de ativos ou produziu dados inconsistentes	5 pontos
F-10	Qualidade da classificação/relatório	Severidade mal classificada, falso negativo não crítico ou relatório incompleto	3 pontos
F-11	Validação inadequada	Reteste que atesta correção indevidamente, com reincidência da mesma vulnerabilidade	5 pontos
F-12	Falha de Qualidade Geral	Entregas incompletas, ausência de evidências, negligência (catch-all)	1 ponto

3.4.1 Os pontos indicados são cumulativos e correspondem a dedução direta na Nota de Desempenho da Trilha GVUL (item 5.3), observado teto mensal de 20 (vinte) pontos para o conjunto das falhas deste item, ainda que a soma das ocorrências no mês ultrapasse esse valor.

4. TRILHA 3 — SRIS (ITEM 3)

ID	Indicador	Severidade	Prazo / Meta
NMS-25	Início de triagem após acionamento do SOC	Todas	15 minutos
NMS-26	Contenção	Crítica	30 minutos
NMS-27	Contenção	Alta	4 horas
NMS-28	Contenção	Média	12 horas
NMS-29	Contenção	Baixa	24 horas
NMS-30	Erradicação e Recuperação	Todas	Meta: percentual de incidentes concluídos dentro do RTO

ID	Indicador	Severidade	Prazo / Meta
			(Recovery Time Objective) acordado por tipo de incidente
NMS-31	Notificação de incidente com potencial dever de comunicação regulatória (BACEN/ANPD) à área de Segurança Corporativa	Todas, quando aplicável	2 horas após a confirmação do incidente
NMS-32	Relatório pós-incidente (RCA / lições aprendidas)	Todas	5 dias úteis após encerramento

4.1 Os prazos de contenção indicados aplicam-se de forma uniforme, independentemente de a equipe SRIS estar atuando presencialmente ou em regime remoto, nos termos do item 4 (formas de fornecimento) e da escala de atuação SRIS-N1/N2 prevista no Anexo I-A.

4.2 A meta de Erradicação e Recuperação depende da definição, pelo Banco da Amazônia, do RTO (Recovery Time Objective) acordado para cada tipo de incidente, a ser alinhado ao Plano de Continuidade de Negócios (BCP) e ao Plano de Recuperação de Desastres (DRP) do Banco.

4.3 A notificação de que trata a tabela acima tem por finalidade subsidiar o cumprimento, pelo Banco da Amazônia, do prazo regulatório de 72 (setenta e duas) horas para comunicação de incidentes aos órgãos competentes (BACEN, ANPD), não eximindo a CONTRATADA das demais obrigações de comunicação e evidenciação previstas neste Anexo e no Termo de Referência.

4.4 [NMS-33] MTTR (Tempo Médio de Resposta): tempo decorrido entre o escalonamento do ticket (marco final do MTTD, apurado na Trilha 1 — item 2.1.1) e a resolução/encerramento do incidente pelo time de SRIS, contemplando as fases de análise, contenção, erradicação e recuperação, apurado mensalmente como métrica complementar desta trilha.

4.5 Falhas de Qualidade

ID	Falha	Descrição	Pontos / Ocorrência
F-13	Contenção ineficaz / reabertura do incidente	Incidente declarado contido ou encerrado que reabre pela mesma causa raiz em até 30 dias	10 pontos — falha grave
F-14	Erro de procedimento na resposta	Execução incorreta de playbook/procedimento, causando dano adicional ou perda de evidência	8 pontos — falha grave
F-15	Falha de comunicação/escalonamento	Comunicação inadequada, incompleta ou fora do fluxo definido durante o incidente	5 pontos
F-16	Quebra de cadeia de custódia	Evidências não preservadas ou registradas de forma auditável	5 pontos
F-17	Falha de Qualidade Geral	Entregas incompletas, ausência de evidências, negligência (catch-all)	1 ponto

4.5.1 Os pontos indicados são cumulativos e correspondem a dedução direta na Nota de Desempenho da Trilha SRIS (item 5.3), observado teto mensal de 20 (vinte) pontos para o conjunto das falhas deste item, ainda que a soma das ocorrências no mês ultrapasse esse valor.

5. CRITÉRIOS DE PONTUAÇÃO E CÁLCULO DA NOTA DE DESEMPENHO

5.1 Para cada trilha, apura-se mensalmente o percentual de conformidade de cada grupo de indicadores (número de ocorrências atendidas dentro do prazo, dividido pelo total de ocorrências elegíveis no mês).

5.1.1 No Grupo B da Trilha XDR baseado em SIEM, que reúne indicadores de prazo (Gestão de Regras, Gestão de Fontes de Log e Teste de Efetividade) e o indicador FIC — este último já expresso como percentual, e não como razão de ocorrências —, a conformidade do grupo corresponde à média aritmética simples entre: (a) a conformidade agregada dos indicadores de prazo do grupo; e (b) o percentual apurado do FIC no mês.

5.2 Na Trilha XDR baseado em SIEM, a Nota de Desempenho Mensal corresponde à média ponderada dos percentuais de conformidade dos Grupos A a D, descontados os pontos apurados no Grupo E (Falhas de Qualidade), observados os seguintes pesos por grupo:

Grupo A (Escalação de Alertas) — 40%; Grupo B (Gestão de Regras, Integrações e FIC) — 30%; Grupo C (Ciclo de Relatórios) — 15%; Grupo D (Atendimento Administrativo) — 15%; Grupo E (Falhas de Qualidade) — dedução direta de pontos da Nota consolidada, não compondo a média ponderada dos demais grupos.

5.3 Nas Trilhas GVUL e SRIS, compostas por grupo único de indicadores, a Nota de Desempenho corresponde diretamente ao percentual de conformidade apurado no mês, descontados os pontos de falha eventualmente identificados.

5.4 Período de amadurecimento: indicadores novos ou alterados terão prazo de amadurecimento de 15 (quinze) a 60 (sessenta) dias corridos, conforme a complexidade, durante o qual serão apurados e reportados ao Banco sem impacto na Nota de Desempenho ou na glosa. Aplica-se, em particular, ao indicador FIC (item 2.2.1), cujo período de amadurecimento será de 60 (sessenta) dias corridos contados do Go-Live.

6. REGRA DE CONVERSÃO EM GLOSA

6.1 A glosa mensal de cada trilha é calculada conforme a seguinte fórmula, aplicada à respectiva Nota de Desempenho:

Glosa (%) = 0 (zero), se Nota ≥ 95;

Glosa (%) = MÍNIMO [30%; (95 − Nota)], se Nota < 95.

6.2 A glosa apurada em cada trilha incide sobre o valor individual do respectivo item (Item 1, 2 ou 3), conforme o Mapa de Composição de Preços, sendo o desconto total aplicado à fatura mensal única correspondente à soma das glosas apuradas nas 3 (três) trilhas.

6.3 Ao ser atingido o teto de 30% (trinta por cento) de glosa em qualquer trilha, o fato deverá ser formalmente comunicado à área competente do Banco da Amazônia para avaliação da aplicação das Sanções Administrativas previstas no item 13 do Termo de Referência (Anexo I), sem prejuízo da continuidade da apuração mensal das demais trilhas, nos mesmos moldes do disposto na Cláusula 3.4 do contrato de SOC atualmente vigente.

6.4 Em caso de descumprimentos recorrentes de um mesmo indicador por 3 (três) meses consecutivos, o Banco poderá determinar a revisão do peso do grupo correspondente ou a exigência de plano de ação corretivo pela CONTRATADA, sem prejuízo da glosa apurada no período de referência.

7. CONDIÇÕES GERAIS DE AFERIÇÃO

7.1 A contagem dos prazos poderá ser suspensa em caso de dependência de terceiros ou de ação exclusiva do Banco, mediante registro formal do motivo da pendência no sistema de registro aplicável a cada trilha, nos termos do item 8.

7.2 Eventos causados exclusivamente pelo Banco não serão considerados na aferição dos NMS.

7.3 O encerramento de chamado, ticket ou registro de vulnerabilidade depende de aprovação do Banco e da entrega das evidências correspondentes.

8. EVIDÊNCIAS E FONTES DE AFERIÇÃO

8.1 Trilhas XDR baseado em SIEM e SRIS: registros da própria plataforma da CONTRATADA (SIEM, XDR, SOAR ou equivalente) e, para os indicadores de natureza incidental ou de escalação (NMS-01 a NMS-04 e NMS-25 a NMS-32), tickets registrados e mantidos atualizados no ITSM/ServiceNow do Banco da Amazônia, conforme Anexo I-A.

8.2 Trilha GVUL: registros da própria plataforma de Gestão de Vulnerabilidades da CONTRATADA, complementados pelo ticket de Encaminhamento gerado no ITSM/ServiceNow, conforme itens 5.4 e 5.5 do Anexo I-A.

9. RELATÓRIOS

9.1 Relatório de Serviços Prestados (RSP): mensal, contemplando, para cada trilha, a Nota de Desempenho apurada, os indicadores individuais, as falhas registradas e a glosa correspondente, além do desconto total aplicado à fatura mensal única.

9.2 Relatório Técnico Mensal: consolidação técnica das atividades, incidentes, vulnerabilidades tratadas e indicadores complementares (MTTD, MTTR, FCR, MRR e FIC), conforme o Termo de Referência.

10. EXEMPLO ILUSTRATIVO DE APURAÇÃO MENSAL

10.1 Este exemplo é meramente ilustrativo, com valores fictícios, e tem por finalidade demonstrar a aplicação prática da metodologia de Nota de Desempenho e da regra de conversão em glosa. Considera-se, para fins didáticos, um mês de referência posterior ao período de amadurecimento do indicador FIC.

10.2 Trilha 1 — XDR baseado em SIEM (Item 1)

10.2.1 Grupo A — Escalação de Alertas

ID	Severidade	Alertas elegíveis	Dentro do prazo	Conformidade
NMS-01	Crítica	5	5	100%
NMS-02	Alta	10	9	90%
NMS-03	Média	20	18	90%
NMS-04	Baixa	15	14	93,3%
—	Total do Grupo A	50	46	92%

10.2.2 Grupo B — Regras, Integrações e FIC

ID	Indicador	Elegíveis	Dentro do prazo/meta	Conformidade
NMS-06	Gestão de Regras de Correlação — criação	4	4	100%
NMS-07	Gestão de Regras de Correlação — alteração	2	2	100%
NMS-08	Gestão de Fontes de Log — nova integração	1	1	100%
NMS-09	Gestão de Fontes de Log — ajuste de integração	1	1	100%
NMS-10	Teste de Efetividade das Regras de Detecção	1	1	100%
—	Subtotal — indicadores de prazo	9	9	100%

FIC [NMS-11] apurado no mês: 70% (abaixo da meta de 80% definida no item 2.2.3).

Conformidade do Grupo B, pela regra do item 5.1.1 = média entre indicadores de prazo (100%) e FIC (70%) = (100% + 70%) ÷ 2 = 85%.

10.2.3 Grupo C — Ciclo de Relatórios

ID	Indicador	Elegíveis	Dentro do prazo	Conformidade
NMS-12	Relatório Semanal (4 semanas no mês)	4	4	100%
NMS-13	Relatório Mensal (entrega)	1	1	100%
NMS-14	Apresentação do Relatório Mensal	1	1	100%
—	Total do Grupo C	6	6	100%

10.2.4 Grupo D — Atendimento Administrativo

ID	Indicador	Elegíveis	Dentro do prazo	Conformidade
NMS-17	Atendimento a Solicitações e Dúvidas Diversas	7	6	85,7%
NMS-18	Concessão de Acesso	3	3	100%
—	Total do Grupo D	10	9	90%

Consolidando os 4 (quatro) grupos, com os pesos definidos no item 5.2:

Grupo	% de Conformidade Apurado	Peso	Contribuição Ponderada
A — Escalação de Alertas	92%	40%	36,8
B — Regras, Integrações e FIC	85%	30%	25,5
C — Ciclo de Relatórios	100%	15%	15,0
D — Atendimento Administrativo	90%	15%	13,5

Subtotal ponderado (Grupos A a D): 36,8 + 25,5 + 15,0 + 13,5 = 90,8 pontos.

No mês, houve 1 (uma) ocorrência de “Falha em Alerta” [F-04] (Grupo E), correspondendo a 3 pontos de dedução direta, valor muito abaixo do teto mensal de 30 pontos previsto no item 2.5.1.

Nota de Desempenho da Trilha 1 = 90,8 − 3 = 87,8.

Glosa da Trilha 1 = MÍNIMO [30%; (95 − 87,8)] = MÍNIMO [30%; 7,2%] = 7,2%.

10.3 Trilha 2 — GVUL (Item 2)

ID	Indicador	Elegíveis	Dentro do prazo/meta	Conformidade
NMS-19	Execução de varredura conforme calendário	4	4	100%
NMS-20	Identificação/classificação/encaminhamento — Crítica	5	5	100%
NMS-21	Identificação/classificação/encaminhamento — Alta	7	6	85,7%
NMS-22	Acompanhamento e escalonamento de pendências	5	5	100%
NMS-23	Validação pós-correção (reteste)	4	4	100%
—	Total do Grupo (Trilha 2)	25	24	96%

Não houve, no mês, ocorrência de falhas de qualidade listadas no item 3.4 (F-08 a F-12).

Nota de Desempenho da Trilha 2 = 96.

Como a Nota é igual ou superior a 95, a glosa da Trilha 2 é igual a 0% (dentro da franquia do item 6.1).

10.4 Trilha 3 — SRIS (Item 3)

ID	Indicador	Elegíveis	Dentro do prazo/meta	Conformidade
NMS-25	Início de triagem após acionamento do SOC	4	4	100%
NMS-26	Contenção — Crítica	1	1	100%
NMS-27	Contenção — Alta	1	1	100%
NMS-28	Contenção — Média	1	0	0%
NMS-29	Contenção — Baixa	1	1	100%
NMS-32	Relatório pós-incidente (RCA / lições aprendidas)	2	2	100%
—	Total do Grupo (Trilha 3)	10	9	90%

O desvio de contenção refere-se ao indicador NMS-28 (Contenção — Média): um único incidente contido em 14 horas, acima do prazo aplicável de 12 horas. Não houve, no mês, ocorrência de falhas de qualidade listadas no item 4.5 (F-13 a F-17).

Nota de Desempenho da Trilha 3 = 90.

Glosa da Trilha 3 = MÍNIMO [30%; (95 − 90)] = MÍNIMO [30%; 5%] = 5%.

10.5 Aplicação da glosa na fatura mensal única

Considerando, a título ilustrativo, a seguinte composição de valores mensais por item (Mapa de Composição de Preços fictício, sem correspondência com valores reais do certame):

Item / Trilha	Valor mensal do item (ilustrativo)	Glosa apurada	Valor da glosa (R$)
Item 1 — XDR baseado em SIEM	R$ 100.000,00	7,2%	R$ 7.200,00
Item 2 — GVUL	R$ 100.000,00	0%	R$ 0,00
Item 3 — SRIS	R$ 100.000,00	5%	R$ 5.000,00
Total da fatura mensal única	R$ 300.000,00	—	**R$ 12.200,00**

Valor líquido da fatura mensal, após a glosa: R$ 300.000,00 − R$ 12.200,00 = R$ 287.800,00.

Como nenhuma das 3 (três) trilhas atingiu o teto de 30% no mês de referência, não há, neste exemplo, acionamento do item 6.3 (comunicação à área competente para avaliação de Sanções Administrativas).

PREGÃO ELETRÔNICO N. 90029/2026
ANEXO I-C
PROVA DE CONCEITO (POC)

1. DISPOSIÇÕES GERAIS

1.1. Com a finalidade de aferir, de forma prática, objetiva e isonômica, a aderência técnica, funcional, operacional e de integração da solução ofertada, a LICITANTE provisoriamente classificada em primeiro lugar deverá submeter sua solução à Prova de Conceito – POC (Proof of Concept), observadas as condições, procedimentos e critérios estabelecidos neste Anexo.

1.2. A POC constitui etapa de avaliação da proposta e será realizada anteriormente à contratação, possuindo caráter eliminatório e constituindo condição obrigatória para aceitação da proposta da LICITANTE.

1.3. A POC não constitui início da execução contratual e não se confunde com:

a) implantação da solução;

b) integração definitiva com o ambiente do Banco;

c) migração de dados, regras ou casos de uso;

d) testes técnicos da implantação;

e) Testes de Aceitação pelo Usuário – UAT;

f) homologação;

g) Go-Live;

h) operação assistida;

i) estabilização; ou

j) aceite contratual.

1.4. A POC terá por finalidade validar as capacidades essenciais relacionadas aos seguintes componentes do objeto:

a) Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM – XDR baseado em SIEM;

b) Serviço e Solução Integrada de Gestão de Vulnerabilidades – GVUL;

c) capacidades tecnológicas e fluxos operacionais relacionados à Resposta a Incidentes de Segurança na Primeira Linha de Defesa – SRIS;

d) integração multidomínio entre detecção, análise, vulnerabilidades, incidentes e resposta;

e) automação e orquestração – SOAR;

f) análise comportamental – UEBA;

g) Threat Intelligence;

h) governança, rastreabilidade e auditabilidade da solução.

1.5. Não integram o escopo da POC, como objetos autônomos de demonstração:

a) o Serviço de Implantação, Integração, Migração, Homologação e Transição Operacional do Cyber Fusion Center;

b) os Serviços Técnicos Especializados sob demanda, mensurados em UST; e

c) as turmas de Capacitação Técnica.

1.6. A exclusão prevista no item anterior não impede que funcionalidades relacionadas a implantação, integração, documentação ou operação sejam demonstradas quando necessárias à comprovação dos requisitos tecnológicos estabelecidos no roteiro da POC.

1.7. A avaliação será realizada exclusivamente com base no Roteiro Objetivo de Testes constante do Item 4 deste Anexo, aplicando-se os mesmos procedimentos e critérios de aprovação a todas as LICITANTES eventualmente convocadas.

1.8. Não haverá atribuição de pontuação, classificação qualitativa, avaliação subjetiva ou bonificação por funcionalidades adicionais. Cada teste obrigatório receberá exclusivamente uma das seguintes classificações:

a) ATENDIDO; ou

b) NÃO ATENDIDO.

1.9. Funcionalidades adicionais, superiores ou não exigidas no roteiro poderão ser registradas no relatório técnico, exclusivamente para fins informativos, sem influência na aprovação, reprovação ou classificação da LICITANTE.

