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 12.846/2013, Decreto Federal nº 8.945/2016, Lei Complementar nº. 123/2006 - Estatuto da ME e EPP, a Lei nº 14.133/2021, IN SEGES 73/2022 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.

O Banco da Amazônia também veda a participação de empresas que estejam sob pena de interdição de direitos previstos na Lei 9.605/1998 (Leis de Crimes Ambientais) em suas licitações.

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 Executiva de Contratações e Gestão de Administração de Contratos - GECOG

Coordenadoria de Processos Licitatórios – COPOL

BANCO DA AMAZÔNIA S.A.
(UASG: 179007)
Diretoria Corporativa
Gerente Executiva de Contratações e Gestão de Administração de Contratos
Coordenadoria de Processos Licitatórios

PREGÃO ELETRÔNICO N. 90008/2026

1. DISPOSIÇÕES PRELIMINARES

1.1. O BANCO DA AMAZÔNIA S.A., através de Pregoeiro, designado pela Ordem de Serviço **Nº 2026/08**, torna público que realizará, nos termos em especial a 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, sob a **forma eletrônica**, pelo critério de julgamento **Menor preço Global**, lote único, cujo objeto está definido no item 2.

Data da sessão pública de abertura: 02/06/2026
Horário: 10h00 (horário de Brasília-DF).
Local: www.gov.br/compras.
Modo de disputa: Aberto.
Critério de julgamento: Menor Preço Global.
Forma de adjudicação: Global.
Regime de execução: Empreitada por preço Global para 5 anos.
Garantia contratual: 5% (cinco por cento) do preço anual pelo período de execução do contrato.
Participação exclusiva de ME/EPP: Não.
Participação de consórcio: Não.
Valor Global estimado: Sigiloso

1.2. O pregão eletrônico será realizado em sessão pública, no sistema de licitações COMPRAS.GOV.BR 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 o fornecimento de solução integrada de rede e segurança voltada à proteção de servidores e cargas de trabalho híbridas, pelo período de 60 (sessenta) meses, abrangendo hardware, software e serviços especializados para implantação de plataforma unificada de proteção cibernética com monitoramento contínuo, detecção, prevenção e resposta a incidentes. A solução deverá integrar, de forma centralizada, camadas de blindagem de vulnerabilidades, análise de ameaças avançadas, detecção e resposta de rede (NDR) e prevenção de intrusão de próxima geração (NGIPS), complementadas por serviço de detecção e resposta gerenciada (MDR) do fabricante. Estão incluídos, ainda, os serviços de instalação, configuração, treinamento operacional e suporte técnico mensal de todas as soluções **CONTRATADAS**, com garantia e atualização contínua de versões, observadas as condições, quantidades e exigências estabelecidas neste Edital e seus Anexos.

2.2. Esta licitação será realizada em **um único lote composto por 12(doze) serviços,** e será adotado o critério de julgamento **Menor Preço Global para 5 anos** e seguirá as regras de apresentação de propostas e lances estabelecidos pelo sistema eletrônico utilizado, composto pelos itens e quantidades descritos na tabela a seguir:

Item	Software	Quant.	Unidade
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas, com detecção e resposta, incluindo garantia e atualização de versões.	1.000	Subscrição
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades.	1.000	Subscrição
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão.	2	Software
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão.	2	Subscrição
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão.	2	Hardware
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas.	2	Subscrição
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS) pelo período de 60 meses.	4	Software
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	4	Hardware
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração.	4	Subscrição
10	Serviço de Instalação das soluções **CONTRATADAS**	3	Serviço
11	Serviços de treinamento das soluções **CONTRATADAS**	3	Treinamento
12	Serviço de suporte mensal das soluções **CONTRATADAS**	60	Serviço

2.3. Os serviços serão executados conforme as especificações técnicas contidas no Anexo I – Termo de Referência, deste Edital e seus anexos.

3. RECURSOS ORÇAMENTÁRIOS

3.1. Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto desta licitação estão previstos no orçamento de despesa do Banco da Amazônia, nas rubricas do orçamento do ano de 2026, conforme a seguir:

Rubricas orçamentárias

Tipo	Descrição	Conta Contábil
Investimento	Equipamentos de process. De dados	26.165-3 / 4103
Dispêndio	Licença de Uso	27.065-2 / 1
Despesa	Execução de Serviços - S/INSS PJ	82.022-9
Treinamento	DESPESAS DE PROCESSAMENTO - TREINAMENTOS P/IMP. INTR. EXTERNO - S/INSS PJ	82.110-1

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 qualquer pessoa 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.

5.2. 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. Os proponentes deverão apresentar declaração de conformidade aos referidos dispositivos, conforme Anexos III,IV, V e VI do presente Edital.

5.2.2. Que estejam cumprindo penalidade que as impeça de licitar e contratar com o Banco da Amazônia, nomeadamente:

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

5.2.2.2. Impedimento de licitar e contratar, previsto no inciso III do art. 83 da lei 13.303/2016;

5.2.2.3. Declaração de inidoneidade 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;

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

5.2.3. 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.

5.2.4. 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.

5.3. 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. Não será admitida a participação de cooperativas na presente licitação.

5.5. Não, será admitida a participação de agentes econômicos reunidos em consórcio, tendo em vista que o objeto da licitação não é de grande complexidade, e que durante a fase de planejamento da contratação se identificou várias empresas no mercado capazes de prestar o serviço, além disso, o valor estimado da contratação não é de grande vulto.

5.6. 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.

5.6.1. 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.

5.7. 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 COMPRAS.GOV.BR 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 01 (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. O 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 o seguinte procedimento:

7.1.1. Publicação do Edital;

7.1.2. Credenciamento no sistema de licitações;

7.1.3. Eventual pedido de esclarecimento ou impugnação;

7.1.4. Resposta motivada sobre o eventual pedido de esclarecimento ou impugnação;

7.1.5. Cadastramento da proposta no sistema de licitações;

7.1.6. Apresentação de propostas e lances;

7.1.7. Verificação de efetividade dos lances ou propostas;

7.1.8. Negociação;

7.1.9. Prova de Conceito;

7.1.10. Julgamento;

7.1.11. Habilitação;

7.1.12. Declaração de vencedor;

7.1.13. Interposição de recurso;

7.1.14. Adjudicação e homologação.

8. CONSULTAS, ADITAMENTOS 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 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, limitado ao último dia útil anterior à data da abertura da sessão pública, para ciência de todas as proponentes.