1.10. Após a conclusão da POC, será elaborado Relatório Técnico de Avaliação contendo, no mínimo:

a) identificação da LICITANTE;

b) identificação da solução, fabricante, produto, edição e versão demonstrados;

c) relação dos profissionais participantes;

d) identificação dos testes executados;

e) resultado individual de cada teste;

f) evidências correspondentes;

g) eventuais ocorrências técnicas registradas;

h) observações apresentadas pela LICITANTE, quando cabíveis; e

i) conclusão pela aprovação ou reprovação.

1.11. A proposta somente será considerada tecnicamente aceita após a aprovação da solução na POC.

1.12. Em caso de reprovação, serão adotados os procedimentos previstos no Edital, incluindo a desclassificação da proposta e convocação da LICITANTE subsequente, observada a ordem de classificação.

2. FORMA, PRAZOS E CONDIÇÕES DE EXECUÇÃO

2.1. A POC será realizada, preferencialmente, de forma remota, mediante videoconferência pela plataforma Microsoft Teams disponibilizada pelo Banco da Amazônia, podendo o Banco determinar, mediante justificativa técnica, a realização de atividade presencial ou em ambiente controlado.

2.2. A sessão poderá ser integralmente gravada pelo Banco da Amazônia, inclusive áudio, vídeo e compartilhamento de tela, para composição do processo licitatório e suporte à elaboração do Relatório Técnico de Avaliação.

2.3. A LICITANTE deverá iniciar a POC em até 5 (cinco) dias úteis após sua convocação.

2.4. A partir da primeira sessão, a LICITANTE disporá de até 5 (cinco) dias úteis para conclusão integral da POC, de acordo com agenda definida pelo Banco.

2.5. O prazo previsto no item 2.4 poderá ser prorrogado, mediante decisão fundamentada do Banco:

a) por ocorrência técnica não imputável à LICITANTE;

b) por indisponibilidade de ambiente, sistema ou recurso cuja disponibilização seja de responsabilidade do Banco;

c) por caso fortuito ou força maior devidamente comprovado; ou

d) por outra circunstância tecnicamente justificada que não comprometa a isonomia do procedimento.

2.6. Falhas de conectividade, indisponibilidade do Microsoft Teams ou de recursos sob responsabilidade do Banco não serão computadas em prejuízo da LICITANTE.

2.7. A condução da POC deverá ser realizada por profissionais indicados pela LICITANTE, que serão responsáveis pela operação da solução, execução dos procedimentos e apresentação das evidências.

2.8. Será admitida a participação de profissionais do fabricante, distribuidor, parceiro tecnológico ou terceiro especializado exclusivamente como suporte técnico passivo, observado que:

a) a demonstração deverá permanecer sob condução da LICITANTE;

b) os terceiros não poderão assumir a condução da POC;

c) não poderão substituir os profissionais da LICITANTE na execução sistemática dos testes;

d) poderão prestar esclarecimentos técnicos quando solicitados pelo Banco ou apoiar internamente a LICITANTE na solução de questões pontuais; e

e) a participação deverá ser previamente identificada e registrada em ata.

2.9. A presença do fabricante ou parceiro não será utilizada como critério de aprovação ou reprovação, permanecendo a LICITANTE responsável pela demonstração da capacidade de operar e integrar a solução ofertada.

2.10. A POC poderá ser executada em ambiente de demonstração, laboratório, tenant de teste, sandbox ou ambiente equivalente, desde que:

a) corresponda à mesma solução, edição, arquitetura e conjunto de funcionalidades ofertados;

b) utilize versões estáveis e oficialmente suportadas;

c) estejam disponíveis todos os módulos necessários aos testes obrigatórios;

d) não sejam utilizadas funcionalidades que não integrem a proposta comercial; e

e) os resultados sejam tecnicamente reproduzíveis na solução ofertada.

2.11. Não serão aceitas, como substituição à demonstração prática exigida, funcionalidades:

a) previstas exclusivamente em roadmap futuro;

b) ainda não disponíveis comercialmente;

c) dependentes de desenvolvimento futuro específico para o Banco;

d) dependentes de módulo ou licenciamento não contemplado na proposta; ou

e) apresentadas exclusivamente mediante slides, vídeos previamente gravados ou materiais publicitários.

2.12. Documentação oficial do fabricante, manuais, fichas técnicas ou evidências equivalentes poderão complementar a demonstração prática, mas não substituí-la nos testes classificados como obrigatórios.

2.13. A LICITANTE deverá compartilhar a tela durante a execução dos procedimentos práticos, permitindo à equipe avaliadora acompanhar comandos, configurações, eventos, resultados, logs e evidências relevantes.

2.14. O Banco poderá solicitar, para robustecer a comprovação dos resultados:

a) acesso temporário e de somente leitura ao ambiente de demonstração;

b) exportação de logs;

c) relatórios técnicos;

d) registros de auditoria;

e) arquivos JSON, CSV ou outro formato estruturado suportado;

f) evidências de API;

g) capturas de tela;

h) registros de execução dos playbooks; ou

i) outros artefatos gerados diretamente pela solução durante os testes.

2.15. O acesso previsto no item anterior, quando solicitado, deverá possuir privilégio mínimo necessário e não poderá permitir ao Banco alterar configurações ou dados do ambiente da LICITANTE.

2.16. Os testes deverão utilizar exclusivamente dados sintéticos, anonimizados, fictícios ou especialmente preparados para a POC, salvo autorização expressa do Banco para utilização de outro conjunto de dados.

2.17. A POC será realizada sem qualquer ônus para o Banco da Amazônia.

3. TRANSPARÊNCIA E ACOMPANHAMENTO

3.1. Será permitida a participação, na condição de observadores, de até representantes das demais LICITANTES, conforme regras estabelecidas no Edital, mediante identificação e apresentação de procuração ou documento equivalente que demonstre seus poderes de representação.

3.2. Os observadores:

a) não poderão interferir na execução;

b) não poderão formular perguntas diretamente à LICITANTE avaliada;

c) não poderão sugerir procedimentos;

d) não poderão interromper os testes; e

e) deverão observar as regras de confidencialidade e segurança do Banco.

3.3. A gravação oficial da POC será realizada exclusivamente pelo Banco, não sendo permitida aos observadores gravação paralela, captura de tela ou outro registro que possa comprometer informações protegidas da solução ou do processo.

3.4. Todas as ocorrências relevantes, suspensões, repetições de testes, falhas técnicas e decisões da equipe avaliadora deverão ser registradas.

4. ROTEIRO OBJETIVO DE TESTES DA POC

4.1 Regras de avaliação

4.1.1. Todos os testes identificados na tabela deste item como OBRIGATÓRIOS deverão ser atendidos.

4.1.2. Cada teste possuirá:

a) identificador único;

b) capacidade avaliada;

c) procedimento mínimo;

d) evidência esperada; e

e) critério binário de aprovação.

4.1.3. Será considerado ATENDIDO o teste em que a LICITANTE execute integralmente o procedimento e apresente a evidência definida, demonstrando o resultado esperado.

4.1.4. Será considerado NÃO ATENDIDO o teste quando:

a) a funcionalidade exigida estiver ausente;

b) a funcionalidade depender de produto, licença ou módulo não contemplado;

c) não for possível demonstrar o resultado esperado;

d) a LICITANTE desistir da execução;

e) a evidência apresentada não demonstrar objetivamente a execução do requisito; ou

f) a demonstração depender de desenvolvimento futuro da solução.

4.1.5. A simples existência de integração com determinado produto comercial não será exigida quando o teste puder comprovar a capacidade por API, conector oficial, webhook ou mecanismo equivalente, preservando a neutralidade tecnológica.

4.2 Monitoramento, Detecção e XDR baseado em SIEM

ID	Requisito obrigatório	Procedimento mínimo	Critério objetivo de aprovação
POC-01	Coleta e ingestão de múltiplas fontes	Ingerir eventos provenientes de pelo menos 3 fontes de naturezas distintas, utilizando no conjunto ao menos 2 mecanismos de coleta suportados, como Syslog, API, arquivo estruturado, agente ou conector	Os eventos das 3 fontes são recebidos pela solução e ficam disponíveis para consulta
POC-02	Parsing e normalização	Demonstrar a transformação de eventos brutos em campos estruturados e pesquisáveis	Os eventos apresentam campos normalizados que permitam identificação de origem, ativo, usuário/identidade, data/hora e evento, quando presentes
POC-03	Correlação multidomínio	Correlacionar eventos provenientes de pelo menos 2 fontes distintas referentes a uma mesma entidade, ativo ou cenário	A solução gera correlação única, alerta ou incidente contendo referência às fontes utilizadas
POC-04	UEBA	Executar ou apresentar cenário controlado de comportamento anômalo de usuário ou entidade	A solução identifica a anomalia e apresenta evidência do comportamento, entidade e respectivo contexto ou risco
POC-05	Threat Intelligence	Importar ou utilizar IoC de teste e correlacioná-lo a evento da POC	O IoC é identificado e seu contexto de Threat Intelligence é apresentado pela solução
POC-06	Priorização baseada em risco	Gerar eventos com diferentes contextos ou níveis de criticidade	A solução atribui prioridade, severidade ou risco de maneira rastreável e apresenta os fatores considerados
POC-07	Cenário controlado de ataque	Executar cenário simulado seguro que gere evento de segurança identificável	A solução detecta o cenário e gera alerta ou incidente correspondente
POC-08	Investigação	A partir de alerta gerado na POC, realizar busca, pivoteamento ou timeline	A solução permite reconstruir eventos e acessar evidências utilizadas na análise

4.2.1. Para fins deste Anexo, o XDR baseado em SIEM não será avaliado como solução autônoma de XDR/EDR de endpoint.

4.2.2. Não será exigida, na POC, implantação de novo agente de XDR/EDR nos endpoints do Banco.

4.2.3. Eventos e telemetrias de endpoint poderão ser produzidos em ambiente de demonstração ou por integração com solução de endpoint existente ou equivalente, exclusivamente para comprovação de correlação e interoperabilidade.

4.3 Automação, Orquestração e Resposta

ID	Requisito obrigatório	Procedimento mínimo	Critério objetivo de aprovação
POC-09	Criação automática de incidente	Configurar ou utilizar regra existente que, a partir de alerta gerado durante a POC, produza incidente/caso	O incidente é criado automaticamente e mantém vínculo com o alerta ou evento de origem
POC-10	SOAR / Playbook	Executar playbook contendo ao menos 2 etapas de processamento ou resposta	As etapas são executadas e registradas, com resultado individual e trilha de execução
POC-11	Acionamento de controle externo	Executar, em ambiente controlado, ação por API, conector ou mecanismo suportado, como bloqueio de IP, alteração de regra, desabilitação simulada de identidade, solicitação de contenção ou ação equivalente	A requisição de resposta é efetivamente realizada, seu resultado é retornado ou confirmado e a ação fica registrada
POC-12	Aprovação humana quando requerida	Demonstrar playbook capaz de interromper fluxo automático para autorização de ação sensível	O fluxo permanece aguardando aprovação e somente prossegue após a autorização configurada
POC-13	ITSM	Demonstrar criação e atualização automática de ticket por integração suportada com ServiceNow ou ambiente de teste disponibilizado pelo Banco	O ticket é criado e recebe atualização automática com dados provenientes do incidente
POC-14	Registro de evidências	Demonstrar registro das ações tomadas durante a resposta	A solução apresenta sequência cronológica, responsáveis, comandos/ações e respectivos resultados

4.3.1. Caso o Banco disponibilize ambiente de homologação ou sandbox do ServiceNow, o teste POC-13 será realizado contra esse ambiente.

4.3.2. Caso tal ambiente não seja disponibilizado, será aceita demonstração utilizando conector oficialmente suportado, API ou ambiente de teste da LICITANTE, desde que seja possível comprovar tecnicamente a criação e atualização bidirecional do registro.

4.3.3. A ação de contenção prevista no POC-11 tem por finalidade comprovar a capacidade de orquestração e integração do XDR baseado em SIEM, não a existência de uma nova plataforma XDR de endpoint.

4.4 Gestão de Vulnerabilidades – GVUL

ID	Requisito obrigatório	Procedimento mínimo	Critério objetivo de aprovação

POC-15	Identificação de vulnerabilidades	Realizar ou demonstrar varredura em ativo controlado contendo vulnerabilidade conhecida	A vulnerabilidade é identificada e associada ao ativo correspondente
POC-16	Classificação	Exibir vulnerabilidade identificada e seus atributos de risco	A solução apresenta classificação de severidade e referência técnica aplicável, como CVE/CVSS ou equivalente
POC-17	Priorização baseada em risco	Comparar duas ou mais vulnerabilidades com contextos distintos	A solução apresenta ordenação ou priorização considerando, além da severidade técnica, contexto de risco, exploitabilidade, ameaça ou criticidade do ativo
POC-18	Contextualização por ativo	Associar vulnerabilidade a ativo ou grupo classificado como crítico	A criticidade do ativo fica disponível e influencia ou complementa a avaliação da vulnerabilidade
POC-19	Correlação GVUL × XDR baseado em SIEM	Utilizar vulnerabilidade de ativo que participe de evento ou alerta gerado na POC	O alerta/incidente apresenta ou permite recuperar o contexto da vulnerabilidade correspondente
POC-20	Relatórios	Gerar relatório ou dashboard das vulnerabilidades demonstradas	Relatório/dashboard apresenta ativos, vulnerabilidades, criticidade e status, com possibilidade de exportação

4.5 Integração Multidomínio e Cyber Fusion Center

ID	Requisito obrigatório	Procedimento mínimo	Critério objetivo de aprovação
POC-21	Fluxo integrado fim a fim	Executar cenário envolvendo evento de segurança, ativo com vulnerabilidade conhecida e mecanismo de resposta	A solução permite acompanhar o fluxo desde detecção/correlação até incidente e resposta, preservando o contexto
POC-22	Compartilhamento de contexto	Exibir informações de eventos, ativo,	As informações podem ser relacionadas ou

		identidade, vulnerabilidade e incidente relacionadas ao mesmo caso, quando aplicáveis	acessadas de maneira contextualizada sem necessidade de reconstrução manual desconectada
POC-23	Automação entre capacidades	Gerar evento ou condição que acione automaticamente fluxo subsequente	O acionamento ocorre sem necessidade de criação manual do caso pelo Banco e fica registrado
POC-24	Visão consolidada	Apresentar painel ou interface que consolide informações relevantes do ambiente de segurança	A solução apresenta em visão consolidada dados de pelo menos eventos/incidentes, ativos ou vulnerabilidades e risco/severidade
POC-25	Interoperabilidade	Demonstrar API documentada, conector ou mecanismo equivalente para integração externa	É possível consultar, enviar ou receber dado por mecanismo oficialmente suportado e documentado

4.5.1. A visão consolidada prevista neste item não pressupõe plataforma monolítica ou produto único, sendo admitida arquitetura federada desde que a integração funcional e a preservação de contexto sejam demonstradas.

4.6 Governança, Rastreabilidade e Auditoria

ID	Requisito obrigatório	Procedimento mínimo	Critério objetivo de aprovação
POC-26	Dashboard operacional	Apresentar painel contendo eventos, alertas ou incidentes produzidos durante a POC	Os dados apresentados correspondem aos eventos efetivamente gerados nos testes
POC-27	Indicadores	Demonstrar geração ou cálculo de indicadores de detecção/resposta, incluindo MTTD e/ou MTTR quando aplicáveis	O indicador possui origem de dados e timestamps que permitam verificar seu cálculo
POC-28	Trilha de auditoria	Executar alteração ou ação administrativa controlada	A ação fica registrada com identificação do usuário, data/hora e atividade realizada
POC-29	RBAC	Demonstrar dois perfis com níveis distintos de autorização	Os usuários apresentam permissões distintas correspondentes aos perfis configurados
POC-30	MFA	Demonstrar autenticação multifator no acesso administrativo ou mecanismo equivalente previsto na solução	O segundo fator é efetivamente exigido no processo de autenticação
POC-31	Exportação de evidências	Exportar relatório, log, evento, incidente ou trilha produzido na POC	A informação é exportada em formato suportado e seu conteúdo

			corresponde ao dado demonstrado na solução

5. LIMITES E CONDIÇÕES DOS TESTES

5.1. A POC possui natureza amostral e destina-se à comprovação prática das capacidades críticas especificadas no roteiro, não implicando reprodução integral de todos os requisitos do Termo de Referência ou do Anexo I-A.

5.2. A aprovação na POC não dispensa a LICITANTE, caso contratada, do cumprimento integral de todos os requisitos do Termo de Referência, Anexo I-A, Anexo I-B e demais documentos da contratação.

5.3. Não será exigido durante a POC:

a) processamento real e continuado de 600 GB/dia;

b) varredura simultânea dos 5.000 ativos do Banco;

c) integração efetiva dos 5.000 endpoints previstos como capacidade de cobertura;

d) operação contínua durante 24x7x365;

e) retenção efetiva de dados por 60 meses; ou

f) mobilização da equipe definitiva da futura execução contratual.

5.4. Os requisitos de capacidade, volumetria, retenção, alta disponibilidade, licenciamento, dimensionamento de equipe e suporte poderão ser confirmados por documentação técnica oficial, evidências de configuração, declaração do fabricante quando cabível, proposta técnica e, posteriormente, pelas etapas de implantação e aceite contratual.

5.5. O previsto no item anterior não autoriza o atendimento futuro de funcionalidade inexistente. Toda funcionalidade exigida no roteiro prático deverá estar disponível na solução apresentada durante a POC.

6. EVIDÊNCIAS E ACESSO TÉCNICO

6.1. Para cada teste, a equipe avaliadora deverá associar pelo menos uma evidência que permita confirmar objetivamente o resultado.

6.2. Poderão constituir evidências:

a) capturas de tela produzidas durante a sessão;

b) gravação oficial;

c) logs de aplicação;

d) registros de auditoria;

e) relatórios exportados;

f) arquivos estruturados;

g) resultados de APIs;

h) tickets;

i) registros de playbooks;

j) dashboards; e

k) documentação oficial utilizada exclusivamente de forma complementar.

6.3. Quando solicitado, a LICITANTE deverá disponibilizar à equipe técnica do Banco acesso temporário de somente leitura ao ambiente de demonstração ou entregar evidências técnicas exportáveis capazes de permitir validação independente do resultado.

6.4. Todas as evidências deverão ser identificadas pelo código do respectivo teste.

7. REEXECUÇÃO DE TESTES E OCORRÊNCIAS TÉCNICAS

7.1. Quando determinado teste não puder ser concluído em razão de falha transitória de conectividade, videoconferência, infraestrutura ou ambiente que não represente ausência da funcionalidade avaliada, a equipe técnica poderá autorizar sua reexecução.

7.2. Toda reexecução deverá ser fundamentada e registrada no Relatório Técnico.

7.3. A reexecução não poderá ser utilizada para:

a) desenvolver funcionalidade inexistente;

b) contratar novo módulo;

c) alterar a solução originalmente ofertada;

d) substituir produto ou edição ofertada; ou

e) incluir componente que não integrava a proposta.

7.4. Configurações, parametrizações e ajustes ordinariamente suportados pela solução poderão ser realizados durante a POC, desde que não caracterizem desenvolvimento de nova funcionalidade ou alteração material da proposta.

7.5. Quando a interrupção decorrer exclusivamente de fato imputável ao Banco, o teste será reagendado sem prejuízo à LICITANTE.

8. CRITÉRIOS DE APROVAÇÃO

8.1. Todos os requisitos constantes das tabelas do Item 4 são classificados como OBRIGATÓRIOS E ELIMINATÓRIOS.

8.2. A solução será considerada APROVADA quando todos os testes obrigatórios forem classificados como ATENDIDOS.

8.3. A solução será considerada REPROVADA quando, concluídas as possibilidades de reexecução previstas neste Anexo, houver pelo menos um teste obrigatório classificado como NÃO ATENDIDO.

8.4. Não haverá compensação entre requisitos, pontuação mínima global ou utilização de desempenho superior em determinado teste para suprir o não atendimento de outro.

8.5. Critérios como estética da interface, preferência pessoal, facilidade subjetiva de uso ou outras percepções não mensuráveis não poderão fundamentar reprovação.

8.6. Informações relativas à ergonomia, facilidade de navegação e funcionalidades adicionais poderão constar do relatório exclusivamente como registro informativo.

9. RELATÓRIO DE AVALIAÇÃO

9.1. O relatório deverá utilizar, no mínimo, a seguinte estrutura:

ID do teste	Requisito	Resultado	Evidência	Observações
POC-XX	Descrição	ATENDIDO / NÃO ATENDIDO	Identificação da evidência	Registro objetivo

9.2. A fundamentação de eventual resultado NÃO ATENDIDO deverá indicar expressamente:

a) o procedimento realizado;

b) o comportamento observado;

c) o resultado esperado;

d) a diferença entre resultado observado e esperado; e

e) a evidência que sustenta a conclusão.

9.3. Não será admitida reprovação fundada exclusivamente em expressões genéricas como “baixa efetividade”, “usabilidade inadequada”, “desempenho insuficiente”, “integração deficiente” ou equivalentes sem vinculação a requisito objetivo do roteiro.

9.4. A LICITANTE poderá solicitar o registro, no relatório ou ata da sessão, de observação técnica relacionada ao resultado de determinado teste, sem prejuízo dos mecanismos de recurso previstos no Edital e na regulamentação aplicável.

10. RESULTADO DA POC

10.1. Concluída a avaliação, a equipe técnica emitirá parecer com uma das seguintes conclusões:

I – APROVADA: atendimento de todos os testes obrigatórios;

II – REPROVADA: não atendimento de um ou mais testes obrigatórios, observadas as regras deste Anexo.

10.2. A aprovação na POC constitui condição necessária à aceitação da proposta, mas não gera direito subjetivo à adjudicação ou contratação.

10.3. Em caso de reprovação, serão adotados os procedimentos previstos no Edital para desclassificação e convocação da LICITANTE subsequente.

11. DISPOSIÇÕES FINAIS

11.1. A participação na POC implica ciência das condições estabelecidas neste Anexo.

11.2. Todos os testes deverão ser executados com observância às regras de segurança, confidencialidade, proteção de dados e integridade do processo licitatório.

11.3. A LICITANTE será responsável pelos recursos tecnológicos, licenças, ambientes, profissionais e demais meios necessários à demonstração, ressalvados aqueles que o Banco informar expressamente que disponibilizará.

11.4. A execução da POC não gera obrigação de pagamento, ressarcimento ou indenização pelo Banco.

11.5. A solução, edição, módulos e componentes aprovados na POC deverão corresponder àqueles constantes da proposta aceita e constituirão referência para a implantação contratual, ressalvadas atualizações de versão, evolução tecnológica ou substituições posteriormente admitidas nos termos do contrato, desde que mantida ou ampliada a aderência aos requisitos.

11.6. A aprovação na POC não substitui os testes técnicos, UAT, homologação, Go-Live e aceite previstos para a fase de implantação, os quais serão realizados sobre a solução efetivamente configurada, integrada e disponibilizada no ambiente aplicável à execução contratual.

PREGÃO ELETRÔNICO N. 90029/2026

REQUISITOS MÍNIMOS DE SEGURANÇA PARA SISTEMAS ADQUIRIDOS

ANEXO I-A

REQUISITOS GERAIS DE SEGURANÇA PARA A CONTRATADA

A contratada deverá assinar, no início do contrato, o Termo de Confidencialidade e Sigilo que terá como objetivo definir as regras relativas ao tratamento, acesso, proteção e revelação das informações corporativas do Banco da Amazônia (BASA).

Todos os empregados da empresa **contratada** que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato deverão assinar o Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado. O referido termo deverá ser entregue ao

gestor do contrato antes do início das atividades do profissional.

A contratada deverá:

- adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do BASA;

- comunicar com antecedência mínima de 15 (quinze) dias ao BASA qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do BASA, porventura colocados à disposição para realização dos serviços contratados;

- manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo BASA a tais documentos;

- não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do BASA, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;

- manter seus empregados devidamente informados das normas disciplinares do BASA, bem como das normas de utilização e de segurança das instalações e do manuseio dos documentos;

- manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do BASA;

- garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do Banco da Amazônia;

- assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;

- assumir inteira responsabilidade por quaisquer danos ou prejuízos causados ao BASA e a terceiros, incluindo prejuízos financeiros, por dolo ou culpa, de seus empregados, decorrentes dos serviços ora contratados;

- garantir e manter total e absoluto sigilo sobre as informações manuseadas as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;

- não repassar a terceiros, em nenhuma hipótese, qualquer informação sobre a arquitetura e/ou documentação, assim como dados e/ou metadados trafegados, produtos desenvolvidos e entregues, ficando responsável juntamente com o BASA por manter a segurança da informação relativa aos dados e procedimentos durante a execução das atividades e em período posterior ao término da execução do contrato;

- assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BASA através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado;

- providenciar para que os produtos e artefatos da contratação sejam entregues em perfeito estado, com a segurança necessária, garantindo o transporte, o seguro, a entrega e a implantação nos locais indicados pelo BASA sem quaisquer danos, avarias ou ônus adicionais para o BASA.

COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM

A contratada deve garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo que o BASA tenha todas as garantias legais enquanto tomador do serviço e proprietário das informações, se hospedadas na nuvem.

A contratada deverá:

- cumprir integralmente as diretrizes da Resolução CMN 4.893/21;
- fornecer acesso ao BASA aos dados e às informações a serem processados ou armazenados pela empresa contratada;
- assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador;
- apresentar conformidade com a norma ABNT NBR ISO/IEC 27001:2013 referente aos serviços de computação em nuvem e aos data centers que hospedem esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao BASA promover diligência destinada a esclarecer ou complementar informações;
- fornecer ao BASA acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e aos controles utilizados na execução dos serviços a serem contratados;
- fornecer informações e recursos de gestão para possibilitar o monitoramento dos serviços a serem prestados;
- assegurar, enquanto o contrato estiver vigente, a identificação e a segregação dos dados dos clientes do BASA por meio de controles físicos ou lógicos e forneça ao BASA documentos e/ou relatórios que evidenciem o cumprimento desta exigência;
- assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do BASA;
- adotar um padrão de identidade federada para permitir o uso de tecnologia **single sign-on** no processo de autenticação dos usuários do serviço de nuvem, o qual deve ser acompanhado de autenticação multifator (MFA).
- registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.
- apoiar o BASA, quando necessário, nas atividades de investigação de incidentes de cibersegurança. Isso inclui fornecer prontamente informações e recursos necessários para a investigação, como logs, registros de eventos e relatórios de auditoria.
- adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, caso o serviço a ser contratado seja relativo ao serviço de execução de aplicação por meio da internet;
- garantir que o ambiente seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados por outros usuários do serviço em nuvem;
- assegurar que toda atualização do sistema seja previamente analisada e homologada antes que possa ser instalada/configurada, além de dispor de documentação de todas as alterações realizadas no serviço e/ou sistema mediante processos formalizados de Gestão e Mudanças;

- assegurar a adoção de medidas de segurança para a transmissão e armazenamento dos dados e das informações processados ou armazenados pelo prestador, e fornecer ao BASA evidências da adoção das referidas medidas;

- notificar ao BASA sobre a intenção de interromper a prestação de serviços com pelo menos trinta dias de antecedência da data prevista para a interrupção;

- conceder o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

- manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

- dispor de Plano de Comunicação de Incidentes e/ou dashboards com informações referentes a saúde dos serviços oferecidos de incidentes que possam ocorrer, informando o BASA os casos de incidentes de segurança da informação, assim considerados os eventos não previstos ou não desejados que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do BASA;

- realizar a análise e gestão de riscos de segurança de informação. A análise deve ter periodicidade no mínimo mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes;

- possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção;

- desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços ou envolvendo dados pessoais de empregados e/ou clientes do BASA;

- realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) e auditorias por terceira parte reconhecidamente confiável, disponibilizando relatório comprobatório a cada três meses para o BASA;

- prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;

- deverá fornecer, sempre que solicitado pelo BASA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de Application Programming Interface (API), caso haja, para análise de segurança e auditorias;

- dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do BASA, incluindo os seguintes itens: solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações), solução de prevenção e detecção de intrusão (IDS/IPS), antivírus, anti-malware, solução anti-DDoS, solução de gestão de logs, solução de gestão integrada de pacotes de correção (patches), solução de correlação de eventos de segurança (SIEM);

- realizar backups e salvaguardas dos conteúdos das comunicações realizadas por meio da solução e permitir a consulta desses dados;

- garantir a exclusividade de direitos, por parte do BASA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como **backups** de segurança.

- comprometer-se a preservar os dados do BASA contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente à BASA qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados;

- operar o serviço dentro do uso proposto, com desempenho razoável e exigindo o mínimo possível de permissões dos demais sistemas do BASA, além de proteger os dados transmitidos por meio dele, quando necessário;

- atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:

- as diretrizes de tratamento;

- o modo de atendimento a solicitações de titulares de dados pessoais;

- as medidas protetivas para garantia da confidencialidade dos dados pessoais;

- as medidas protetivas durante as comunicações com o BASA;

- o registro de atividades de tratamento de dados pessoais;

- a solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;

- a medidas de devolução / descarte dos dados.

- A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:

- inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;

- inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

- não fornecimento a terceiros de dados do BASA, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

- fornecer ao BASA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BASA.

- Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo BASA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se que:

- pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

- a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, desde que em conformidade com a Resolução CMN 4.893/21.

- A empresa deve garantir a adequação e a adoção de medidas pelo BASA, em decorrência de qualquer determinação do Órgãos Governamentais aos quais o BASA é subordinado que impacte sobre o Contrato vigente.

- A empresa deve manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

- É vedado o uso de informações do BASA pela contratada para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

- Em caso de extinção do contrato, a contratada deverá transferir os dados e as informações processados ou armazenados por ele ao novo prestador de serviços ou ao BASA e, após a confirmação da integridade e da disponibilidade dos dados e informações recebidos, os excluir.

- Em caso da decretação de regime de resolução do Banco da Amazônia pelo Banco Central do Brasil, a contratada deverá:

- conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações que estejam em poder da empresa contratada; e

- notificar previamente o responsável pelo regime de resolução sobre sua a intenção de interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção. A contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

REQUISITOS DE ARQUITETURA, DESIGN E MODELAGEM DE AMEAÇAS

O sistema, com recursos web, deverá incorporar, no mínimo, proteção contra:

- **Controle de acesso falho:** as restrições sobre o que os usuários autenticados têm permissão para fazer muitas vezes não são aplicadas de forma adequada. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

- **Falhas criptográficas:** Muitos aplicativos da web e APIs não protegem adequadamente os dados sigilosos, como dados pessoais e financeiros. Os invasores podem roubar ou modificar esses dados fracamente protegidos para conduzir fraude de cartão de crédito, roubo de identidade ou outros crimes. Os dados sigilosos podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requerem precauções especiais quando trocados com o navegador.

- **Injeção:** Injeções ocorrem quando dados informados pelo usuário são enviados para um interpretador como parte de um comando ou uma query. O dado malicioso do atacante faz o interpretador executar comandos que não deveria ou modificar dados. Algumas das injeções mais comuns são SQL, NoSQL, OS command, Mapeamento Relacional de Objeto (ORM), LDAP e Expression Language (EL) ou Object Graph Navigation Library (OGNL). O conceito é idêntico entre todos. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções.

- **Design inseguro:** O design seguro é uma cultura e metodologia que avalia constantemente as ameaças e garante que o código seja desenvolvido e testado de forma robusta para evitar métodos de ataque conhecidos. O design seguro requer um ciclo de vida de desenvolvimento seguro, alguma forma de padrão de design seguro ou biblioteca ou ferramenta de componentes de estradas pavimentadas e modelagem de ameaças.

- **Configuração incorreta de segurança:** geralmente é o resultado de configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas também devem ser corrigidos / atualizados em tempo hábil.

- **Componentes vulneráveis e desatualizados:** componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios do aplicativo. Se

um componente vulnerável for explorado, esse tipo de ataque pode facilitar a perda séria de dados ou o controle do servidor. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas do aplicativo e permitir vários ataques e impactos.

- **Falhas de identificação e autenticação:** as funções do aplicativo relacionadas à autenticação e gerenciamento de sessão são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários temporária ou permanentemente.

- **Falhas de software e integridade de dados:** As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Por exemplo, quando objetos ou dados são codificados ou serializados em uma estrutura que um invasor pode ver e modificar, logo é vulnerável à desserialização insegura. Outro exemplo é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs).

- **Registro (logging) e monitoramento insuficientes:** registro (logging) e monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permite que os invasores ataquem ainda mais os sistemas, mantenham a persistência, ganhem acesso em mais sistemas e adulterem, extraiam ou destruam dados.

- **Server-Side Request Forgery (SSRF):** As falhas de SSRF ocorrem sempre que um aplicativo web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de ACL de rede.

- **Validação de entrada inadequada:** o produto recebe entradas ou dados, mas não valida ou valida incorretamente se a entrada possui as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado pela aplicação.

- **Caracteres Especiais ou maliciosos:** caracteres especiais são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros. Garanta que apenas entradas válidas, esperadas e apropriadas sejam processadas pelo Sistema.

- A solução deverá possuir conformidade com o OWASP TOP 10 vigente visando assegurar a segurança dos dados, gerar confiança entre os usuários, prevenir perdas financeiras e cumprir regulamentações de segurança, proporcionando a integridade e a credibilidade necessárias para um site ou aplicativo.

A solução não deve ser baseada nos frameworks Wordpress ou Joomla.

Deverá ser imposto o menor privilégio em conexões com o banco de dados ou outros sistemas de back-end.

A Contratada deverá realizar configuração segura (hardening) do servidor web no qual a aplicação está hospedada e deverá assegurar que servidores web da aplicação estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmark mais atual.

As seguintes flags e procedimentos relacionados deverão ser adotados em relação às configurações do cabeçalho para a comunicação entre o servidor e o cliente:

- A aplicação deverá instruir o browser a só permitir acesso via HTTPS. Deverá ser ativado o HTTP Strict Transport Security (HSTS) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. O max-age deve ser de pelo menos 31536000 segundos (1 ano);

- O cabeçalho X-Content-Type-Options deverá estar configurado como 'nosniff' para todas as páginas da web;

- A aplicação deverá retornar o cabeçalho X-Frame-Options com o valor DENY ou SAMEORIGIN, que permitirá “framing” das páginas conforme SAME ORIGIN;

- A aplicação deverá ter o CSP habilitado enviando os cabeçalhos de resposta Content-Security-Policy, conforme políticas que atenda critérios de segurança na implementação dessa diretiva;

- A aplicação deverá ter o cabeçalho X-XSS-Protection desabilitado, por meio da configuração do seu valor como 0 (zero);

- A aplicação não deverá possuir os cabeçalhos “fingerprinting”: X-Powered-By, Server, X-AspNet-Version;

- A aplicação deverá forçar content-type para as respostas. Se a aplicação retorna json, a resposta content-type da aplicação deverá ser application/json;

- Os tipos de conteúdo text/ *, / + xml e application/xml também devem especificar um conjunto de caracteres seguro (por exemplo, UTF-8, ISO-8859-1);

- O conteúdo da aplicação não poderá ser incorporado a um site de terceiro por padrão;

- O Cross-Origin Resource Sharing (CORS) e cabeçalho Access-Control-Allow-Origin deverão utilizar uma lista de permissão restrita de domínios e subdomínios confiáveis para correspondência e não oferecer suporte à origem "null", e validar os dados inseridos pelo usuário;

- O cookie emitido pela aplicação deverá possuir os atributos SameSite, SECURE e HttpOnly;

A aplicação deverá utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações

Antes da entrada em produção, a solução passará por homologação quanto a sua segurança. Quaisquer eventuais vulnerabilidades identificadas pela equipe do BASA serão tratadas como defeito de software e deverão obrigatoriamente ser corrigidas pela CONTRATADA.

Realizar configuração segura do servidor web, também conhecido como hardening. Assegurar que servidores WEB estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmarks.

Utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.

REQUISITOS DE ARMAZENAMENTO DE DADOS E PRIVACIDADE

Os recursos de armazenamento de credenciais do sistema deverão ser utilizados para armazenar dados restritos e sigilosos, como dados pessoais, credenciais de usuário ou chaves criptográficas

Dados restritos e sigilosos não deverão:

ser exibidos em mensagens de erro;

- ser armazenados fora do contêiner da aplicação ou de recursos de armazenamento de credenciais do sistema;

- ser armazenados em texto claro, como um banco de dados não criptografado;

- aparecer nos logs de aplicação;
- ser compartilhados com terceiros, exceto se for uma parte necessária da arquitetura;
- ser expostos através de mecanismos IPC (Inter-process Communication);
- ser armazenados localmente ou em arquivos temporários no dispositivo. Em vez disso, os dados deverão ser recuperados de um terminal remoto quando necessário e mantidos apenas em memória.