8.2.1. 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 sítio eletrônico do Banco da Amazônia.

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

8.3. 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.

8.4. As impugnações os pedidos de esclarecimentos não terão em regra, efeito suspensivo, podendo o pregoeiro, motivadamente, conferir-lhes tal efeito.

9. APRESENTAÇÃO DA PROPOSTA NO SISTEMA DE LICITAÇÕES

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

9.1.1. No momento do envio da proposta, o proponente deverá declarar em campo próprio do sistema eletrônico as condições de sua participação, conforme questionário padrão do COMPRAS.GOV.BR

9.1.2. As microempresas e empresas de pequeno porte devem declarar que atendem aos requisitos do artigo 3º da Lei Complementar n. 123/2006, para fazerem jus aos benefícios previstos na referida Lei Complementar. 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.

9.1.3. A declaração falsa sujeitará a proponente às sanções previstas neste Edital.

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

9.2.1. 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.

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

9.2.3. No sistema, **deverá ser cotado preço Global para 05 anos**, 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.

9.2.4. 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.

9.2.5. 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.

9.2.6. O prazo de validade das propostas será de 60 (sessenta) dias, contados da data prevista para abertura dos envelopes, 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- Anexo I deste Edital.

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

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

10.3.5. 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 de **R$ 1.000,00 (hum mil reais)** para todo o item.

10.3.6. 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.

10.3.7. 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.

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

10.4.1. 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.

10.4.2. 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.

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

10.4.4. 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.

10.4.5. 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.

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

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

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

10.5. A presente licitação será julgada pelo critério de julgamento **menor preço Global pelos 5(cinco) anos**, apurado a partir do valor global estimado, nos termos do item 1 do artigo 63 do Regulamento.

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

11.1. Encerrada a etapa competitiva, o Pregoeiro deverá verificar se ocorre o empate ficto em favor de microempresa ou empresa de pequeno porte, assegurando, se for o caso do Certame, o direito de preferência, observando-se o seguinte:
11.2. O empate ficto ocorrerá quando as ofertas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao menor preço, quando este for de proponente que não se enquadre na condição de microempresa ou empresa de pequeno porte;
11.3. Ocorrendo o empate, a microempresa ou a empresa de pequeno porte mais bem classificada, convocada pelo Pregoeiro, poderá, no prazo máximo de 5 (cinco) minutos apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que deve ser adjudicado o objeto em seu favor;
11.4. Se a microempresa ou empresa de pequeno porte melhor classificada não exercer o direito de preferência, deverão ser convocadas as remanescentes que porventura se enquadrem na situação de empate, na ordem classificatória, para o exercício do mesmo direito;
11.5. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem em situação de empate, deve ser realizado sorteio entre elas para que se identifique aquela que primeiro pode apresentar melhor oferta.

11.5.1. Caso a microempresa ou empresa de pequeno porte mais bem classificada deixe de apresentar, no prazo citado no subitem 11.3, nova proposta de preço inferior àquela considerada vencedora do certame ou apresente proposta de preço inaceitável ou deixe de atender às exigências habilitatórias, o Pregoeiro convocará, dentre as empresas remanescentes que porventura se enquadrem na hipótese de empate ficto, na ordem classificatória, a próxima microempresa ou empresa de pequeno porte mais bem classificada para o exercício do mesmo direito de preferência.

11.5.2. O procedimento previsto no subitem 11.5.1 será adotado,

sucessivamente, até a apuração de uma proposta que atenda ao Edital ou até que não haja microempresa ou empresa de pequeno porte que se enquadre na hipótese de empate ficto.

11.6. Na hipótese de não-contratação nos termos previstos no subitem 11.5.1, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame, desde que sua proposta seja aceitável e ele apresente os documentos de habilitação, tudo de acordo com o presente Edital.

12. DESEMPATE

12.1. Nas licitações em que 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:

12.2.1. Produzidos no País;

12.2.2. Produzidos ou prestados por empresas brasileiras;

12.2.3. Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País; e,

12.2.4. Por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

12.3. Persistindo o empate, deverá ser realizado sorteio.

13. VERIFICAÇÃO DA EFETIVIDADE DOS LANCES E PROPOSTAS

13.1. O proponente autor da melhor proposta deverá apresentar, no prazo e modo estipulados pelo Pregoeiro, sua proposta final com o valor equalizado ao seu último lance ofertado, em que deve constar, conforme o caso:

13.1.1. Indicação dos quantitativos e dos custos unitários;

13.1.2. Composição dos custos unitários; e

13.1.3. Detalhamento das Bonificações e Despesas Indiretas (BDI) e dos encargos sociais.

13.1.4. 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. 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.

13.3. 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.

13.3.1. 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.

13.3.2. 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.

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

13.3.4. 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.

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

13.4.1. 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.

13.4.2. 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.

13.4.3. O Pregoeiro deverá conceder prazo adequado, recomendando-se 2 (dois) dias úteis, prorrogáveis por igual período, para que o proponente corrija os defeitos de sua proposta.

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

13.4.5. 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.

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

13.5. 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.

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

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

13.6. Sendo aceitável a proposta, o Pregoeiro convocará o proponente para apresentação dos documentos de habilitação.

14. HABILITAÇÃO

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

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, preferencialmente por funcionalidade disponível no próprio sistema da licitação, na impossibilidade deste meio, por e-mail para licitacoes@basa.com.br ou por meio do SICAF. O Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação mediante a consulta aos seguintes cadastros:

14.2.1. SICAF;

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

14.2.3. 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:

14.2.3.1. Lista de inidôneos do TCU;

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

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

14.3. Caso os resultados das consultas previstas no subitem 14.2 evidenciem a existência de registros impeditivos à contratação do **LICITANTE**, este será inabilitado, ou, inexistindo impedimentos à contratação, o pregoeiro passará a analisar os documentos de habilitação do proponente.

HABILITAÇÃO JURÍDICA.