A aplicação não deverá exibir mensagens de erro detalhadas que possa expor informações privilegiadas.

Senhas ou PINs de acesso não deverão ser expostos através da interface de usuário.

Credenciais de acesso não deverão ser armazenadas dentro do código-fonte do sistema.

Será obrigatória a validação, a filtragem e o tratamento de todos os dados inseridos pelo usuário.

Toda requisição de acesso ao banco de dados deverá passar por processo de validação de autorização.

Será vedada a filtragem de dados no cliente.

Não deverá ser utilizado o método GET (URLs) para o envio de dados restritos ou sigilosos ou para a realização transações financeiras.

O método HTTP deverá ser utilizado de acordo com a operação: GET (read), POST (create), PUT/PATCH (replace/update), e DELETE (delete).

Será proibida a utilização de dados sensíveis (credenciais de acesso, senhas, tokens ou API keys) na URL, deverá ser utilizado cabeçalho Authorization.

Toda requisição de acesso à API deverá passar por processo de validação de autorização.

Um mecanismo de validação de entrada padrão deverá ser utilizado para validar todos os dados em tamanho, tipo, sintaxe e regras de negócio antes de exibi-los ou armazená-los.

Deverá ser utilizada a estratégia de validação do tipo Whitelist.

Será obrigatória a validação content-type de dados publicados (POST) aceitáveis (por exemplo application/x-www-form-urlencoded, multipart/form-data, application/json etc.).

Entradas inválidas deverão ser rejeitadas, ao invés de se tentar sanitizar dados impróprios/maliciosos.

REQUISITOS DE AUTENTICAÇÃO

O sistema deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.

O sistema deve possuir mecanismo de múltiplo fator de autenticação (MFA);

O sistema deve ser capaz de admitir integração com MS-AD (Microsoft Active Diretory) do BASA para login único de usuário (Single Sign On = SSO).

As senhas deverão ser gravadas em banco de dados de forma criptografada.

A tela de log-on não deverá exibir a senha que está sendo informada.

O sistema não deverá armazenar ou transmitir senhas em texto plano.

A tela de entrada dos sistemas deverá validar as informações fornecidas pelo usuário somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar qual parte do dado de entrada está correta ou incorreta.

Em caso de tentativa de log-on inválida, o sistema deverá exibir uma mensagem genérica e nunca exibir as mensagens "usuário inexistente" ou "senha incorreta", de modo a não fornecer mensagens que permitam a um usuário não autorizado deduzir informações de acesso.

Todo acesso administrativo deverá ser restrito e deverá ser garantido o acesso apenas aos usuários autorizados.

Deverá ser utilizado HTTPS para envio de credenciais.

Os sistemas não deverão passar ID de sessão por método HTTP GET.

Deverá ser utilizado sempre o método HTTP POST para a requisição de autenticação.

Será obrigatória a utilização do parâmetro “state” com hash aleatório no processo de autenticação do OAuth.

Será proibido o uso de Basic Authentication.

As autorizações de acesso deverão ser validadas, garantindo que nenhum usuário acessará o que não foi previamente definido em seu perfil.

O processo de login deve ser iniciado através de uma página com um novo cookie de sessão.

Todos os endpoints do sistema deverão ser protegidos por autenticação.

Será proibido o incremento de IDs automaticamente. No lugar, deverá ser utilizado UUID.

REQUISITOS DE GERENCIAMENTO DE SESSÃO DO USUÁRIO

As sessões deverão ser invalidadas pelo terminal remoto após um período de, no máximo, 15 minutos de inatividade e os tokens de acessos devem expirar.

O controle de sessão deverá ser tratado pelo servidor e apenas a persistência dele no cliente.

Os sistemas deverão implementar token de sessão por requisição com alta aleatoriedade, devendo ser utilizados tokens personalizados e aleatórios em todos os formulários e URLs que não serão automaticamente enviadas pelo navegador.

Toda as páginas deverão ter um link para o logout o qual, ao clicar, o sistema deverá realizar o logout sem antes questionar o usuário. O logout deve destruir todo o estado da sessão no lado servidor e os cookies no lado cliente.

Será proibido o uso de “response_type=token”.

Dados de usuários, atributos e políticas utilizados pelos controles de acesso, não podem ser manipulados pelos usuários finais, a menos que especificamente autorizado na arquitetura do projeto.

O sistema deverá utilizar o princípio do menor privilégio, os usuários só devem ser capazes de acessar funções, arquivos de dados, URLs, controladores, serviços e outrosoken recursos, para os quais possuam autorização específica.

Em caso de sistemas que utilizam JWT (JSON Web Token):t

- Será obrigatório o uso de chaves randômicas (JWT Secret);
- Será proibido armazenar dados confidenciais em tokens JWT.
- Será proibida a extração do algoritmo do cabeçalho (deverá ser validado no back-end);
- Deverá ser utilizado no back-end o algoritmo RS256;
- Será obrigatório regras de time-out de sessão do usuário de 15 minutos, access token de 3 minutos e refresh token de 8 horas.

REQUISITOS DE COMUNICAÇÃO DE REDE

O sistema deverá ser capaz de suportar a pilha dupla IPV4 e IPv6.

Todas as comunicações externas entre os servidores do sistema e os clientes deverão ser encriptadas.

O sistema deverá utilizar criptografia para as comunicações externas entre os servidores do sistema e os clientes. Os dados deverão ser criptografados na rede utilizando somente TLS 1.2 ou superior.

O sistema não deverá permitir o uso do SSL, TLS 1.0 e TLS 1.1.

Deve-se usar os seguintes algoritmos: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 e SHAKE256.

Será vedada a utilização de cifras com vulnerabilidades divulgadas e/ou conhecidas.

As requisições deverão ser limitadas (através de rate limit ou outra solução semelhante), a fim de se evitar ataques de DoS (negação de serviço) ou força bruta.

Deverá ser utilizada a validação de “redirect_url” no servidor para permitir apenas URL’s da *whitelist.*

Tráfegos HTTP deverão ser redirecionados para HTTPS.

A propriedade “readOnly” deverá ser configurada como “true” em esquemas de objeto para todas as propriedades que podem ser recuperadas por meio de APIs, mas nunca deverão ser modificadas.

Os modos de depuração do servidor da Web ou de aplicativos e da estrutura de aplicativos deverão ser desativados em produção para eliminar recursos de depuração, consoles de desenvolvedor e divulgações de segurança não intencionais.

REQUISITOS DE RESPOSTAS HTTP

Os cabeçalhos HTTP ou qualquer parte da resposta HTTP não deverão expor informações detalhadas da versão dos componentes do sistema.

A aplicação deverá retornar os seguintes códigos:

- 405 Method Not Allowed: sempre que um método solicitado não for apropriado para o recurso solicitado
- 406 Not Acceptable: sempre que o formato suportado não for correspondido. Requisições content-type deverão ser validadas para permitir apenas o formato suportado (por exemplo application/xml, application/json etc.)
- HTTP 200: código de resposta do status de sucesso do HTTP, indica que a solicitação foi bem-sucedida;
- HTTP 302: indica que o recurso solicitado foi movido temporariamente para a URL fornecida pelo cabeçalho Location.
- HTTP 401: para qualquer ação não autorizada no sistema.
- HTTP 429: para solicitações que excedam o limite de requisição permitido.
- HTTP 415: para solicitações contendo cabeçalhos de tipo de conteúdo ausentes ou inesperados

A aplicação deverá ter defesas contra ataques de poluição de parâmetro HTTP, especialmente se a estrutura do aplicativo não faz distinção sobre a origem dos parâmetros de solicitação (GET, POST, cookies, cabeçalhos ou variáveis de ambiente).

Redirecionamentos e encaminhamentos de URL deverão permitir apenas destinos que

aparecem em uma lista de permissões ou deverão mostrar um aviso ao redirecionar para conteúdo potencialmente não confiável.

A aplicação deverá ter proteção contra ataques do tipo SSRF, validando ou higienizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos, campos de entrada de URL, listas de protocolos, domínios, caminhos e portas.

REQUISITOS DE AUDITORIA

A solução deve dispor de logs de eventos para fins de auditoria, incluindo todas as ações administrativas e ações envolvendo os itens arquivados e pesquisados no que tange o arquivamento, visualização, recuperação e remoção de itens.

A solução deve dispor de logs com registro de informações a serem utilizadas na depuração e verificação de falhas da solução, mantendo o registro de toda atividade de arquivamento e recuperação realizada, inclusive para os processos de auditoria realizados.

A solução deve permitir a configuração de usuários (auditores), com permissão de monitorar (auditar) e acessar grupos específicos de caixas postais e/ou todas as mensagens arquivadas.

A solução deve suportar a geração e armazenamento de logs no formato IPV4 e IPv6.

As aplicações deverão implementar um sistema de *logging* que permita auditorias e investigações de incidentes de segurança, fraudes e casos de abuso.

A identificação do usuário, ou ID, deverá ser única, isto é, cada usuário deverá ter uma identificação própria.

Os sistemas de informação e suas respectivas infraestruturas deverão ser configurados de modo a registrar um critério mínimo de informações de logging e auditoria, contendo, no mínimo:

- operações de login e logout;
- tentativas de login malsucedidas;
- acesso a telas cujo conteúdo é sigiloso, em segredo de justiça, possua dados pessoais ou bancários;
- operações de inclusão, alteração ou exclusão de registros no banco de dados;
- execução de jobs e tarefas automatizadas;
- criação, leitura, atualização ou exclusão de informações sigilosas;
- mudanças de configurações no sistema, na rede ou em serviços (inicialização, suspensão e reinicialização de serviços), inclusive a instalação de patches e atualizações de softwares;
- acesso aos bancos de dados de fonte interna e externa;
- falhas que resultem no fechamento anormal da aplicação, especialmente devido à exaustão de recurso ou atingimento do limite de um recurso (como memória do CPU, conexões de rede, espaço no disco etc.);
- acesso e alteração de trilhas de auditoria;
- registros de tráfego de dados de fontes internas e externas; e
- registros de processos internos relacionados às atividades do negócio.

Os registros dos eventos deverão incluir, no mínimo, as seguintes informações:

- identificação inequívoca do autor/ativo que realizou a atividade;

- sistema onde ocorreu ou foi observada a atividade (logger/observador do evento);
- tela (página) do sistema de onde a operação foi realizada;
- tipo de atividade ocorrida (tipo de evento/ação);
- data, hora e fuso horário, observando os mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);
- retorno do sistema em caso de falhas ou sucesso na ação;
- identificador da instância (para sistemas clusterizados);
- para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;
- parâmetros informados pelo usuário (ex: parâmetros repassados aos métodos GET ou POST);
- tempo de resposta do sistema;
- para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada etc.; e
- endereço IP, nome do dispositivo, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

A aplicação não deve registrar credenciais ou detalhes de pagamento.

Os tokens de sessão só devem ser armazenados em logs de forma irreversível e com hash.

Será vedado o envio de informações sensíveis (ex: credenciais de acesso) para logs.

A solução não deverá registrar logs de auditoria em banco de dados da aplicação.

As aplicações deverão registrar logs de rastreamento distribuído (distributed tracing) de requisição.

As aplicações deverão gerar logs em formato que permita a completa identificação dos fluxos de dados

As aplicações deverão registrar eventos relevantes de segurança, incluindo eventos de autenticação bem-sucedidos e com falha, falhas de controle de acesso, falhas de desserialização e falhas de validação de entrada.

A solução deve garantir que todas as fontes de tempo estão sincronizadas com a hora e fuso horário corretos.

Dados de registro devem ser sanitizados para evitar ataques de injeção de registro.

REQUISITOS PARA APIs

A codificação de API deverá incorporar, no mínimo, proteção contra:

a) Broken Object Level Authorization

b) Broken User Authentication

c) Excessive Data Exposure

d) Lack of Resources & Rate Limiting

e) Broken Function Level Authorization

f)Mass Assignment

g) Security Misconfiguration

h) Injection (Injection flaws, tais como SQL e NoSQL, Command Injection etc.)

i)Improper Assets Management

j)Insufficient Logging & Monitoring

k) Conformidade com o OWASP Top 10 API Security Risks em vigor

Deverão ser utilizadas as classes Encoder e Validator da OWASP ESAPI (Enterprise Security API)

Deve ser imposto o menor privilégio quando se conectar ao banco de dados ou outros sistemas de back-end.

O banco de dados não deverá ser acessado por outro canal que não seja a aplicação

Os URLs da API não deverão expor informações confidenciais, tais como a chave da API, tokens de sessão etc.

Objetos serializados deverão usar verificações de integridade ou criptografados para evitar a criação de objetos hostis ou adulteração de dados.

Todos os endpoints acessíveis ao público devem usar um Certificado Digital que tenha sido assinado por uma Autoridade de Certificação aprovada e dentro do prazo de utilização.

Devem ser aplicadas políticas de limitação de taxa (ratelimit) para evitar o abuso da API.

Toda entrada pelo usuário por parâmetros da aplicação ou de forma manipulada em qualquer outra parte da aplicação, deverá ser validada, garantindo as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado."

A solução deve garantir que apenas entradas válidas, esperadas e apropriadas sejam processadas, pois caracteres especiais ou maliciosos são usados para explorar falhas como: SQL injection, XSS, Temlate Injection, entre outros.

PREGÃO ELETRÔNICO N. 90029/2026

CECLARAÇÃO DE CAPACIDADE TÉCNICA

ANEXO I-E

MODELO DE DECLARAÇÃO DE CAPACIDADE TÉCNICA

1. Dados da Licitante

RAZÃO SOCIAL:

CNPJ:

ENDEREÇO:

TELEFONE:

E-MAIL:

2. Declaração

A (nome da LICITANTE) declara que possui capacidade técnica para a prestação dos serviços do OBJETO do presente Termo de Referência.

[Local], XX de XXXX de XXXX.

_____

<Assinatura do Representante legal>

Nome:

Cargo:

CPF:

RG:

PREGÃO ELETRÔNICO N. 90029/2026

ANEXO II

CARTA DE APRESENTAÇÃO DE PROPOSTA

Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação nº...../.....

Objeto: .....

Prezados senhores:

A .....,inscrita no CNPJ sob o nº ....., sediada (endereço completo)....., com o telefone para contato nº (...).....-.....e e-mail ....., por intermédio do seu representante legal o(a) Sr.(a).....(cargo)....., portador(a) da Carteira de Identidade nº..... e do CPF nº....., residente e domiciliado(a) no.....(endereço completo)....., tendo examinado as condições do Edital e dos Anexos que o integram, apresenta a proposta comercial relativa à licitação em epígrafe, assumindo inteira responsabilidade por quaisquer erros ou omissões que tiverem sido cometidos quando da preparação da mesma:

1. Propõe-se o Valor Total de R$ .....(.....), para o fornecimento dos serviços objeto desta licitação.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA	Preço Unitário (R$)	Preço Global (R$)
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	Mês	60		
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	Mês	60		
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	Mês	60		
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	Serviço	1		
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	UST	5.000		
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	Turma	3 (com 15 participantes cada)		
VALOR GLOBAL DO CONTRATO PARA 60 MESES					

Obs.:	**** Regime contínuo de 24x7x365.***		
	***** Sob demanda, a critério do Banco, mediante Ordem de Serviço.***		

2. No valor total proposto estão englobados todos os custos e despesas previstos no Edital Nº...../....., tais como: custos diretos e indiretos, tributos, encargos sociais,

trabalhistas e previdenciários, seguros, taxas, lucro, uniformes, alimentação, transporte, plano de assistência médico-hospitalar e odontológica e outros necessários ao cumprimento integral do objeto.

3. Junta-se detalhamento da proposta.

4. Que, em relação às prerrogativas da Lei Complementar n. 123/2016, o proponente:

( ) Enquadra-se como microempresa, empresa de pequeno porte ou equivalente legal, nos termos previsto no Decreto n. 8.538/2015, conforme certidão expedida pela Junta Comercial ou Cartório de Registro em anexo. Ainda, que:

( ) É optante do Simples Nacional, submetendo-se à alíquota de.....%, apurada com base no faturamento acumulado dos últimos 12 meses.

( ) Não é optante do Simples Nacional.

( ) Não se enquadra na condição de microempresa, empresa de pequeno porte ou equivalente legal.

5. Essa proposta é válida por 60 (sessenta) dias, contados da data prevista para abertura dos envelopes.

6. Até que o contrato seja assinado, esta proposta constituirá um compromisso da..... , observadas as condições do Edital. Caso esta proposta não venha a ser aceita para contratação, O Banco da Amazônia fica desobrigada de qualquer responsabilidade referente à presente proposta.

7. Os pagamentos serão efetuados em conformidade com as condições estabelecidas na Minuta do Contrato.

8. Devem ser utilizados, para quaisquer pagamentos, os dados bancários a seguir: BANCO: .....
AGÊNCIA: .....
CONTA CORRENTE: .....
PRAÇA DE PAGAMENTO: .....

9. Por fim, declara conhecer e aceitar as condições constantes do Edital n. ...../.....e de seus Anexos.

.....
(Local e Data)

.....
(representante legal

PREGÃO ELETRÔNICO N. 90029/2026.
ANEXO III
MODELO DE DECLARAÇÃO

DECLARAÇÃO DE CONFORMIDADE AO ARTIGO 38 DA LEI N. 13.303/2016

Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação n. ...../.....
Objeto: .....

Prezados senhores,

A ....., inscrita no CNPJ sob o n. ....., sediada.....(endereço completo)....., com o telefone para contato n. (.....).....-..... e e-mail ....., por intermédio do seu representante legal o(a) Sr.(a)..... , ...(cargo)....., portador(a) da Carteira de Identidade n. ..... e do CPF n. ....., residente e domiciliado(a) no .....(endereço completo) ..... , DECLARA, para os devidos fins legais, que a empresa não incorre em nenhum dos impedimentos para participar de licitações e ser contratada, prescritos no artigo 38 da Lei n. 13.303/2016, quais sejam:

(i) cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;

(ii) suspensa pela empresa pública ou sociedade de economia mista;

(iii) declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;

(iv) constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

(v) cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

(vi) constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

(vii) cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

(viii) que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

Aplica-se a vedação também:

(i) à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

(ii) a quem tenha relação de parentesco, até o terceiro grau civil, com:

a) dirigente de empresa pública ou sociedade de economia mista;

b) empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

c) autoridade do ente público a que a empresa pública ou sociedade de economia mista esteja vinculada.