14.4. Para sua habilitação jurídica, o proponente deve comprovar a possibilidade da aquisição de direitos e da contratação de obrigações por meio de carteira de identificação, contrato social, estatuto social ou outro documento constitutivo compatível com o objeto da licitação, bem como documento que comprova os poderes de seus representantes e decreto de autorização de funcionamento para empresas estrangeiras, conforme exigido neste Edital.

HABILITAÇÃO FISCAL.

14.5. Para fins de Habilitação fiscal, a **LICITANTE** deverá apresentar a documentação de acordo com os documentos abrangidos no SICAF. Caso a documentação do SICAF esteja desatualizada, a empresa deverá enviar os documentos relativos à regularidade fiscal para com a Fazenda Federal, Previdência Social e Fundo de Garantia do Tempo de Serviço – FGTS e trabalhista (certidão emitida pelo Tribunal Superior do Trabalho – TST) pelo próprio sistema COMPRAS.GOV.BR.gov.

HABILITAÇÃO TÉCNICA.

14.6. A comprovação do atendimento ao parâmetro qualificação técnica consistirá nos documentos exigidos **no item 29** - "Dos Critérios de Qualificação Técnica" do Anexo I – Termo de Referência.

14.7. O(s) atestado(s) de capacidade técnica poderá(ão) ser apresentado(s) em nome e com CNPJ da matriz e/ou da(s) filial(is) do **LICITANTE**;

14.8. Somente será aceito atestado expedido após a conclusão do contrato ou se decorrido, pelo menos, 1 (um) ano de sua execução, exceto se firmado para ser executado em prazo inferior;

14.9. 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.

14.10. 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;

14.11. 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.

HABILITAÇÃO ECONÔMICO-FINANCEIRA.

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

14.12.1. 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:

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

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

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

14.12.2. Certidão negativa de feitos sobre falência da sede do interessado.

14.12.3. O proponente que apresentar resultados econômicos iguais ou inferiores a 1 (um) em qualquer dos índices exigidos deverá comprovar que **possui patrimônio líquido ou capital social** equivalente a 10% (dez por cento) do valor total estimado da contratação.

14.12.4. 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.

14.12.5. 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.

14.12.6. O proponente em recuperação judicial ou extrajudicial poderá participar da presente licitação, desde que atenda às condições para comprovação da capacidade econômica e financeira previstas neste Edital.

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

14.13.1. 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);

14.13.2. 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;

14.13.3. 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;

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

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

14.15. 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:

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

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

14.15.3. O Pregoeiro, se for o caso de diligência, deverá 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;

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

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

14.16. Se o proponente desatender às exigências habilitatórias, o Pregoeiro examinará a proposta do proponente subsequente, e se aceita, solicitará os documentos de habilitação, e assim, sucessivamente, até a apuração de proposta e documentação que atenda os termos do Edital, cujo proponente será declarado vencedor.

14.17. 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 Pregoeiro deverá declarar vencedor o proponente autor da melhor proposta que atender todas as condições exigidas neste Edital.

15.2. Declarado o vencedor, durante a sessão pública, qualquer proponente poderá manifestar imediata e motivadamente a intenção de recorrer no prazo de até 30 (trinta) minutos, quando lhe será concedido o prazo de 3 (três) dias úteis para apresentação das razões do recurso, ficando os demais proponentes desde logo intimados para apresentar contrarrazões em igual número de dias, que começam a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

15.2.1. A falta de manifestação imediata e motivada do proponente importará a decadência do direito de recurso e a adjudicação do objeto da licitação pelo Pregoeiro ao vencedor.

15.2.2. Entende-se por manifestação motivada da intenção de recorrer a indicação sucinta dos fatos e das razões do recurso, sem a necessidade de indicação de dispositivos legais ou regulamentares violados ou de argumentação jurídica articulada.

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

15.2.4. 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.

15.3. 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 3 (três) dias úteis, prorrogáveis por iguais períodos, para reavaliar sua decisão e dar os seguintes encaminhamentos, conforme o caso:

15.4.1. 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;

15.4.2. Se não acolher as razões recursais, deverá produzir relatório e encaminhar o recurso para a autoridade competente, para decisão definitiva, que deve ser produzida em 10 (dez) dias úteis, prorrogáveis por iguais períodos. Nesta última hipótese, a autoridade competente deverá tomar a decisão definitiva sobre o recurso.

15.4.2.1. A decisão definitiva sobre o recurso deverá ser publicada no sítio eletrônico do Banco da Amazônia.

15.4.2.2. Na hipótese do subitem 15.4.1, após a publicação da decisão de acolhimento no sítio eletrônico do Banco da Amazônia, 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. ADJUDICAÇÃO E HOMOLOGAÇÃO

16.1. Se não houver recurso, a declaração de vencedor realizada pelo Pregoeiro equivale e faz as vezes da adjudicação, cabendo a homologação à autoridade competente. Se houver recurso, a autoridade competente deverá realizar a adjudicação e homologação da licitação no mesmo ato.

16.2. Na fase de homologação, a autoridade competente poderá:

16.2.1. Homologar a licitação;

16.2.2. Revogar a licitação por razões de interesse público decorrentes de fato superveniente que constitua óbice manifesto e incontornável;

16.2.3. Anular a licitação por ilegalidade, salvo as situações em que:

16.2.3.1. O vício de legalidade for convalidável; ou

16.2.3.2. O vício de legalidade não causar dano ou prejuízo à empresa ou a terceiro; ou

16.2.3.3. O vício de legalidade não contaminar a totalidade do processo de licitação, caso em que deve determinar ao Pregoeiro o refazimento do ato viciado e o prosseguimento da licitação.

16.2.4. O vício de legalidade será convalidável 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.

16.2.5. A revogação ou anulação da licitação, depois da fase de apresentação de lances ou propostas, dependerá da concessão de prazo de 3 (três) dias úteis para que os proponentes interessados ofereçam manifestação.

16.2.6. A revogação ou anulação da licitação, ainda que parcial, deverá ser motivada, abordando-se todos os fundamentos apresentados pelos proponentes que ofereceram manifestação.

17. CONTRATAÇÃO

17.1. 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 VII, e seus adendos decorrentes do Código de Conduta e Integridade da Banco da Amazônia (*consultar no site www.bancoamazonia.com.br*).

17.1.1. 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.