(iii) cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a respectiva empresa pública ou sociedade de economia mista promotora da licitação ou contratante há menos de 6 (seis) meses.

.....
(Local e Data)

.....
(representante legal)

PREGÃO ELETRÔNICO N. 90029/2026.
ANEXO IV
MODELO DE DECLARAÇÃO

MINUTA DE DECLARAÇÃO DE CONHECIMENTO DO TEOR DO DECRETO Nº 7.203, DE 04.06.2010

Para participar do Pregão Eletrônico nº 90029/2026, cujo objeto **********, consoante com as disposições desse Edital e seus anexos e pelo Regulamento Interno de Licitações e Contratos do Banco da Amazônia S.A. a empresa *** (razão social), inscrita no CNPJ/MF sob o nº **.***.***/0001-**, sediada em *** (UF), na Rua (Avenida etc) ***, nº *** (endereço completo), por intermédio do seu representante legal, Sr(ª) ***, portador(a) do RG nº ***-SSP/** e do CPF/MF nº ***.***.***-**, abaixo assinado(a), **DECLARA** que: **a)** tem conhecimento do teor do Decreto nº 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da administração pública federal; e **b)** em cumprimento ao citado decreto, não utilizará durante toda a vigência do contrato a ser firmado com o Banco da Amazônia S.A. mão de obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º (terceiro) grau, de agente público que exerça cargo em comissão ou função de confiança no CONTRATANTE.

*(**INDICAR SOMENTE AS UNIDADES ARREMATADAS)**

********* (UF), ******** de 20****.

_____
assinatura do(a) declarante

ANEXO V
PREGÃO ELETRÔNICO N. 90029/2026.

MODELO DE DECLARAÇÃO

MINUTA DE DECLARAÇÃO DE CONHECIMENTO LEI DE IMPROBIDADE ADMINISTRATIVA

(Lei nº 8.429/1992) e a Lei nº 12.846/2013 e seus regulamentos (em conjunto, "Leis Anticorrupção")

Para participar do Pregão Eletrônico nº 90029/2026, cujo objeto é **********, , consoante com as disposições desse Edital e seus anexos e pelo Regulamento Interno de Licitações e Contratos do Banco da Amazônia S.A., a empresa **** (razão social), inscrita no CNPJ/MF sob o nº **.***.***/0001-**, sediada em **** (UF), na Rua (Avenida etc) *****, nº *** (endereço completo), por intermédio do seu representante legal, Sr(ª) *****, portador(a) do RG nº *******-SSP/** e do CPF/MF nº ***.***.***-**, abaixo assinado(a), **DECLARA** que: **a)** tem conhecimento do teor Lei de Improbidade Administrativa (Lei nº 8.429/1992) e a Lei nº 12.846/2013 e seus regulamentos, que dispõe sobre as normas de prevenção à corrupção previstas na legislação brasileira; e b) se comprometem a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores, bem como exigir o seu cumprimento pelos terceiros por elas contratados. Adicionalmente, cada uma das Partes declara que tem e manterá até o final da vigência do contrato um código de ética e conduta próprio, cujas regras se obriga a cumprir fielmente. Sem prejuízo da obrigação de cumprimento das disposições de seus respectivos código de ética e conduta, ambas as Partes desde já se obrigam a, no exercício dos direitos e obrigações previstos no Contrato e no cumprimento de qualquer uma de suas disposições: (i) não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente e (ii) adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados.

********* (UF), ******** de 20**.

PREGÃO ELETRÔNICO N. 90029/2026.
ANEXO VI
MINUTA DO CONTRATO

Contrato n. ...../.....

TERMO DE CONTRATO DE FORNECIMENTO .....QUE ENTRE SI FAZEM O BANCO DA AMAZÔNIA S.A. E A EMPRESA .....

Por este instrumento particular de Contrato, em que são partes, de um lado o Banco da Amazônia S.A., sociedade de economia mista, vinculado ao Governo Federal, com sede em Belém (PA), na Avenida Presidente Vargas, nº 800, Bairro Campina, inscrito no CNPJ/MF sob o nº 04.902.979/0001-44, representado neste ato por seu Gerente de **********, Sr.**********, ********** (nacionalidade), ********** (estado civil), ********** (profissão), portador do RG nº *******SSP/** e do CPF/MF nº ***.***.***-**, domiciliado e residente nesta cidade, doravante denominado CONTRATANTE, e de outro lado a empresa **********, com sede em ********** (UF), na Rua (Avenida, Quadra etc) **********, nº ***, Bairro **********, CEP: nº *****-***, inscrita no CNPJ/MF sob o nº **.***.***/0001-**, representada neste ato por seu ********** (cargo), Sr(ª).********** (nome completo),********** (nacionalidade), ********** (estado civil), ********** (profissão), portador do RG nº *******/SSP-(UF) e do CPF/MF nº ***.***.***-**, doravante denominada CONTRATADA, por este instrumento e na melhor forma de direito, nos termos da decisão do Comitê **********, datada de **/**/2026, ajustam o presente Contrato, nos termos do Edital do Pregão Eletrônico Nº 90029/2026, sujeitando, ainda, as partes às disposições da Lei 13.303/16, de 30.06.2016, do Decreto Federal nº 8.945/2016 e do Regulamento de Licitações e Contratos do Banco da Amazônia S. A. e suas alterações, conforme cláusulas e condições seguintes:

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. Contratação de empresa para prestação de Serviços Gerenciados de Segurança Operacional Cibernética (SOC), no modelo de Cyber Fusion Center (CFC), compreendendo a disponibilização, implementação, integração, operação, sustentação e evolução contínua de solução integrada que contemple, de forma indissociável, as capacidades de Monitoramento e Resposta a Incidentes e Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM), Gestão de Vulnerabilidades (GVUL) e Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS), em regime de alta disponibilidade 24x7x365, incluindo Serviços Técnicos Especializados e capacitação técnica sob demanda, pelo período de 60 (sessenta) meses.

1.2. O presente contrato decorre do processo n. ...../ ....., realizado pelo edital de licitação n. 90029/2026

2 - CLÁUSULA SEGUNDA – ADENDOS

2.1. Fazem parte integrante do presente contrato, como se nele estivessem transcritos, os seguintes adendos:

Adendo 1 – Termo de Referência
Adendo 1 A – Especificações técnicas da Solução completa

Adendo 1 B – Níveis Mínimos de Serviços (NMS)
Adendo 2 – PROPOSTA
Adendo 3 – TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO
Adendo 4 - TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES
Adendo 5 – TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS DE INFORMAÇÕES DO EMPREGADO TERCEIRIZADO
Adendo 6 – MATRIZ DE RISCO

2.1. Este contrato e seus Adendos são considerados como único termo e suas regras deverão ser interpretados de forma harmônica. Em caso de divergência insuperável entre as regras do contrato e de outras condições licitadas, configuradas pelo Edital Pregão Eletrônico nº 90029/2026 e seus documentos anexos e a proposta apresentadas pelo contratado prevalecerá em prol das condições que foram licitadas, preservado o princípio da boa fé objetiva.

3. CLÁUSULA TERCEIRA – PRAZOS

3.1. O prazo de inicio de execução do objeto desta contratação deverá ser de acordo com o especificado no item 4 do Termo de Referência, Adendo 1 deste Contrato, e o prazo de vigência deste contrato é de 60 (sessenta) meses, contados a partir da data da assinatura do contrato.

3.1.1. Os prazos previstos neste Contrato, de execução poderão ser prorrogados, durante a vigência contratual, com a aquiescência da CONTRATADA, por decisão do agente de fiscalização administrativa, por meio de termo aditivo.

4. CLÁUSULA QUARTA – VALOR DO CONTRATO E RECURSOS ORÇAMENTÁRIOS

4.1. Como contrapartida à execução do objeto do presente Contrato, O Banco da Amazônia deve pagar à CONTRATADA o valor global para 60 meses de R$ ====.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA	Preço Unitário (R$)	Preço Global (R$)
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	Mês	60		
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	Mês	60		
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	Mês	60		
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	Serviço	1		
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	UST	5.000		
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	Turma	3 (com 15 participantes cada)		
VALOR GLOBAL DO CONTRATO PARA 60 MESES					

Obs.:	**** Regime contínuo de 24x7x365.***		
	***** Sob demanda, a critério do Banco, mediante Ordem de Serviço.***		

4.1.1. O valor contratado inclui todos os impostos e taxas vigentes na Legislação Brasileira para a execução do objeto desta contratação, e , também, todos os custos diretos e indiretos inerentes, tais como os a seguir indicados, porém sem se limitar aos mesmos: despesas com pessoal (inclusive obrigações sociais, viagens e diárias), despesas administrativas, administração, lucro e outras despesas necessárias a boa realização do objeto desta contratação, isentando O Banco da Amazônia de quaisquer ônus adicionais.

4.2. Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto deste contrato estão previstos no orçamento do Banco da Amazônia :

ITEM	DESCRIÇÃO	RUBRICA
1*	Serviço e Solução Integrada de Monitoramento e Resposta a Incidentes e de Detecção e Resposta Estendidas Baseada em SIEM (XDR baseado em SIEM).	82.559-0
2*	Serviço e Solução Integrada de Gestão de Vulnerabilidades (GVUL).	
3*	Serviço e Solução Integrada de Resposta a Incidentes de Segurança na Primeira Linha de Defesa (SRIS) para suporte à resposta a incidentes, incluindo triagem, contenção, erradicação e recuperação.	
4	Serviço de implantação, integração, migração, homologação e transição operacional do Cyber Fusion Center	82.543-3
5**	Serviços Técnicos Especializados sob demanda, destinados a consultorias, revisões, integrações e customizações de segurança.	82.559-0
6**	Capacitação técnica e treinamentos relacionados às soluções e serviços objeto da contratação (sob demanda).	82.548-4
Obs.:	** Regime contínuo de 24x7x365.*	
	*** Sob demanda, a critério do Banco, mediante Ordem de Serviço.*	

5. CLÁUSULA QUINTA – DA GARANTIA DO CONTRATO

5.1. Para garantia do fiel e perfeito cumprimento de todas as obrigações ora ajustadas, a CONTRATADA deve, dentro de 10 (dez) dias úteis, contados a partir da assinatura do Contrato, apresentar garantia ao Banco da Amazônia, no valor equivalente a 5% (cinco por cento) do valor total desta contratação, que deve cobrir o período de execução do Contrato e estender-se até 3 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação ou renovação contratual e complementada em casos de aditivos e apostilas para reajustes.

5.1.1. A CONTRATADA deve prestar garantia numa das seguintes modalidades:

a) **Fiança Bancária**, acompanhado dos seguintes documentos a seguir listados, para análise e aceitação por parte do Banco da Amazônia:
I - Estatuto Social e ata de posse da diretoria da Instituição Financeira;
II - Quando Procuradores, encaminhar as procurações devidamente autenticadas, com poderes específicos para representar a Instituição Financeira;

III - Balanços Patrimoniais e Demonstração de Resultado dos últimos dois anos, acompanhado das notas explicativas e respectivos pareceres do Conselho de Administração e Auditores Independentes;
IV - Memória de cálculo do Índice de Adequação de Capital (Índice da Basileia) e Índice de Imobilização, comprovando que a instituição financeira está enquadrada no limite estabelecido pelo Banco Central, para comparação e validação com os dados disponíveis no "site" do Banco Central do Brasil (www.bcb.gov.br).

b) **Caução em dinheiro**, valor depositado pela CONTRATADA, no Banco ....., Agência ....., Conta Corrente n. ....., em nome do Banco da Amazônia. A cópia do recibo será entregue ao gestor do contrato.

c) **Seguro Garantia** feito junto à entidade com situação regular no mercado de seguros do Brasil, nos termos estipulados no anexo ao Edital de Licitação, para análise e aceitação por parte do Banco da Amazônia.

5.1.2. A garantia, qualquer que seja a modalidade escolhida, deve assegurar o pagamento de:
a) prejuízos advindos do não cumprimento ou do cumprimento irregular do objeto do presente contrato;

b) prejuízos diretos causados ao Banco da Amazônia decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e compensatórias aplicadas pelo Banco da Amazônia à CONTRATADA; e

d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

5.2. A inobservância do prazo fixado nesta Cláusula para apresentação da garantia acarreta a aplicação de multa de 0,1% (um centésimo por cento) sobre o valor total do Contrato, por dia de atraso, limitada a 2,5% (dois vírgula cinco por cento) sobre o valor total do Contrato.

5.2.1. O atraso superior a 25 (vinte e cinco) dias para a apresentação da garantia autoriza o Banco da Amazônia a:
a) promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações; ou

b) reter o valor da garantia dos pagamentos eventualmente devidos à CONTRATADA até que a garantia seja apresentada.

5.3. A garantia deve ser considerada extinta:

a) com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Banco da Amazônia, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato; ou

b) após 3 (três) meses do término da vigência do presente Contrato.

6. CLÁUSULA SEXTA – EXECUÇÃO DO CONTRATO

6.1. O serviço deverá ser fornecido rigorosamente conforme estabelecido neste Contrato e no Adendo 1 – Termo de Referência, e no edital de licitação 90029/2026 e seus anexos e nas

especificações neles contidas, sendo que a inobservância de qualquer condição poderá acarretar a não aceitação dos mesmos, sem qualquer ônus para O Banco da Amazônia.

6.1.1. A CONTRATADA deverá prestar os serviços especificados no objeto deste instrumento de Contrato, cumprindo todas as obrigações e responsabilidades assim indicadas no Termo de Referência.

6.1.2. O BANCO DA AMAZÔNIA deverá acompanhar e assegurar as condições necessárias para a prestação dos serviços, cumprindo rigorosamente todas as obrigações e responsabilidades assim indicadas no Termo de Referência.

6.2. A CONTRATADA é responsável pelos danos causados direta ou indiretamente ao Banco da Amazônia ou a terceiros em razão da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Banco da Amazônia.

6.3. A gestão do presente Contrato deve ser realizada pela área requisitante do CONTRATANTE. A gestão do contrato abrange o encaminhamento de providências, devidamente instruídas e motivadas, identificadas em razão da fiscalização da execução do contrato, suas alterações, aplicação de sanções, rescisão contratual e outras medidas que importem disposição sobre o contrato.

6.4. A fiscalização da execução do presente Contrato será realizada por agentes de fiscalização da GESEC, que devem ser designados pelo gestor do contrato, permitindo-se designar mais de um empregado e atribuir-lhes funções distintas, como a fiscalização administrativa e técnica, consistindo na verificação do cumprimento das obrigações contratuais por parte da CONTRATADA, com a alocação dos recursos, pessoal qualificado, técnicas e materiais necessários.

6.5. O gestor do contrato pode suspender a sua execução em casos excepcionais e motivados tecnicamente pelo fiscal técnico do Contrato, devendo comunicá-la ao preposto da CONTRATADA, indicando:

a) o prazo da suspensão, que pode ser prorrogado, se as razões que a motivaram não estão sujeitas ao controle ou à vontade do gestor do contrato;

b) se deve ou não haver desmobilização, total ou parcial, e quais as atividades devem ser mantidas pela CONTRATADA;

c) o montante que deve ser pago à CONTRATADA a título de indenização em relação a eventuais danos já identificados e o procedimento e metodologia para apurar valor de indenização de novos danos que podem ser gerados à CONTRATADA.

6.6. Constatada qualquer irregularidade na licitação ou na execução contratual, o gestor do contrato deve, se possível, saneá-la, evitando-se a suspensão da execução do Contrato ou outra medida como decretação de nulidade ou rescisão contratual.

6.6.1. Na hipótese prevista neste subitem, a CONTRATADA deve submeter ao Banco da Amazônia, por escrito, todas as medidas que lhe parecerem oportunas, com vistas a reduzir ou eliminar as dificuldades encontradas, bem como os custos envolvidos. O BANCO DA AMAZÔNIA compromete-se a manifestar-se, por escrito, no prazo máximo de 10 (dez) dias consecutivos, quanto à sua aprovação, recusa ou às disposições por ela aceitas, com seus custos correlatos.

6.7. As partes CONTRATANTES não são responsáveis pela inexecução, execução tardia ou parcial de suas obrigações, quando a falta resultar, comprovadamente, de fato necessário, cujo

efeito não era possível evitar ou impedir. Essa exoneração de responsabilidade deve produzir efeitos nos termos do parágrafo único do artigo 393 do Código Civil Brasileiro.

6.8. No caso de uma das partes se achar impossibilitada de cumprir alguma de suas obrigações, por motivo de caso fortuito ou força maior, deve informar expressa e formalmente esse fato à outra parte, no máximo até 10 (dez) dias úteis contados da data em que ela tenha tomado conhecimento do evento.

6.8.1. A comunicação de que trata este subitem deve conter a caracterização do evento e as justificativas do impedimento que alegar, fornecendo à outra parte, com a maior brevidade, todos os elementos comprobatórios e de informação, atestados periciais e certificados, bem como comunicando todos os elementos novos sobre a evolução dos fatos ou eventos verificados e invocados, particularmente sobre as medidas tomadas ou preconizadas para reduzir as consequências desses fatos ou eventos, e sobre as possibilidades de retomar, no todo ou em parte, o cumprimento de suas obrigações contratuais.

6.8.2. O prazo para execução das obrigações das partes, nos termos desta Cláusula, deve ser acrescido de tantos dias quanto durarem as consequências impeditivas da execução das respectivas obrigações da parte afetada pelo evento.

6.9. A não utilização pelas partes de quaisquer dos direitos assegurados neste Contrato, ou na Lei em geral, ou no Regulamento, ou a não aplicação de quaisquer sanções, não invalida o restante do Contrato, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação ou de ações futuras.

6.10. Qualquer comunicação pertinente ao Contrato, a ser realizada entre as partes contratantes, inclusive para manifestar-se, oferecer defesa ou receber ciência de decisão sancionatória ou sobre rescisão contratual, deve ocorrer por escrito, preferencialmente nos seguintes e-mails:

E-mail Banco da Amazônia - .....
E-mail CONTRATADA - .....

6.10.1. As partes são obrigadas a verificar os e-mails referidos neste subitem a cada 24 (vinte e quatro) horas e, se houver alteração de e-mail ou qualquer defeito técnico, devem comunicar à outra parte no prazo de 24 (vinte e quatro) horas.

6.10.2. Os prazos indicados nas comunicações iniciam em 2 (dois) dias úteis a contar da data de envio do e-mail.

6.11. A execução do presente Contrato e das parcelas do presente Contrato estão condicionadas à expedição, por parte do Gestor de Contrato do Banco da Amazônia, das respectivas ordens de fornecimento dos bens.

7. CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. O BANCO DA AMAZÔNIA, por meio do agente de fiscalização técnica, deve receber o objeto do presente Contrato, forma estabelecida no Adendo 1 deste contrato– Termo de Referência, conforme abaixo:

a) A prestação dos serviços serão recebidas provisoriamente no prazo de 5 (cinco) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo, em conformidade com as especificações e no adendo 1 - Termo de Referência.

b) Os serviços serão recebidos definitivamente no prazo de até 30 dias úteis, contados do recebimento provisório, por empregado, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante Termo de Recebimento,

7.2. Acaso verifique o descumprimento de obrigações por parte da CONTRATADA, o agente de fiscalização técnica ou administrativo deve comunicar ao preposto desta, indicando, expressamente, o que deve ser corrigido e o prazo máximo para a correção DE 10 DIAS ÚTEIS. O tempo para a correção deve ser computado no prazo de execução do Contrato, para efeito de configuração da mora e suas cominações.

7.2.1. Realizada a correção pela CONTRATADA, abrem-se novamente os prazos para os recebimentos estabelecidos nesta Cláusula.

8. CLÁUSULA OITAVA – CONDIÇÕES DE FATURAMENTO E PAGAMENTO

8.1. O pagamento é condicionado ao recebimento definitivo, conforme Cláusula Sétima, e deve ser efetuado conforme Termo de Referência, mediante a apresentação de Nota Fiscal/Documento Equivalente pela CONTRATADA à unidade de gestão de contrato do Banco da Amazônia, que deve conter o detalhamento do objeto executado, o número deste Contrato, a agência bancária e conta corrente na qual deve ser depositado o respectivo pagamento.

8.1.1. O pagamento será efetuado no prazo de até 30 (TRINTA) dias úteis, contados a partir da validação do Relatório de Serviços Prestados (RSP) pela fiscalização do contrato conforme modelo e parâmetros definidos no Anexo I-B – Níveis Mínimos de Serviço (NMS).

8.1.2. A CONTRATADA somente deverá emitir a Nota Fiscal após a aprovação formal do RSP pelos fiscais designados, sendo esta aprovação condição indispensável para a liquidação e o pagamento do valor correspondente.

8.1.3. Caso haja interesse de ambas as partes, o prazo de pagamento, considerada a data do efetivo desembolso, poderá ser reduzido desde que seja concedido o desconte estabelecido pelo Departamento Econômico Financeiro, sendo que a taxa de deságio deverá ser no mínimo equivalente ao CDI (Certificado de Depósito Interbancário), acrescida da taxa de juros de 12% (doze por cento) ao ano.

8.1.3. As faturas que apresentarem erros ou cuja documentação suporte esteja em desacordo com o contratualmente exigido devem ser devolvidas à CONTRATADA pela unidade de gestão de contrato do BANCO DA AMAZÔNIA S.A. para a correção ou substituição. O BANCO DA AMAZÔNIA S.A., por meio da unidade de gestão de contrato, deve efetuar a devida comunicação à CONTRATADA dentro do prazo fixado para o pagamento. Depois de apresentada a Nota Fiscal/Fatura, com as devidas correções, o prazo previsto no subitem acima deve começar a correr novamente do seu início, sem que nenhuma atualização ou encargo possa ser imputada ao BANCO DA AMAZÔNIA S.A..
Havendo controvérsia sobre a execução do objeto, quanto à dimensão, à qualidade e à quantidade, o montante correspondente à parcela incontroversa deverá ser pago no prazo previsto no subitem acima e o relativo à parcela controvertida deve ser retido.

8.3. É vedado o pagamento antecipado.
8.4. É permitido ao BANCO DA AMAZÔNIA S.A. descontar dos créditos da CONTRATADA qualquer valor relativo à multa, ressarcimentos e indenizações, sempre observado o contraditório e a ampla defesa.
8.5. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo BANCO DA AMAZÔNIA S.A., o valor devido deve ser acrescido de atualização financeira, desde

a data do vencimento até a data do efetivo pagamento, à taxa nominal de 6% a.a. (seis por cento ao ano), acrescido dos encargos, calculados da seguinte forma:

EM = I x VP x N

Onde:

EM = Encargos moratórios devidos;
I = Índice de atualização financeira, calculado como: (6 / 100 / 365) = 0,00016438;
VP = Valor da parcela em atraso;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

9. CLÁUSULA NONA – SUBCONTRATAÇÃO

9.1. Será admitida a subcontratação parcial, mediante prévia e expressa autorização do Banco da Amazônia, exclusivamente para atividades específicas, acessórias ou de elevada especialização que não integrem o núcleo operacional contínuo do Cyber Fusion Center.

10. CLÁUSULA DÉCIMA – ALTERAÇÕES INCIDENTES SOBRE O OBJETO DO CONTRATO

10.1. A alteração incidente sobre o objeto do Contrato deve ser consensual e pode ser quantitativa, quando importa acréscimo ou diminuição do objeto do Contrato, ou qualitativa, quando a alteração diz respeito a características e especificações técnicas do objeto do Contrato.

10.1.1. A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do artigo 81 da Lei n. 13.303/2016, devendo observar o seguinte:

a) a aplicação dos limites deve ser realizada separadamente para os acréscimos e para as supressões, sem que haja compensação entre os mesmos;

b) deve ser mantida a diferença, em percentual, entre o valor global do Contrato e o valor orçado pelo Banco da Amazônia, salvo se o fiscal técnico do Contrato apontar justificativa técnica ou econômica, que deve ser ratificada pelo gestor do Contrato;

10.1.2. A alteração qualitativa não se sujeita aos limites previstos nos § 1º e 2º do artigo 81 da Lei n. 13.303/2016, devendo observar o seguinte:

a) os encargos decorrentes da continuidade do Contrato devem ser inferiores aos da rescisão contratual e aos da realização de um novo procedimento licitatório;

b) as consequências da rescisão contratual, seguida de nova licitação e contratação, devem importar prejuízo relevante ao interesse coletivo;

c) as mudanças devem ser necessárias ao alcance do objetivo original do Contrato, à otimização do cronograma de execução e à antecipação dos benefícios sociais e econômicos decorrentes;

d) a capacidade técnica e econômico-financeira da CONTRATADA deve ser compatível com a qualidade e a dimensão do objeto contratual aditado;

e) a motivação da mudança contratual deve ter decorrido de fatores supervenientes não previstos e que não configurem burla ao processo licitatório;

f) a alteração não deve ocasionar a transfiguração do objeto originalmente contratado em outro de natureza ou propósito diverso.

10.2. As alterações incidentes sobre o objeto devem ser:

a) instruídas com memória de cálculo e justificativas de competência do fiscal técnico e do fiscal administrativo do Banco da Amazônia, que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites;

b) as justificativas devem ser ratificadas pelo gestor do Contrato do Banco da Amazônia; e

c) submetidas à área jurídica e, quando for o caso, à área financeira do Banco da Amazônia;

10.3. As alterações contratuais incidentes sobre o objeto e as decorrentes de revisão contratual devem ser formalizadas por termo aditivo firmado pela mesma autoridade que firmou o contrato, devendo o extrato do termo aditivo ser publicado no sítio eletrônico do Banco da Amazônia.

10.4. Não caracterizam alteração do contrato e podem ser registrados por simples apostila, dispensando a celebração de termo aditivo:

a) a variação do valor contratual para fazer face ao reajuste de preços;

b) as atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no Contrato;

c) a correção de erro material havido no instrumento de Contrato;

d) as alterações na razão ou na denominação social da CONTRATADA;

e) as alterações na legislação tributária que produza efeitos nos valores contratados.

11. CLÁUSULA DÉCIMA PRIMEIRA – EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO

11.1. O equilíbrio econômico-financeiro do Contrato deve ocorrer por meio de:

a) reajuste: instrumento para manter o equilíbrio econômico-financeiro do contrato diante de variação de preços e custos que sejam normais e previsíveis, relacionadas com o fluxo normal da economia e com o processo inflacionário, devido ao completar 1 (um) ano a contar da data da proposta;

b) revisão: instrumento para manter o equilíbrio econômico-financeiro do Contrato diante de variação de preços e custos decorrentes de fatos imprevisíveis ou previsíveis, porém com consequências incalculáveis, e desde que se configure álea econômica extraordinária e extracontratual, sem a necessidade de periodicidade mínima.

11.2. O reajuste deve ser concedido de ofício pelo BANCO DA AMAZÔNIA S.A. e deve observar o índice conforme informado no Termo de Referência Adendo 1 deste contrato:

11.3. A revisão deve ser precedida de solicitação da CONTRATADA, acompanhada de comprovação:

a) dos fatos imprevisíveis ou previsíveis, porém com consequências incalculáveis;

b) da alteração de preços ou custos, por meio de notas fiscais, faturas, tabela de preços, orçamentos, notícias divulgadas pela imprensa e por publicações especializadas e outros documentos pertinentes, preferencialmente com referência à época da elaboração da proposta e do pedido de revisão; e
c) de demonstração analítica, por meio de planilha de custos e formação de preços, sobre os impactos da alteração de preços ou custos no total do Contrato.

11.3.1. A revisão que não for solicitada durante a vigência do Contrato considera-se preclusa com a prorrogação ou renovação contratual ou com o encerramento do Contrato.

11.3.2. Caso, a qualquer tempo, a CONTRATADA seja favorecida com benefícios fiscais isenções e/ou reduções de natureza tributárias em virtude do cumprimento do Contrato, as vantagens auferidas serão transferidas ao Banco da Amazônia, reduzindo-se o preço.

11.3.3. Caso, por motivos não imputáveis à CONTRATADA, sejam majorados os gravames e demais tributos ou se novos tributos forem exigidos da CONTRATADA, cuja vigência ocorra após a data da apresentação da Proposta, O Banco da Amazônia absorverá os ônus adicionais, reembolsando a CONTRATADA dos valores efetivamente pagos e comprovados, desde que não sejam de responsabilidade legal direta e exclusiva da CONTRATADA.

11.4. Os pedidos de revisão serão decididos em decisão fundamentada no prazo máximo de 60 (sessenta) dias contados da formalização do requerimento.

11.4.1. O BANCO DA AMAZÔNIA poderá realizar diligências junto à CONTRATADA para que esta complemente ou esclareça alguma informação indispensável à apreciação dos pedidos. Nesta hipótese, o prazo estabelecido neste subitem ficará suspenso enquanto pendente a resposta pela CONTRATADA.

12. CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE

12.3. **Das Obrigações e Responsabilidades da Contratante:**

incluir

12.2. Das Obrigações e Responsabilidades da Contratante:

incluir

13. CLÁUSULA DÉCIMA TERCEIRA – RESCISÃO

13.2. O inadimplemento contratual de ambas as partes autoriza a rescisão, que deve ser formalizada por distrato e antecedida de comunicação à outra parte contratante sobre a intenção de rescisão, apontando-se as razões que lhe são determinantes, dando-se o prazo de 10 (dez) dias úteis para eventual manifestação.

13.3. A parte que pretende a rescisão deve avaliar e responder motivadamente a manifestação referida no subitem precedente no prazo de 10 (dez) dias úteis, comunicando a outra parte, na forma prevista neste Contrato, considerando-se o Contrato rescindido com a referida comunicação.

13.4. Aplica-se a teoria do adimplemento substancial, devendo as partes contratantes ponderar, no que couber, antes de decisão pela rescisão:

a) impactos econômicos e financeiros decorrentes do atraso na fruição dos benefícios do empreendimento;

b) riscos sociais, ambientais e à segurança da população local decorrentes do atraso na fruição dos benefícios do empreendimento;

c) motivação social e ambiental do empreendimento;

d) custo da deterioração ou da perda das parcelas executadas;

e) despesa necessária à preservação das instalações e dos objetos já executados;

f) despesa inerente à desmobilização e ao posterior retorno às atividades;

g) possibilidade de saneamento dos descumprimentos contratuais;

h) custo total e estágio de execução física e financeira do Contrato;

i) empregos diretos e indiretos perdidos em razão da paralisação do Contrato;

j) custo para realização de nova licitação ou celebração de novo Contrato;

k) custo de oportunidade do capital durante o período de paralisação.

13.5. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pela CONTRATADA pode dar ensejo à rescisão contratual, sem prejuízo das demais sanções.

13.5.1. Na hipótese deste subitem, o Banco da Amazônia pode conceder prazo para que a CONTRATADA regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade da CONTRATADA de corrigir a situação.

13.6. Além das hipóteses de rescisão prevista neste contrato dever ser observados o disposto no item 22 do Adendo 1 – Termo de Referência.

14. CLÁUSULA DÉCIMA QUARTA – SANÇÕES ADMINISTRATIVAS

14.2. Pela inexecução total ou parcial do Contrato, o Banco da Amazônia poderá, garantida a prévia defesa, de acordo com o processo administrativo preceituado no artigo 109 do Regulamento, aplicar ao contratado as sanções de advertência ou suspensão temporária de participação em licitação e impedimento de contratar com o Banco da Amazônia por prazo não superior a 2 (dois) anos, que podem ser cumuladas com multa.

14.3. As sanções administrativas devem ser aplicadas diante dos seguintes comportamentos da CONTRATADA:

a) dar causa à inexecução parcial ou total do Contrato;

b) não celebrar o Contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

c) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

d) prestar declaração falsa durante a licitação ou a execução do Contrato;

e) praticar ato fraudulento na execução do contrato;

a) comportar-se com má-fé ou cometer fraude fiscal.

b) praticar atos ilícitos visando a frustrar os objetivos da licitação.

14.4. A sanção de suspensão, referida no inciso III do artigo 83 da Lei n. 13.303/2016, deve observar os seguintes parâmetros:

a) se não se caracterizar má-fé, a pena base deve ser de 6 (seis) meses;

b) caracterizada a má-fé ou intenção desonesta, a pena base deve ser de 1 (um) ano e a pena mínima deve ser de 6 (seis) meses, mesmo aplicando as atenuantes previstas.

14.4.1. As penas bases definidas neste subitem devem ser qualificadas nos seguintes casos:

a) em 1/2 (um meio), se a CONTRATADA for reincidente;

b) em 1/2 (um meio), se a falta da CONTRATADA tiver produzido prejuízos relevantes para O Banco da Amazônia.

14.4.2. As penas bases definidas neste subitem devem ser atenuadas nos seguintes casos:

a) em 1/4 (um quarto), se a CONTRATADA não for reincidente;

b) em 1/4 (um quarto), se a falta da CONTRATADA não tiver produzido prejuízos relevantes para O Banco da Amazônia;

c) em 1/4 (um quarto), se a CONTRATADA tiver reconhecido a falta e se dispuser a tomar medidas para corrigi-la; e

d) em 1/4 (um quarto), se a CONTRATADA comprovar a existência e a eficácia de procedimentos internos de integridade, de acordo com os requisitos do artigo 57 do Decreto n. 11.129/2022.

14.4.3. Na hipótese deste subitem, se não caracterizada má-fé ou intenção desonesta e se a CONTRATADA contemplar os requisitos para as atenuantes previstos nas alíneas acima, a pena de suspensão deve ser substituída pela de advertência, prevista no inciso I do artigo 83 da Lei n. 13.303/2016.

14.5. A CONTRATADA estará sujeita às multas previstas no item 24 do Adendo 1 – Termo de Referência.

14.5.1. O valor das multas apurado, após o processo administrativo, será descontado da garantia, dos pagamentos eventualmente devidos ao Banco, se houver.

14.5.2. Inexistindo pagamento devido ao Banco, ou sendo este insuficiente, caberá à parte contrária efetuar o pagamento do que for devido, no prazo máximo de 10 (dez) dias consecutivos, contados da data da comunicação de confirmação da

multa, em depósito em conta corrente própria em nome do Banco.

14.5.3. Em não se realizando o pagamento nos termos definidos no item acima, far-se-á a sua cobrança judicialmente.

15. CLÁUSULA DÉCIMA QUINTA – RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANCO DA AMAZÔNIA

15.2. Com fundamento no artigo 5º da Lei n. 12.846/2013, constituem atos lesivos ao Banco da Amazônia as seguintes práticas:

a) fraudar o presente Contrato;

b) criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o Contrato;

c) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações deste Contrato, sem autorização em lei, no ato convocatório da licitação pública ou neste instrumento contratual; ou

d) manipular ou fraudar o equilíbrio econômico-financeiro deste Contrato; e

e) realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei n. 12.846/2013, Decreto n. 11.129/2022, Lei n. 13.303/15, ou de quaisquer outras leis ou regulamentos aplicáveis, ainda que não relacionadas no presente Contrato.

15.3. A prática, pela CONTRATADA, de atos lesivos ao Banco da Amazônia, a sujeitará, garantida a ampla defesa e o contraditório, às seguintes sanções administrativas:

a) multa, no valor de 0,1% (um décimo por cento) a 20% (vinte por cento) do faturamento bruto do último exercício anterior ao da instauração do processo administrativo, excluídos os tributos, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação;

b) publicação extraordinária da decisão condenatória.

15.3.1. Na hipótese da aplicação da multa prevista na alínea “a” deste subitem, caso não seja possível utilizar o critério do valor do faturamento bruto da pessoa jurídica, a multa será de R$ 6.000,00 (seis mil reais) a R$ 60.000.000,00 (sessenta milhões de reais).

15.3.2. As sanções descritas neste subitem serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e natureza das infrações.

15.3.3. A publicação extraordinária será feita às expensas da empresa sancionada e será veiculada na forma de extrato de sentença nos seguintes meios:

a) em jornal de grande circulação na área da prática da infração e de atuação do licitante ou, na sua falta, em publicação de circulação nacional;

b) em edital afixado no estabelecimento ou no local de exercício da atividade do licitante, em localidade que permita a visibilidade pelo público, pelo prazo mínimo de 30 (trinta) dias; e

c) no sítio eletrônico do licitante, pelo prazo de 30 (trinta) dias e em destaque na página

principal do referido sítio.