17.1.2. A assinatura poderá ser eletrônica, conforme decisão do gestor do contrato.

17.2. No momento da assinatura do contrato o Banco realizará:

17.2.1. 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 22024, alterada pela Lei nº 14.973 de 2024;

17.2.2. Consulta 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

17.3. 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.

17.3.1. 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.

17.4. Todas as disposições sobre o contrato estão previstas no Anexo VII – Minuta de Instrumento Contratual, deste Edital.

18. SANÇÕES ADMINISTRATIVAS

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

18.1.1. 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;

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

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

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

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

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

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

18.2. 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 e suas subsidiárias, por prazo não superior a 2 (dois) anos, de acordo com os critérios do Artigo 109 do Regulamento.

18.3. As penalidades referentes à inexecução do Contrato estão estabelecidas no Termo de Referência Anexo I e Anexo VII – Minuta de Instrumento Contratual, deste Edital.

18.1 RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANCO DA AMAZÔNIA

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

18.1.1. Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo do procedimento licitatório;

18.1.2. Impedir, perturbar ou fraudar a realização de qualquer ato do procedimento licitatório;

18.1.3. Afastar ou procurar afastar proponente, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

18.1.4. Fraudar a licitação ou contrato dela decorrente;

18.1.5. Criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação ou celebrar contrato administrativo;

18.1.6. Obter vantagem ou benefício indevido, por meio fraudulento, de modificações no ato convocatório da licitação;

18.1.7. Manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados.

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

18.2.1. 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;

18.2.2. Publicação extraordinária da decisão condenatória.

18.3. Na hipótese da aplicação da multa prevista no subitem 19.2.1, 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).

18.3.1. 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.

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

18.3.2.1. 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;

18.3.2.2. 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

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

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

18.4. 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.

18.4.1. 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.

18.4.2. 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.

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

18.4.4. 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.

18.4.5. 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, inclusive suas eventuais alterações, sem prejuízo ainda da aplicação do ato de que trata o artigo 21 do Decreto n. 11.129/2022.

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

18.6. 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.

19. DISPOSIÇÕES FINAIS

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

19.2. 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.

19.3. 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).

19.4. 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.

19.5. 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.

19.6. Fazem parte integrante deste Edital os seguintes Anexos:

ANEXO I: TERMO DE REFERÊNCIA
ANEXO I A: **ESPECIFICAÇÕES TÉCNICAS**
ANEXO I B: DEMANDA DE SERVIÇOS
ANEXO I C: ACORDO DOS NÍVEIS DE SERVIÇO
ANEXO I D: GARANTIA E ASSISTÊNCIA TÉCNICA
ANEXO I E: REQUISITOS PARA SUPORTE REDE E SEGURANÇA
ANEXO I F: MATRIZ DE TESTES DA PROVA DE CONCEITO (POC)
ANEXO II: CARTA DE APRESENTAÇÃO DE PROPOSTA
ANEXO III, IV, V e VI: DECLARAÇÕES
ANEXO VII: MINUTA DE INSTRUMENTO CONTRATUAL
ANEXO VIII: TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO
ANEXO IX: TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES
ANEXO X: MATRIZ DE RISCO
ANEXO XI: REQUISITOS TÉCNICOS OBRIGATÓRIOS

19.7. 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, 12 de maio de 2025.

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

PREGÃO ELETRÔNICO 90008/2026

ANEXO I

1. DEFINIÇÃO DO OBJETO

1.1. Contratação de empresa, nos termos da Lei nº 13.303/2016, cujo objeto é o fornecimento de solução integrada de rede e segurança voltada à proteção de servidores e cargas de trabalho híbridas, pelo período de 60 (sessenta) meses, abrangendo hardware, software e serviços especializados para implantação de plataforma unificada de proteção cibernética com monitoramento contínuo, detecção, prevenção e resposta a incidentes. A solução deverá integrar, de forma centralizada, camadas de blindagem de vulnerabilidades, análise de ameaças avançadas, detecção e resposta de rede (NDR) e prevenção de intrusão de próxima geração (NGIPS), complementadas por serviço de detecção e resposta gerenciada (MDR) do fabricante. Estão incluídos, ainda, os serviços de instalação, configuração, treinamento operacional e suporte técnico mensal de todas as soluções **CONTRATADAS**, com garantia e atualização contínua de versões, observadas as condições, quantidades e exigências estabelecidas neste Termo de Referência e seus Anexos, sendo a contratação realizada pelo critério de menor preço global, a saber:

Item	Software	Quant.	Unidade
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas, com detecção e resposta, incluindo garantia e atualização de versões.	1.000	Subscrição
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades.	1.000	Subscrição
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão.	2	Software
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão.	2	Subscrição
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão.	2	Hardware
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas.	2	Subscrição
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS) pelo período de 60 meses.	4	Software
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	4	Hardware
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração.	4	Subscrição
10	Serviço de Instalação das soluções **CONTRATADAS**	3	Serviço
11	Serviços de treinamento das soluções **CONTRATADAS**	3	Treinamento
12	Serviço de suporte mensal das soluções **CONTRATADAS**	60	Serviço

2. FORMA DE FORNECIMENTO E MODO DE DISPUTA

2.1. Forma de fornecimento: o fornecimento do objeto será integral.
2.2. O Modo de Disputa será aberto.

3. FORMA DE SELEÇÃO DO FORNECEDOR E CRITÉRIO DE JULGAMENTO DA 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.

3.2. O critério de avaliação desta licitação será feito pelo critério de “Menor Preço” Global, observadas todas as demais condições deste Termo de Referência, na forma da lei.

3.3. Caso licitação, Ata de Registro de preços? Não.

3.4. Caso licitação, seleção em lote único de acordo com o item 1.1 deste termo de referência.

3.5. A solução a ser **CONTRATADA** constitui um ecossistema integrado de blindagem de vulnerabilidades, detecção e resposta a ameaças avançadas, NDR, NGIPS e MDR. Esses módulos dependem de console única, correlação nativa de eventos, trilhas de auditoria unificadas e resposta coordenada a incidentes. A divisão em lotes distintos comprometeria a interoperabilidade, a rastreabilidade e a responsabilização contratual, dificultando a manutenção dos níveis mínimos de serviço e a efetividade operacional da defesa cibernética do Banco. A modelagem em lote único elimina zonas cinzentas de suporte entre fornecedores, reduz o risco de incompatibilidade técnica entre camadas, preserva a governança centralizada e é a alternativa técnica e economicamente mais justificada. Esta justificativa está detalhada nos itens 3.33 e 3.44 do Estudo Técnico Preliminar, anexado a este Termo de Referência, e atende à orientação do TCU quanto à motivação para não parcelar.