15.3.4. A aplicação das sanções previstas neste subitem não exclui, em qualquer hipótese, a obrigação da reparação integral do dano causado.

15.4. A prática de atos lesivos ao Banco da Amazônia será apurada e apenada em Processo Administrativo de Responsabilização (PAR), instaurado pelo Gestor do Contrato e conduzido por comissão composta por 2 (dois) servidores designados.

15.4.1. Na apuração do ato lesivo e na dosimetria da sanção eventualmente aplicada, o Banco da Amazônia deve levar em consideração os critérios estabelecidos no artigo 7º e seus incisos da Lei n. 12.846/2013.

15.4.2. Caso os atos lesivos apurados envolvam infrações administrativas à Lei n. 13.303/16 ou a outras normas de licitações e contratos da administração pública, e tenha ocorrido a apuração conjunta, o licitante também estará sujeito a sanções administrativas que tenham como efeito restrição ao direito de participar em licitações ou de celebrar contratos com a administração pública, a serem aplicadas no PAR.

15.4.3. A decisão administrativa proferida pela autoridade julgadora ao final do PAR será publicada no Diário Oficial da União.

15.4.4. O processamento do PAR não interferirá na instauração e seguimento de processo administrativo específicos para apuração da ocorrência de danos e prejuízos ao Banco da Amazônia resultantes de ato lesivo cometido pelo licitante, com ou sem a participação de agente público.

15.4.5. O PAR e o sancionamento administrativo obedecerão às regras e parâmetros dispostos em legislação específica, notadamente, na Lei n. 12.846/2013 e no Decreto n. 11.129/2022.

15.5. A responsabilidade da pessoa jurídica na esfera administrativa não afasta ou prejudica a possibilidade de sua responsabilização na esfera judicial.

15.6. As disposições deste item se aplicam quando o licitante se enquadrar na definição legal do parágrafo único do artigo 1º da Lei n. 12.846/2013.

15.7. Não obstante o disposto nesta Cláusula, a CONTRATADA está sujeita a quaisquer outras responsabilizações de natureza cível, administrativa e, ou criminal, previstas neste Contrato e, ou na legislação aplicável, no caso de quaisquer violações.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICIDADE E CONFIDENCIALIDADE

16.1. Quaisquer informações relativas ao presente Contrato, somente podem ser dadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, após autorização, por escrito, do Banco da Amazônia. Para os efeitos desta Cláusula, deve ser formulada a solicitação, por escrito, ao Banco da Amazônia, informando todos os pormenores da intenção da CONTRATADA, reservando-se, ao Banco da Amazônia, o direito de aceitar ou não o pedido, no todo ou em parte.

17. CLÁUSULA DÉCIMA SÉTIMA – POLÍTICA DE RELACIONAMENTO E ANTICORRUPÇÃO

17.1. A CONTRATADA assume o compromisso de deferência a práticas de integridade em todo o encadeamento contratual, com expressa observância aos princípios contidos no Código de Condutas e Integridade do BANCO DA AMAZÔNIA S.A., cuja íntegra esta disponibilizada no site do Banco da Amazônia S.A. (www.bancoamazonia.com.br), bem como no termo de compromisso que integra o presente Contrato.

17.2. O BANCO DA AMAZÔNIA S.A. reserva-se no direito de realizar auditoria na CONTRATADA para verificar sua conformidade com as Leis e o seu Programa Anticorrupção, sendo a CONTRATADA responsável por manter em sua guarda todos os arquivos e registros evidenciando tal conformidade, assim como disponibilizá-los ao BANCO DA AMAZÔNIA S.A. dentro de 5 (cinco) dias a contar de sua solicitação.

18. CLÁUSULA DÉCIMA OITAVA - MATRIZ DE RISCO

18.1. A CONTRATADA e o CONTRATANTE se obrigam a assumir os riscos para prestação do objeto deste Contrato, conforme alocação descrita na **Matriz de Risco** – Adendo 6, deste Contrato.

19. CLÁUSULA DÉCIMA NONA – FORO

19.1. As partes contratantes elegem o foro da Comarca de ....., Estado do ....., para a solução de qualquer questão oriunda do presente Contrato, com exclusão de qualquer outro.

19.2 . E, por estarem justas e contratadas, as partes assinam o presente instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo, para que produzam os efeitos legais, por si e seus sucessores.

..... de .....de 20.....

Pelo Banco da Amazônia:

....

Pela CONTRATADA:

.....

Testemunhas:

1ª.....
Nome:
CPF:

2ª.....
Nome:
CPF:

PREGÃO ELETRÔNICO N. 90029/2026.

ANEXO VII

ADENDO AO CONTRATO

TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO

Por este instrumento particular, a CONTRATADA compromete-se a cumprir integralmente as disposições da Política Anticorrupção, Política de Responsabilidade Socioambiental e da Política de Relacionamento com Fornecedores do Banco da Amazônia da qual tomou conhecimento neste ato por meio da leitura da cópia que lhe foi disponibilizada.

E, para fiel cumprimento desse compromisso, a CONTRATADA declara e garante que nem ela, diretamente ou por intermédio de qualquer subsidiária ou afiliada, e nenhum de seus diretores, empregados ou qualquer pessoa agindo em seu nome ou benefício, realizou ou realizará qualquer ato que possa consistir em violação às proibições descritas (i) na Lei n. 12.846/2013, doravante denominada "Lei Anticorrupção Brasileira", (ii) na Lei Contra Práticas de Corrupção Estrangeiras de 1977 dos Estados Unidos da América (*United States Foreign Corrupt Practices Act of 1977*, 15 U.S.C. §78-dd-1, et seq., conforme alterado), doravante denominada FCPA, (iii) e nas convenções e pactos internacionais dos quais o Brasil seja signatário, em especial a Convenção da OCDE sobre Combate à Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, a Convenção das Nações Unidas contra a Corrupção e a Convenção Interamericana contra a Corrupção – OEA, todas referidas como "Normas Anticorrupção", incluindo pagamento, oferta, promessa ou autorização de pagamento de dinheiro, objeto de valor ou mesmo de valor insignificante mas que seja capaz de influenciar a tomada de decisão, direta ou indiretamente, a:

a) qualquer empregado, oficial de governo ou representante de, ou qualquer pessoa agindo oficialmente para ou em nome de uma entidade de governo, uma de suas subdivisões políticas ou uma de suas jurisdições locais, um órgão, conselho, comissão, tribunal ou agência, seja civil ou militar, de qualquer dos indicados no item anterior, independente de sua constituição, uma associação, organização, empresa ou empreendimento controlado ou de propriedade de um governo, ou um partido político (os itens A a D doravante denominados conjuntamente autoridade governamental);

b) oficial legislativo, administrativo ou judicial, independentemente de se tratar de cargo eletivo ou comissionado;

c) oficial de, ou indivíduo que ocupe um cargo em, um partido político;

d) candidato ou candidata a cargo político;

e) um indivíduo que ocupe qualquer outro cargo oficial, cerimonial, comissionado ou herdado em um governo ou qualquer um de seus órgãos; ou

f) um oficial ou empregado(a) de uma organização supranacional (por exemplo, Banco Mundial, Nações Unidas, Fundo Monetário Internacional, OCDE) (doravante denominado oficial de governo);

g) ou a qualquer pessoa enquanto se saiba, ou se tenha motivos para crer que qualquer porção de tal troca é feita com o propósito de:

g.1.) influenciar qualquer ato ou decisão de tal oficial de governo em seu ofício, incluindo deixar de realizar ato oficial, com o propósito de assistir O Banco da Amazônia ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro;

g.2.) assegurar vantagem imprópria;

g.3) induzir tal oficial de governo a usar de sua influência para afetar ou influenciar qualquer ato ou decisão de uma autoridade governamental com o propósito de assistir O Banco da Amazônia ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro; ou

g.4) fornecer um ganho ou benefício pessoal ilícito, seja financeiro ou de outro valor, a tal oficial de governo.

A CONTRATADA, inclusive seus diretores, empregados e todas as pessoas agindo em seu nome ou benefício, com relação a todas as questões afetando O Banco da Amazônia ou seus negócios, se obrigam a:

a) permanecer em inteira conformidade com as Leis Anticorrupção, e qualquer legislação antissuborno, anticorrupção e de conflito de interesses aplicável, ou qualquer outra legislação, regra ou regulamento de propósito e efeito similares, abstendo-se de qualquer conduta que possa ser proibida a pessoas sujeitas às Leis Anticorrupção;

b) tomar todas as precauções necessárias visando prevenir ou impedir qualquer incompatibilidade ou conflito com outros serviços ou com interesses do Banco da Amazônia, o que inclui o dever de comunicar as relações de parentesco existentes entre os colaboradores da CONTRATADA e do Banco da Amazônia; e

c) observar, no que for aplicável, o Programa de *Compliance* do Banco da Amazônia, sobre o qual declara ter pleno conhecimento.

Entendendo que é papel de cada organização fomentar padrões éticos e de transparência em suas relações comerciais, O Banco da Amazônia incentiva a CONTRATADA, caso ainda não possua, a elaborar e implementar programa de integridade próprio, observando os critérios estabelecidos no Decreto n. 8.420/2015.

Caso a CONTRATADA ou qualquer de seus colaboradores venha a tomar conhecimento de atitudes ilícitas ou suspeitas, especialmente se referentes à violação das Leis Anticorrupção, deve informar prontamente ao Banco da Amazônia, por meio do Canal de Denúncias ..... e no telefone .....

Fica esclarecido que, para os fins do Contrato, a CONTRATADA é responsável, perante O Banco da Amazônia e terceiros, pelos atos ou omissões de seus colaboradores.

Por fim, a CONTRATANTE declara estar ciente de que a fiel observância deste instrumento é fundamental para a condução das atividades inerentes ao Contrato maneira ética e responsável constituindo falta grave, passível de imposição de penalidade, qualquer infração, no disposto deste instrumento.

.....
(Local e Data)

.....
(representante legal)

PREGÃO ELETRÔNICO N. 90029/2026.
ANEXO VIII
TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES

Este Termo de Compromisso é celebrado entre:

BANCO DA AMAZÔNIA, Endereço Avenida Presidente Vargas, 800, Belém, Pará, inscrito no CNPJ/MF 04.902.979/0001-44, neste ato representadas pelo Gestor do Contrato e pelo Fiscal do Contrato, abaixo assinado ("CONTRATANTE"), e a [RAZÃO SOCIAL DA CONTRADA], Endereço [ENDEREÇO DA CONTRATADA], inscrita no CNPJ/MF [CNPJ DA CONTRATADA], neste ato representadas por seus sócios-administradores, na forma de seu contrato social e pelo seu Preposto, todos abaixo assinados ("CONTRATADA"), CONTRATANTE e CONTRATADA em conjunto denominadas como Partes:

CONSIDERANDO QUE as Partes, por meio do contrato [NÚMERO DO CONTRATO] ("Contrato"), estão estabelecendo uma relação jurídica para a prestação de serviços especializados em [OBJETO DO CONTRATO], pela CONTRATADA à CONTRATANTE sendo que para serem executados, necessariamente incluem o acesso, o conhecimento e o tratamento de dados e informações corporativas da CONTRATANTE pela CONTRATADA, além do uso de equipamentos, de recursos computacionais e outros que envolvam a possibilidade de divulgação de informações restritas, de exclusivo interesse da CONTRATANTE, sob a posse, guarda e domínio da CONTRATADA;

CONSIDERANDO QUE as Partes podem divulgar entre si informações classificadas como restritas e/ou sigilosas, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios;

CONSIDERANDO QUE as Partes desejam ajustar as condições de revelação das Informações Restritas e/ou sigilosas, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as Partes celebrar o presente Termo de Compromisso e Sigilo de Dados e Informações ("Termo"), o qual se regerá pelas considerações acima, bem como, **pelas considerações que forem pertinentes constantes na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).**

1. OBJETO

1.1. Este Termo tem por objeto exclusivo proteger as Informações Confidenciais que venham a ser fornecidas ou reveladas pela CONTRATANTE à CONTRATADA, bem como disciplinar a forma pela qual elas devem ser utilizadas pela CONTRATADA.

1.2. Todas as informações ou dados revelados ou fornecidos, direta ou indiretamente, pela CONTRATANTE ou por terceiros em nome desta à CONTRATADA, ou obtida por esta de forma lícita, independentemente de divulgação explícita, em quaisquer meios de

armazenamento ou transmissão e independente do formato, rotulação ou forma de envio, devem ser tratadas como Informações Confidenciais.

1.3. A CONTRATADA reconhece que as Informações Confidenciais são de propriedade exclusiva da CONTRATANTE ou são advindas de terceiros e estão sob sua responsabilidade.

1.4. As Informações Confidenciais poderão estar contidas e serem transmitidas por quaisquer meios, incluindo, entre outros, as formas escritas, gráfica, verbal, mecânica, eletrônica, digital, magnética ou criptográfica.

2. RESTRIÇÕES QUANTO À UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1. A CONTRATADA reconhece a importância de se manter as Informações Confidenciais em segurança e sob sigilo, mesmo após o término de vigência do presente Termo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem prévia autorização da CONTRATANTE, a qualquer terceiro estranho a este Termo.

2.2. Sem prejuízo das demais obrigações previstas neste Termo, a CONTRATADA obriga-se a:

(i) Tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pela CONTRATANTE e preservar o seu sigilo, de acordo com a legislação vigente;

(ii) Preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo ou comercializar a terceiros;

(iii) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;

(iv) Não copiar ou reproduzir, por qualquer meio ou modo: (a) informações classificadas em qualquer grau de sigilo; (b) informações relativas aos materiais de acesso restrito do DA CONTRATANTE salvo autorização da autoridade competente.

(v) Não utilizar, reter, duplicar modificar, adulterar, subtrair ou adicionar qualquer elemento das Informações Confidenciais que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pela CONTRATANTE para finalidades específicas;

(vi) Não modificar ou adulterar as Informações Confidenciais fornecidas pela CONTRATANTE, bem como a não subtrair ou adicionar qualquer elemento a essas Informações Confidenciais;

(vii) Armazenar e transmitir as Informações Confidenciais digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia;

(viii) Devolver à CONTRATANTE, ou a exclusivo critério dessa destruir, todas as Informações Confidenciais que estejam em seu poder em até 48h (quarenta e oito horas), contados da data da solicitação; e

(ix) Informar imediatamente a CONTRATANTE qualquer violação a este Termo.

3. PROTEÇÃO DE DADOS PESSOAIS

3.1. A CONTRATADA obriga-se a, sempre que aplicável, atuar em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física identificada ou identificável ("Dados Pessoais") e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais"), bem como seguir as instruções informadas pela CONTRATANTE quanto ao tratamento dos Dados Pessoais que teve acesso em função do presente Termo.

3.2. A CONTRATADA compromete-se a auxiliar a CONTRATANTE: i) com a suas obrigações judiciais ou administrativas, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e ii) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.

3.3. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da relação estabelecida com a CONTRATANTE ou na execução das atividades ligadas a este Termo, a CONTRATADA deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade da relação negocial conforme as disposições acordadas, a CONTRATADA concorda em notificar formalmente este fato a CONTRATANTE, que terá o direito de resolver a relação negocial sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

4. DISPOSIÇÕES GERAIS

4.1. A CONTRATADA declara estar ciente de que o manuseio inadequado das Informações Confidenciais, sua divulgação ou revelação não autorizada a quaisquer terceiros representarão, por si só, prejuízo ao patrimônio, à imagem e reputação da CONTRATANTE, e implicará em sua responsabilização civil ou criminal, de acordo com a violação verificada, obrigando-se ao ressarcimento das perdas e danos decorrente.

4.2. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a CONTRATADA, além de sanções penais cabíveis, ao pagamento a CONTRATANTE e a terceiros pelas perdas e danos, diretos e indiretos, decorrentes do evento de descumprimento, facultada ainda a CONTRATANTE a rescisão do presente Termo e demais acordos que estiverem vigentes com a CONTRATADA.

4.3. Este Termo não impõe obrigações à CONTRATADA com relação às Informações Confidenciais que (i) já sejam lícita e comprovadamente de conhecimento da CONTRATADA anteriormente à da sua divulgação pela CONTRATANTE; (ii) sejam ou venham a se tornar de conhecimento público, sem qualquer intervenção da CONTRATADA e (iii) sejam divulgadas à CONTRATADA por qualquer terceiro que as detenham em legitima posse, sem que isto constitua violação de dever de confidencialidade previamente assumido com a CONTRATANTE.

4.4. Se a CONTRATADA vier a ser obrigada a divulgar, no todo ou em parte, as Informações Confidenciais por qualquer ordem judicial ou autoridade governamental competente, a CONTRATADA poderá fazê-lo desde que notifique imediatamente a CONTRATANTE, para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4.5. Se a CONTRATADA, na hipótese aqui tratada, tiver que revelar as Informações Confidenciais, divulgará tão somente a informação que foi legalmente exigível e envidará seus melhores esforços para obter tratamento de segredo para quaisquer Informações Confidenciais que revelar, nos precisos dispositivos deste Termo e da lei.

4.6. A CONTRATADA concorda que não deve se opor à cooperação ou empenho de esforços com a CONTRATANTE para auxiliar na adoção das medidas judiciais competentes, sendo certo que nada poderá ser exigido ou solicitado a CONTRATADA que não esteja dentro dos estritos limites legais.

4.7. O presente Termo permanecerá em vigor por prazo indeterminado, independentemente da formalização de qualquer negócio entre as Partes.

4.8. Quaisquer alterações a este Termo somente terão validade e eficácia se forem devidamente formalizadas através de termo aditivo firmado entre as Partes.

4.9. O presente Termo será interpretado pela legislação da República Federativa do Brasil e as Partes desde já elegem o foro da Cidade de Belém, Estado do Pará, para dirimir qualquer controvérsia oriunda deste instrumento, salvo disposição específica pela legislação aplicável.

E, por estarem assim justas e contratadas, as Partes firmam o presente Instrumento em 02 (duas) vias de igual teor e forma.

[Local], XX de XXXX de XXXX.

CONTRATANTE	**CONTRATADA**
_____ **Nome** **Gestor do Contrato**	_____ **Nome** **Socio/Administrador**

Nome **Fiscal do Contrato**	**Nome** **Preposto**

PREGÃO ELETRÔNICO N. 90029/2026.

ANEXO IX

TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DO EMPREGADO TERCEIRIZADO

Eu, [NOME DO EMPREGADO], portador do CPF nº [NÚMERO DO CPF], declaro, como empregado da [RAZÃO SOCIAL DA CONTRATADA], estar ciente de minhas responsabilidades profissionais quanto à segurança dos recursos computacionais e das informações corporativas do Banco da Amazônia S.A., cujos acessos me serão franqueados para desempenho, exclusivo, das funções para as quais fui expressamente contratado e designado.

Por esse termo de responsabilidade e confidencialidade, comprometo-me a:

a) Manter-me atualizado com a Política de Segurança da Informação e Cibernética e demais Políticas Internas e Normas de Segurança do BANCO DA AMAZÔNIA;
b) Manter o sigilo absoluto de minhas senhas de acesso à rede coorporativa e a sistemas, estando ciente que minhas senhas são pessoais e intrasferíveis, cabendo a mim, exclusivamente, a guarda sigilosa, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de minhas senhas;
c) Manter sigilo absoluto de informações do BANCO DA AMAZÔNIA que me sejam franqueados em função da minha atividade profissional;
d) Manter vigilância dos materiais, máquinas, ferramentas e outros pertences de minha propriedade guardados no local dos serviços, quando forem prestados nas dependências do BANCO DA AMAZÔNIA, além de zelar pelos equipamentos, materiais e quaisquer outros recursos de propriedade da DO BANCO DA AMAZÔNIA colocados eventualmente à minha disposição, utilizando-os de maneira correta e cuidadosa e estritamente para os fins do cumprimento das minhas atividades;
e) Manter sigilo das informações do BANCO DA AMAZÔNIA ou de terceiros, classificadas como sigilosas, restritas e internas, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;
f) Não copiar, reproduzir, transferir ou usar indevidamente quaisquer informações do BANCO DA AMAZÔNIA para qualquer outra finalidade que não seja a promoção dos serviços contratados, observando-se o disposto neste termo;
g) Não utilizar, reter ou duplicar as informações que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo BANCO DA AMAZÔNIA;
h) Não transferir as informações corporativas do Banco da Amazônia para outros meios de armazenamento (físicos e nuvem), não autorizados pelo Banco, para fins particulares, sob pena de responsabilização por vazamento de dados;
i) Não utilizar as informações de forma que possa configurar concorrência desleal com o BANCO DA AMAZÔNIA, tampouco explorá-las em outros negócios ou oportunidades comerciais, sem prévia e expressa autorização do BANCO DA AMAZÔNIA;

j) Não comentar, compartilhar ou publicar na Internet ou em mídias sociais, ou qualquer plataforma de armazenagem aberta de dados, como repositórios digitais, quaisquer informações relacionadas à prestação de serviços que tem junto ao BANCO DA AMAZÔNIA a não ser que tenha havido prévia e expressa autorização;
k) Não realizar qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências do BANCO DA AMAZÔNIA, exceto quando relacionada a atividade contratada;
l) Cessar o uso, bem como devolver, imediatamente após o término do Contrato, todos os materiais, informações, documentos, recursos (inclusive crachás, usuários de acesso a sistemas etc.) do BANCO DA AMAZÔNIA que tenham me sido emprestados ou de qualquer forma disponibilizados;
m) Acessar os ambientes do BANCO DA AMAZÔNIA, sejam eles físicos ou lógicos, estritamente para a execução da prestação dos serviços contratados;
n) Respeitar às leis vigentes de direito autoral e Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) bem como as demais leis, normas e políticas de proteção de dados pessoais corporativas;
o) Manter sigilo de dados pessoais cujo BANCO DA AMAZÔNIA figura como controlador ou operador, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;
p) Seguir as instruções recebidas do BANCO DA AMAZÔNIA em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes e aplicáveis, devendo garantir sua licitude e idoneidade;
q) Tratar todos os Dados Pessoais como restritos, exceto se já eram de conhecimento público sem qualquer contribuição sua, ainda que a relação contratual entre as Partes venha a ser resolvida, e independentemente dos motivos que derem causa;
r) Notificar o BANCO DA AMAZÔNIA assim que tomar conhecimento de qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (i) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (ii) de quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (iii) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente;
s) Ter a ciência de que o BANCO DA AMAZÔNIA monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação;
t) Comunicar imediatamente ao meu Gerente imediato ou diretamente ao fiscal do contrato qualquer falha, suspeita ou ameaça por mim detectada aos ativos do BANCO DA AMAZÔNIA, como informações, recursos de tecnologia da informação, ambientes físicos, imagem e reputação;
u) Respeitar às leis vigentes de direito autoral e no que couber, ter como ação os princípios e práticas descritos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no que tange à segurança, a privacidade e o tratamento das informações, bem como, adotar ações no presente para a plena observância da referida lei no momento de sua vigência;

Sendo estas responsabilidades estendidas:

a) Para fora das dependências do BANCO DA AMAZÔNIA e fora dos horários normais de trabalho quando na execução de trabalho remoto, em cliente ou em outra dependência do Banco;
b) Por tempo indeterminado, mesmo após o término da relação profissional da CONTRATADA com o BANCO DA AMAZÔNIA, no que tange a não divulgação e comercialização de informações sigilosas e informações pessoais;

Estou ciente que transgressões destas normas são consideráveis faltas graves e que poderei responder civil e penalmente por quaisquer prejuízos causados ao Banco da Amazônia.

[Local], XX de XXXX de XXXX.

_____

[NOME DO EMPREGADO TERCEIRIZADO]

PREGÃO ELETRÔNICO N. 90029/2026.
ANEXO X
MATRIZ DE RISCO

RISCO	DESCRIÇÃO	CONSEQUÊNCIA	MITIGAÇÃO	RESONSABILIZAÇÃO
Planejamento da Contratação – Pesquisa de Preços	Realização de pesquisa de preços com metodologia inadequada, amostra insuficiente, referências não comparáveis ou valores que não representem adequadamente o objeto, podendo resultar em orçamento estimativo superestimado ou subestimado.	Antieconomicidade, orçamento incompatível com o mercado, propostas inexequíveis ou excessivas, questionamentos pelos órgãos de controle, impugnação, suspensão ou necessidade de repetição do certame.	Utilizar cesta diversificada de preços; analisar contratações públicas comparáveis e propostas de fornecedores; registrar tecnicamente os critérios de inclusão e exclusão das referências; justificar diferenças de escopo e volumetria; revisar e validar o Mapa de Preços antes da publicação do Edital; manter memória de cálculo e documentação que permita a rastreabilidade da formação do orçamento.	Banco da Amazônia
Competitividade – Requisitos Técnicos	Definição involuntária de requisitos técnicos excessivamente específicos ou cuja combinação somente possa ser atendida por número muito restrito de fornecedores.	Restrição à competitividade, redução do número de participantes, direcionamento involuntário do certame, impugnações, representações ou anulação do procedimento.	Realizar chamamento ou consulta pública prévia ao mercado, divulgando os requisitos técnicos relevantes; colher contribuições de potenciais fornecedores; avaliar tecnicamente os	Banco da Amazônia

			questionamentos recebidos; admitir tecnologias e certificações equivalentes sempre que tecnicamente possível; manter requisitos vinculados a necessidades objetivas do Banco e utilizar a POC para validação da solução efetivamente ofertada.	
Competitividade – Subcontratação	Estabelecimento de vedação excessivamente ampla à subcontratação, impedindo a utilização legítima de fabricantes, especialistas ou parceiros para atividades acessórias ou de alta especialização.	Restrição indevida à competitividade e redução do universo de potenciais participantes.	Admitir subcontratação parcial, mediante prévia e expressa autorização do Banco, para atividades específicas, acessórias ou de alta especialização; manter vedada a subcontratação do núcleo operacional permanente do CFC; preservar a responsabilidade integral da CONTRATADA pelos serviços, NMS, segurança, integração e resultados.	Banco da Amazônia
Cronograma do Processo Licitatório	Prazo reduzido entre a retomada/reabertura do processo licitatório e o encerramento do contrato vigente.	Pressão sobre as equipes, redução do tempo disponível para análise, diligências, POC, julgamento,	Manter cronograma crítico atualizado; acompanhar marcos do certame; preservar integralmente os prazos	Banco da Amazônia

		contratação e transição, com risco de decisões açodadas ou descontinuidade dos serviços.	necessários à análise técnica, habilitação, POC e contratação; antecipar providências administrativas e técnicas; estabelecer pontos de controle e escalonamento gerencial; planejar medidas de continuidade legalmente admissíveis caso haja risco concreto de descontinuidade.	
Risco atinente ao Tempo da Execução	Atraso na execução do objeto contratual por ação ou omissão imputável à CONTRATADA.	Atraso da implantação, aumento de custos, comprometimento do cronograma, risco de descontinuidade ou redução temporária da capacidade de segurança.	Plano de Implantação detalhado; cronograma com marcos e responsáveis; acompanhamento contínuo; operação assistida; mecanismos de contingência e rollback; aplicação dos NMS, glosas e sanções previstas contratualmente.	Contratado
Dependências do Banco durante a Implantação	Retardo na disponibilização, pelo Banco, de acessos, informações, ambientes, validações, homologações, aprovações ou demais insumos necessários à implantação.	Atraso de atividades dependentes, extensão do cronograma e impacto sobre a entrada em produção.	Matriz de responsabilidades; cronograma com dependências claramente identificadas; definição de prazos internos de validação; acompanhamento periódico; registro tempestivo das pendências;	Banco da Amazônia

			escalonamento à governança do contrato; replanejamento formal das atividades diretamente impactadas.	
Implantação e Migração Inicial	Falha, atraso ou execução inadequada da migração, integração, homologação ou transição entre o ambiente vigente e o novo CFC, quando decorrente da atuação da CONTRATADA.	Perda de cobertura de monitoramento, indisponibilidade, perda de eventos, falhas em regras de detecção, aumento da exposição a ameaças e atraso do Go-Live.	Plano de Implantação e Transição; prazo e marcos definidos; testes unitários e de integração; UAT; homologação pelo Banco; coexistência temporária quando necessária; plano de rollback; operação assistida; correção e reteste das não conformidades antes do aceite.	Contratado
Disponibilidade da Plataforma SaaS	Indisponibilidade total ou parcial das plataformas, componentes ou serviços SaaS utilizados pelo CFC.	Interrupção ou degradação do monitoramento, detecção, análise, gestão de vulnerabilidades ou resposta a incidentes.	Arquitetura de alta disponibilidade; redundância e contingência geográfica; monitoramento contínuo da disponibilidade; DRP/BCP testados; capacidade de recuperação; NMS de disponibilidade; notificações de incidentes; aplicação de glosas e penalidades previstas.	Contratado
Segurança da Informação e	Incidente de segurança, acesso indevido,	Comprometimento da confidencialidad	MFA; menor privilégio; segregação de	Contratado

Proteção de Dados	vazamento, exposição, alteração ou tratamento irregular de dados provocado por falha, ação ou omissão da CONTRATADA ou de subcontratada autorizada.	e, integridade ou disponibilidade; prejuízo financeiro e reputacional; sanções administrativas e regulatórias; impactos relacionados à LGPD e à regulamentação do CMN/BCB.	funções; credenciais nominativas; criptografia; trilhas de auditoria; monitoramento; termos de confidencialidade ; gestão de vulnerabilidades; notificação tempestiva de incidentes; cooperação na resposta; auditorias e diligências; responsabilização contratual e aplicação das medidas previstas no TR e na legislação.	
Integridade e Retenção de Logs	Perda, exclusão indevida, corrupção, alteração ou indisponibilidade de logs, eventos, evidências ou demais registros, inclusive aqueles mantidos nos 48 meses adicionais de cold storage.	Comprometimento de investigações, auditorias, evidências forenses, rastreabilidade e atendimento regulatório.	Manter 12 meses em camada de consulta imediata e 48 meses adicionais em arquivamento seguro; mecanismos de integridade, imutabilidade e rastreabilidade; exportação automática e segura quando utilizada; verificação periódica da completude e recuperabilidade; cópias sob custódia do Banco quando aplicável; testes de recuperação; auditoria dos processos de retenção e exportação.	Contratado

Dependência Tecnológica – Vendor Lock-in e Portabilidade	Dependência excessiva da solução ou do fornecedor, especialmente para recuperação e transferência dos logs históricos, configurações, regras, playbooks, evidências e dados mantidos em cold storage no encerramento do contrato.	Dificuldade ou atraso na substituição da CONTRATADA, custos adicionais, risco de indisponibilidade, perda de informações ou comprometimento da continuidade operacional.	Plano de saída e transição; obrigação de portabilidade de dados e documentação; exportação em formatos estruturados, documentados e reutilizáveis; fornecimento de dicionário de dados e metadados quando aplicável; definição prévia dos protocolos e mecanismos técnicos de transferência; testes de exportação, restauração e importação; validação de integridade; cronograma de transição; suporte à nova contratada; vedação à retenção dos dados como condição para encerramento.	Compartilhado: Contratado quanto à portabilidade e entrega; Banco quanto ao planejamento, acompanhamento e aceite da transição.
Descontinuidade Tecnológica	Descontinuação, fim de suporte, aquisição, alteração substancial ou encerramento de produto, plataforma, fabricante ou serviço utilizado na solução durante os 60 meses do contrato.	Obsolescência, perda de suporte, redução de funcionalidades, vulnerabilidades não corrigidas, necessidade de migração tecnológica ou indisponibilidade.	Exigir soluções com suporte oficial e ciclo regular de atualização; monitorar avisos de EOL/EOS; obrigação de comunicação antecipada ao Banco; atualização e evolução tecnológica contínuas; substituição por	Contratado

			solução sucessora ou equivalente/superior, mediante prévia aprovação e testes; preservação das integrações, funcionalidades, dados, NMS e continuidade, sem redução das obrigações contratuais.	
Risco Econômico da Proposta – "Jogo de Planilha"	Distribuição artificial ou desequilibrada de preços entre itens heterogêneos em contratação julgada pelo menor preço global, inclusive concentração de margens em itens com maior probabilidade de consumo.	Sobrepreço em itens específicos, vantagem indevida durante a execução, distorção econômica da proposta ou aumento do custo efetivo do contrato.	Julgamento pelo menor preço global associado à análise dos preços unitários e totais de cada item; estabelecimento de valores máximos individualizados; rejeição de item acima do limite estimado; análise de exequibilidade; vedação à compensação ou redistribuição de preços entre itens; pagamento de UST e capacitação exclusivamente pelo efetivamente demandado, autorizado e aceito.	Banco da Amazônia, quanto aos controles de aceitabilidade e julgamento da proposta.
Risco da Atividade Empresarial – Custos Operacionais Ordinários	Elevação ordinária de custos de licenças, subscrições, mão de obra, provedores, infraestrutura em nuvem, processamento,	Redução da margem ou do lucro da CONTRATADA e aumento de seus custos de execução.	Planejamento empresarial e adequada formação da proposta; aplicação exclusivamente do reajuste anual previsto contratualmente,	Contratado, ressalvado o reajuste anual contratualmente previsto.

	armazenamento, suporte ou outros componentes necessários à execução.		pelo ICTI/IPEA, observado o interregno mínimo; vedada transferência automática ao Banco de variações ordinárias dos componentes de custo.	
Risco da Atividade Empresarial – Enquadramento Tributário	Alteração de enquadramento tributário decorrente da situação da empresa ou erro da CONTRATADA na avaliação da incidência tributária aplicável.	Aumento de custos ou redução da margem da CONTRATADA.	Planejamento tributário, avaliação prévia da legislação aplicável e correta composição dos preços da proposta.	Contratado
Risco Cambial Ordinário	Variação ordinária do Real em relação ao Dólar, Euro ou outra moeda estrangeira utilizada pela CONTRATADA para aquisição de licenças, subscrições ou serviços.	Aumento do custo suportado pela CONTRATADA.	Planejamento financeiro, contratação adequada de fornecedores, mecanismos empresariais de proteção cambial quando considerados necessários e adequada composição dos preços ofertados.	Contratado
Risco Extraordinário e Imprevisível	Ocorrência de eventos extraordinários e imprevisíveis, ou previsíveis de consequências incalculáveis, alheios à atuação ordinária das partes, capazes de impactar substancialmente a execução ou os custos do contrato.	Impossibilidade ou dificuldade relevante de execução e eventual ruptura da equação econômico-financeira.	Registro e comprovação do evento; adoção de medidas de contingência; reprogramação formal de atividades quando necessária; análise individualizada de eventual pedido de recomposição do equilíbrio econômico-	Compartilhado, conforme a natureza e a causa do evento e a Matriz de Riscos contratual.

			financeiro, mediante demonstração do evento, excepcionalidade, nexo causal e impacto econômico efetivo.	
Fato imputável ao Banco	Retardamento, suspensão ou determinação do Banco que comprovadamente impeça ou onere a execução contratual, sem causa atribuível à CONTRATADA.	Atraso da execução e eventual impacto econômico comprovado.	Registro formal da ocorrência; reprogramação do cronograma; análise dos impactos; adoção das medidas contratuais cabíveis e eventual recomposição quando presentes os requisitos legais e contratuais.	Banco da Amazônia
Risco Trabalhista e Previdenciário	Responsabilização do Banco da Amazônia por obrigações trabalhistas ou previdenciárias relacionadas aos profissionais utilizados pela CONTRATADA ou por subcontratados autorizados.	Custos trabalhistas, previdenciários, honorários, multas, condenações e outras despesas para o Banco.	Exigência e acompanhamento da regularidade trabalhista e previdenciária; responsabilidade integral da CONTRATADA; ressarcimento, retenção ou compensação de valores quando juridicamente cabível; manutenção das condições de habilitação durante a execução.	Contratado
Risco Tributário e Fiscal	Responsabilização do Banco por recolhimento tributário ou fiscal incorreto decorrente de informação, documento, enquadramento	Débito tributário/fiscal, multas, juros ou necessidade de restituição.	Correta emissão de documentos fiscais; manutenção da regularidade fiscal; conferência das retenções; ressarcimento ou	Contratado

	ou obrigação imputável à CONTRATADA, sem culpa do Banco.		compensação de valores quando juridicamente cabível; obrigação da CONTRATADA de prestar todas as informações tributárias necessárias.	