3.6. O julgamento das propostas será por lote único para melhor gestão dos contratos, pois os serviços serão executados por um único fornecedor e tendo em vista a complexidade de realizar a divisibilidade do objeto da licitação por tratar-se de prestação de serviços, bem como deverá ser considerada vencedora a empresa que apresentar o menor preço global, desde que atendidos os requisitos previstos neste Termo de Referência e mediante a apresentação da Planilha de Composição de Custos e Formação de Preços, **Anexo VI-C**.

3.7. Para efeito de julgamento, os lances ofertados e deverão obedecer à seguinte composição de preço:

PREÇO GLOBAL = (preço unitário do serviço X quantidade).

3.7.1. A proposta apresentada de acordo com o modelo do **ANEXO II** e os lances formulados deverá indicar preço global para os serviços, incluindo o fornecimento de todas as especificações e condições do projeto conforme os anexos deste termo de referência, além da assistência técnica durante o período de garantia de sessenta meses, treinamento e o suporte técnico. Os Valores deverão ser expressos em real, contendo no máximo 02 (duas) casas decimais.

4. PRAZO DE EXECUÇÃO/ENTREGA DO OBJETO DA CONTRATAÇÃO

4.1. O prazo para implantação dos serviços será listado na tabela abaixo sendo que todos os prazos são firmados a contar da data de assinatura do contrato:

Item	Software	Quant.
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão	60 dias
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades.	60 dias
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão.	60 dias

4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão.	60 dias
5	Camada de hardware para solução de análise de ameaças avançadas, incluindo atualização de versão.	60 dias
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas.	60 dias
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	60 dias
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	60 dias
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração.	60 dias
10	Serviço de Instalação das soluções **CONTRATADAS**	60 dias
11	Serviços de treinamento das soluções **CONTRATADAS**	60 dias
12	Serviço de suporte mensal das soluções **CONTRATADAS**	60 dias

4.2. Todos os prazos da tabela acima são limites; serviços podem ser entregues antes, mas o descumprimento acarretará multas conforme este Termo de Referência.

4.3. A implantação dos novos serviços deverá ser sincronizada com a desinstalação da rede atual, onde a **CONTRATANTE** fará a gestão dos contratos de modo a garantir que nenhum dos sites atuais da rede fique sem atendimento

4.4. A **CONTRATADA** deverá apresentar o Projeto Executivo e o Plano de Implantação em no máximo 15 dias consecutivos, contados a partir da assinatura do contrato.

4.5. O Projeto Executivo e o Plano de Implantação deverão ser aprovados pela **CONTRATANTE**.

4.6. Em caso de rejeição (primeira) do Plano de Implantação pela **CONTRATANTE**, a **CONTRATADA** deverá reapresentá-lo com as devidas correções/adequações em, no máximo, 5 (cinco) dias consecutivos a partir de sua rejeição.

4.7. O detalhamento do Plano de Implantação deverá conter, no mínimo, a descrição de:

4.7.1. Cronograma detalhado ao nível de atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência, identificando o marco de conclusão destas atividades durante o processo de implantação;

4.7.1.1. Plano de Testes – com cronograma distinto e pormenorizado – a ser utilizado como roteiro para a aceitação dos serviços definidos neste Termo de Referência;

4.7.1.2. Plano de Migração – com cronograma distinto e pormenorizado – da atual rede corporativa da **CONTRATANTE** para a solução proposta pela **CONTRATADA**; IV. Topologias da rede (física e lógica).

4.7.1.3. O Plano de Migração deverá prever a conectividade temporária entre a atual rede corporativa da **CONTRATANTE** e a solução proposta pela **CONTRATADA**, garantindo a migração dos serviços existentes.

4.7.2. O Plano de Testes consiste num documento onde deverão estar descritos todos os procedimentos a serem realizados pela **CONTRATANTE** ou seu preposto, com a finalidade de verificar as funcionalidades dos serviços contratados e as suas consequentes aceitações.

4.7.3. Com a finalidade exclusiva de facilitar e padronizar a instalação dos serviços pela **CONTRATADA** ou seu preposto, deverá prever no Plano de Testes um modelo de tabela, contemplando cada serviço contratado.

4.7.4. Na tabela anteriormente mencionada, para cada procedimento de instalação a ser realizado pela **CONTRATADA**, deverá conter os resultados esperados em conformidade como especificado neste Termo de Referência.

4.7.5. Os procedimentos descritos no Plano de Testes serão realizados no momento da aceitação dos serviços pela **CONTRATANTE** ou seu preposto, após a instalação e configuração dos serviços pela **CONTRATADA**.

4.7.5.1. A **CONTRATADA** deverá apresentar, semanalmente, relatórios de acompanhamento das atividades, nos quais deverão constar as atividades realizadas e a duração de cada atividade.

4.7.5.2. A **CONTRATADA** deverá documentar, em forma de relatório, os estados da infraestrutura física antes e depois das instalações realizadas.

4.7.5.3. Este relatório deverá ser entregue para a **CONTRATANTE** para a aceitação do serviço.

4.8. Caso não seja possível o cumprimento do prazo estabelecido, a **CONTRATADA** deverá comunicar formalmente as razões com antecedência mínima de 10 (dez) dias corridos, sob pena de aplicação das penalidades previstas neste Termo de referência, ressalvadas situações de caso fortuito e força maior, devidamente justificadas e aceitas pela **CONTRATANTE**

5. JUSTIFICATIVAS/FUNDAMENTAÇÃO DA CONTRATAÇÃO

5.1. A presente contratação está fundamentada no Estudo Técnico Preliminar elaborado pela equipe técnica do Banco da Amazônia, que analisou detalhadamente os aspectos técnicos, operacionais, estratégicos e financeiros da solução proposta, considerando os seguintes pontos:

I. A contratação tem como base o **Estudo Técnico Preliminar – Solução Integrada de Rede e Segurança**, que apresenta a descrição detalhada do objeto, a análise de viabilidade técnica e econômica, as justificativas qualitativas e quantitativas, a matriz de riscos, o levantamento de mercado e a comparação de alternativas, demonstrando a necessidade e a oportunidade da contratação.

II. Trata-se da **continuidade da estratégia institucional de fortalecimento da infraestrutura tecnológica e de segurança cibernética** do Banco da Amazônia, iniciada na década de 2000 e consolidada por meio de contratações cíclicas de soluções de proteção e monitoramento corporativo. A nova contratação representa a evolução para uma arquitetura unificada e inteligente, com integração entre as camadas de detecção, prevenção e resposta a incidentes.

III. A **não contratação** da solução implicaria riscos elevados à **continuidade operacional** do Banco, incluindo exposição a ataques cibernéticos, falhas de monitoramento, indisponibilidade de sistemas críticos (core bancário, Internet Banking, PIX e SPB) e descumprimento de exigências regulatórias, com potenciais impactos financeiros e reputacionais significativos.

IV. A contratação visa assegurar a **modernização da infraestrutura de segurança da informação**, consolidando uma **plataforma integrada de rede e segurança** capaz de ampliar a visibilidade sobre ameaças, automatizar respostas a incidentes, proteger ambientes híbridos (on-premises e nuvem) e garantir a **resiliência cibernética e a conformidade com a LGPD e as normas do Banco Central**.

V. Os **resultados esperados** incluem: maior eficiência na detecção e mitigação de ameaças, **redução do tempo médio de detecção e resposta (MTTD/MTTR)**, **governança centralizada**, **monitoramento contínuo 24x7x365**, **atualização automática de assinaturas e versões**, além de **disponibilidade mínima de 99,7%** nos ambientes críticos.

VI. A contratação foi considerada **plenamente viável sob os aspectos técnico, operacional e econômico**, apresentando o **melhor custo-benefício** e reduzindo o custo total de propriedade (TCO), conforme demonstrado na análise comparativa do ETP. A adoção do **modelo full-solution**, com

integração completa de hardware, software e serviços MDR do fabricante, assegura eficiência operacional, rastreabilidade e governança unificada.

VII. A solução será **CONTRATADA** em **lote único**, conforme justificativa técnica apresentada no ETP, em razão da **interdependência entre as camadas de proteção, detecção, prevenção e resposta**, que exigem integração nativa e gestão centralizada. A fragmentação comprometeria a coerência técnica da arquitetura, a interoperabilidade e a eficácia da segurança.

5.2. 5.Esta contratação está alinhada com os instrumentos estratégicos e normativos do Banco da Amazônia, conforme descrito abaixo:

I. **Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2024–2025**, aprovado pela Portaria nº 239/2023 – GABIN, especialmente aos objetivos **OE-07** e **OE-08**, que tratam da modernização da infraestrutura tecnológica, da ampliação da resiliência cibernética e da continuidade operacional dos serviços de TI.

II. **Alinhamento ao Planejamento Estratégico 2023–2030** do Banco da Amazônia, que estabelece como pilares a inovação, a segurança, a sustentabilidade e a excelência operacional. A implantação da Solução Integrada de Rede e Segurança contribui diretamente para a consolidação da **transformação digital** e o fortalecimento da **infraestrutura tecnológica e de governança** da instituição.

III. **Conformidade com o normativo interno NP 025 – Processo de Seleção e Aquisição de Serviços e Produtos de TI**, assegurando a aderência às diretrizes de **governança institucional**, **planejamento estratégico** e **práticas de contratação pública de tecnologia da informação** previstas na Lei nº 13.303/2016 e nas políticas internas do Banco da Amazônia.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO E DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

6.1. A solução **CONTRATADA** consiste na implantação de uma plataforma integrada de rede e segurança, composta por camadas complementares de proteção, detecção, prevenção e resposta cibernética, abrangendo os módulos de blindagem de vulnerabilidades, detecção e resposta de rede (NDR), prevenção de intrusão de próxima geração (NGIPS) e serviço de detecção e resposta gerenciada (MDR). A arquitetura da solução foi projetada para oferecer proteção de ponta a ponta, visibilidade total do tráfego e integração unificada entre ambientes físicos, virtuais e em nuvem, assegurando a resiliência e a continuidade das operações tecnológicas do Banco da Amazônia.

6.2. A plataforma deverá operar de forma centralizada e automatizada, por meio de console única de gerenciamento, permitindo monitoramento contínuo 24x7x365, correlação inteligente de eventos, análise comportamental e resposta automatizada a incidentes, com utilização de mecanismos de inteligência artificial e machine learning. Deverá assegurar alta disponibilidade (HA) entre datacenters, redundância de componentes críticos, balanceamento dinâmico de carga e replicação segura de dados, garantindo níveis mínimos de disponibilidade de 99,7%.

6.3. A arquitetura da solução incluirá os seguintes componentes principais:

6.3.1. Blindagem de Vulnerabilidades: módulo responsável pela descoberta automática de vulnerabilidades, aplicação de virtual patching, análise contínua de integridade e conformidade, e integração nativa com ambientes híbridos (on-premises e nuvem), compatível com VMware, AWS, Azure e Google Cloud.

6.3.2. Detecção e Resposta de Rede (NDR): sensores dedicados com capacidade mínima de inspeção de 20 Gbps, atuando em modo espelhado ou inline, com inspeção profunda de pacotes (DPI), análise comportamental, detecção de tráfego criptografado (TLS), identificação de anomalias, atividades suspeitas e comunicações de comando e controle (C&C).

6.3.3. Prevenção de Intrusão de Próxima Geração (NGIPS): dispositivos de hardware dedicados com throughput mínimo de 40 Gbps, operando em alta disponibilidade, com suporte a inspeção SSL/TLS, controle granular de aplicações, detecção de exploits e ataques avançados, aplicação automática de assinaturas e filtros comportamentais.

6.3.4. Serviço de Detecção e Resposta Gerenciada (MDR): serviço provido pelo fabricante, com operação 24x7x365, equipe especializada para análise de alertas, caça ativa de ameaças (threat hunting), correlação de eventos, resposta a incidentes e emissão de relatórios mensais de desempenho e segurança.

6.3.5. Camada de Gerenciamento Unificado: console central para administração, correlação e auditoria de todos os módulos da solução, com autenticação multifator (MFA), dashboards analíticos personalizáveis, relatórios técnicos e executivos, alarmes automáticos, registro de logs e integração com sistemas corporativos de SIEM e SOAR.

6.3.6. Infraestrutura de Hardware e Software Integrada: fornecimento completo de appliances, servidores e licenças, com atualização automática de versões e assinaturas, garantia de funcionamento por 60 (sessenta) meses e suporte técnico especializado para todos os componentes da solução.

6.4. Todos os serviços deverão ser prestados de forma ininterrupta (24x7x365), com suporte técnico remoto e local, monitoramento proativo, atendimento multilíngue, substituição imediata de equipamentos em caso de falha (RMA) e atendimento conforme os Acordos de Nível de Serviço (SLA) definidos no contrato.

6.5. A **CONTRATADA** será responsável por toda a operação fim a fim da solução, incluindo fornecimento, instalação, configuração, ativação, homologação, treinamento técnico, suporte mensal, substituição de componentes, garantia e documentação técnica atualizada, observando as exigências do Banco da Amazônia e as recomendações do fabricante.

6.6. As especificações técnicas detalhadas encontram-se descritas no **Anexo I A** – Especificações Técnicas do Termo de Referência, que integra o presente documento para todos os fins.

7. PROVA DE CONCEITO (POC)

7.1. Será realizada Prova de Conceito (PoC) com a **LICITANTE** provisoriamente classificada em primeiro lugar, após a fase de julgamento e antes da adjudicação do objeto, com a finalidade de comprovar, de forma prática, objetiva, verificável e mensurável, a aderência da solução ofertada aos requisitos técnicos essenciais previstos no Edital, neste Termo de Referência, no Anexo I A – Especificações Técnicas e no Anexo I F – Matriz de Testes da Prova de Conceito (PoC).

7.2. A PoC constitui etapa de validação técnica da solução ofertada e terá por objeto a verificação funcional, técnica e de integração da solução, especialmente quanto aos requisitos críticos de arquitetura integrada, interoperabilidade, visibilidade operacional, correlação de eventos, geração de alertas, investigação, resposta, trilhas de auditoria, relatórios, integrações corporativas e gerenciamento centralizado.

7.3. A PoC não se destina à mera apresentação comercial, demonstração conceitual, exposição institucional ou promessa de implementação futura, devendo demonstrar, em ambiente controlado e por meio de roteiro formal de testes, o funcionamento real das funcionalidades mínimas exigidas para a execução do objeto.

7.4. A convocação para a PoC será realizada pelo Pregoeiro, observada a ordem de classificação, e indicará, no mínimo:

a) data, horário e local de realização;
b) prazo para início da demonstração;
c) duração estimada da sessão;
d) matriz de testes, cenários e evidências esperadas;
e) requisitos que serão validados;
f) critérios objetivos de aceitação e reprovação;
g) composição da comissão técnica responsável pela avaliação.

7.5. A PoC será conduzida por comissão técnica formalmente designada pela **CONTRATANTE**, composta por representantes das áreas técnica e demandante, podendo contar com apoio da área de segurança da informação, da fiscalização contratual ou de outros profissionais tecnicamente habilitados.

7.6. Compete à comissão técnica conduzir a sessão de PoC, acompanhar a execução dos testes, verificar as evidências apresentadas, registrar os resultados obtidos e elaborar relatório circunstanciado de aprovação ou reprovação da solução ofertada.

7.7. Os demais **LICITANTE**s poderão acompanhar a realização da PoC na condição de ouvintes, vedada qualquer interferência na condução dos testes, assegurado o registro formal do resultado e das evidências produzidas.

7.8. A **LICITANTE** convocada deverá disponibilizar, sem ônus para a **CONTRATANTE**, todos os recursos necessários à realização da PoC, inclusive licenças temporárias, equipamentos, appliances, imagens, módulos, acessos, credenciais, templates, documentação técnica, integrações, equipe técnica especializada e demais insumos indispensáveis à execução do roteiro de testes.

7.9. A solução apresentada na PoC deverá corresponder à solução ofertada na proposta comercial e técnica da **LICITANTE**, sendo vedada a substituição de fabricante, arquitetura, componentes essenciais, console de gerenciamento, módulos principais ou modelo de integração informado na proposta.

7.10. Serão admitidos apenas ajustes meramente operacionais relacionados ao ambiente de testes, desde que previamente aceitos pela comissão técnica, devidamente registrados no relatório da PoC e sem alteração substancial da solução ofertada, sem prejuízo da isonomia e da vinculação ao instrumento convocatório.

7.11. A PoC será realizada com base nos procedimentos, roteiro mínimo, matriz de testes, evidências esperadas, critérios de avaliação e condições de aprovação e reprovação previstos no Anexo I F – Matriz de Testes da Prova de Conceito (PoC), que integra este Termo de Referência para todos os fins.

7.12. Cada caso de teste será avaliado com resultado expresso de “ATENDE” ou “NÃO ATENDE”, vedada avaliação genérica, subjetiva, intermediária ou dissociada das especificações do Edital, deste Termo de Referência e de seus anexos.

7.13. A validação da PoC ocorrerá exclusivamente com base no que for efetivamente demonstrado durante a sessão, não sendo admitida, para fins de aprovação, a simples declaração unilateral da **LICITANTE**, roadmap de produto, funcionalidade futura, customização não implementada ou correção posterior de requisito crítico não atendido.

7.14. Serão considerados requisitos críticos aqueles assim classificados no Anexo I F, especialmente os relacionados à arquitetura integrada, console de gerenciamento, correlação nativa de eventos, visibilidade centralizada, geração de alertas, investigação, resposta, integração entre camadas, trilhas de auditoria, integrações corporativas e aderência aos serviços do fabricante, quando aplicável.

7.15. A PoC será considerada aprovada somente se a **LICITANTE** atender a 100% (cem por cento) dos casos de teste classificados como críticos e, cumulativamente, atingir o percentual mínimo global de aprovação estabelecido no Anexo I F.

7.16. O não atendimento de qualquer caso de teste classificado como crítico implicará reprovação da PoC e consequente desclassificação da **LICITANTE** provisoriamente classificada em primeiro lugar, convocando-se a **LICITANTE** subsequente, observada a ordem de classificação, para submissão ao mesmo procedimento.

7.17. Também será reprovada a **LICITANTE** que deixar de comparecer à sessão de PoC, não disponibilizar os recursos necessários à realização da prova, não demonstrar os requisitos exigidos ou não alcançar o percentual mínimo global de aprovação definido no Anexo I F.

7.18. Não será admitida a correção posterior de falhas substanciais da solução demonstrada, nem a substituição de componentes essenciais após a realização da PoC, exceto quando a comissão técnica reconhecer, de forma motivada, que a intercorrência decorreu exclusivamente de indisponibilidade de ambiente, infraestrutura ou recurso de responsabilidade da **CONTRATANTE**.

7.19. Ao final da PoC, a comissão técnica elaborará relatório circunstanciado, contendo, no mínimo:

a) identificação da **LICITANTE** avaliada;
b) data, horário e local da sessão;
c) relação dos testes executados;
d) resultado individual de cada caso de teste;
e) evidências produzidas;
f) requisitos atendidos e não atendidos;
g) eventuais ocorrências registradas durante a sessão;
h) conclusão fundamentada quanto à aprovação ou reprovação da solução ofertada.

7.20. O relatório da PoC integrará os autos do processo licitatório e servirá de fundamento técnico para a aceitação ou desclassificação da proposta, observados os princípios do julgamento objetivo, da vinculação ao instrumento convocatório, da isonomia, da competitividade e da seleção da proposta mais vantajosa.

7.21. O detalhamento dos procedimentos, casos de teste, critérios de avaliação, evidências esperadas e condições de aprovação e reprovação da PoC consta do ANEXO I F – Matriz de Testes da Prova de Conceito (PoC), que integra este Termo de Referência.

8. REQUISITOS DA CONTRATAÇÃO

8.1. Requisitos de Integração

8.1.1. A solução deverá ser compatível com os sistemas, plataformas e protocolos atualmente utilizados pelo Banco da Amazônia, observando os seguintes critérios:

Suporte a padrões abertos e protocolos de segurança e integração corporativa, incluindo TLS 1.3, IPsec, LDAP/AD, SAML, RADIUS, Syslog e SNMPv3;

Compatibilidade com sistemas de autenticação, gerenciamento e SIEM/SOAR da **CONTRATANTE**, com console única de administração, autenticação multifator (MFA) e trilhas de auditoria;

Integração nativa com ambientes de nuvem pública (AWS, Azure, Google Cloud) e ambientes on-premises, em arquiteturas híbridas e multicloud;

Interoperabilidade com a infraestrutura tecnológica existente (data centers, diretórios, ferramentas de monitoração e governança), sem degradação de desempenho ou quebra de compatibilidade técnica.

8.2. Requisitos Funcionais

8.2.1. A solução **CONTRATADA** deverá prover:

Blindagem automatizada de vulnerabilidades para servidores e cargas de trabalho híbridas, com descoberta contínua, virtual patching e monitoramento de integridade;

Detecção e Resposta de Rede (NDR) com inspeção profunda, análise comportamental, identificação de C&C, exfiltração e anomalias, inclusive em tráfego criptografado;

Prevenção de Intrusão de Próxima Geração (NGIPS) com inspeção SSL/TLS, controle granular de aplicações, detecção de exploits e atualização automática de assinaturas;

Serviço de Detecção e Resposta Gerenciada (MDR) do fabricante, 24x7x365, com caça de ameaças, análise de causa raiz e relatórios mensais;

Gerenciamento centralizado com dashboards, alarmes, relatórios executivos e técnicos, histórico de auditoria e correlação inteligente de eventos;

Integração com ambientes de nuvem e sistemas corporativos, assegurando proteção uniforme e governança centralizada;

SLA mínimo de 99,7% para os ambientes críticos e alta disponibilidade entre datacenters;

Serviços de instalação, configuração, homologação, treinamento e suporte técnico mensal para todos os componentes da solução.

8.3. Requisitos Não Funcionais

8.3.1. A solução deverá atender aos seguintes atributos:

Escalabilidade modular (licenças, sensores, throughput) e evolução tecnológica contínua durante a vigência;
Alta disponibilidade e desempenho, com redundância de componentes, failover e replicação segura entre datacenters;
Segurança lógica fim a fim, com autenticação forte, criptografia, segregação de funções e controle de acesso baseado em perfis;
Monitoramento e gestão centralizados, com logs e relatórios acessíveis à **CONTRATANTE**;
Compatibilidade com as políticas de segurança, continuidade de negócios (DRP/BCP) e governança de TI da **CONTRATANTE**.

8.4. Necessidade de Treinamentos e Requisitos para Implementação da Solução

8.4.1. A **CONTRATADA** deverá oferecer, sem ônus para a **CONTRATANTE**:

Treinamento técnico e prático (hands-on) com carga horária mínima de 40 horas por módulo (Vulnerabilidades, NDR e NGIPS), ministrado por profissionais certificados pelo fabricante;
Conteúdo abrangendo operação da console, gestão de políticas, relatórios, resposta a incidentes (MDR) e procedimentos de contingência;
Material didático digital/presencial, instrutores certificados;
Suporte adicional pós-treinamento por 90 dias;
Demonstração funcional durante a implantação;
Treinamento online ou nas dependências da **CONTRATANTE**.

8.5. Indicação de Necessidade de Contratações Correlatas ou Interdependentes

8.5.1. A execução do objeto dependerá exclusivamente da **CONTRATADA**, sendo de sua responsabilidade:

Fornecimento de todos os profissionais, equipamentos, insumos e ferramentas;
Atendimento NOC/SOC 24x7x365, local e remoto, com canais 0800, e-mail e portal;
Realização de configurações, integrações e homologações em conformidade com a **CONTRATANTE**;
Fornecimento de manuais técnicos e itens de suporte à execução;
Substituição (RMA) imediata de equipamentos com falha, conforme SLA.

8.6. Requisitos de Segurança Adicionais

8.6.1. A solução deverá atender, adicionalmente, aos seguintes requisitos:

Segmentação lógica e controles por criticidade/serviço;
Detecção e resposta a ameaças por padrões e anomalias comportamentais;
Conformidade com BACEN, LGPD, ISO 27001/NIST e políticas internas;
Armazenamento de logs e métricas por no mínimo 12 meses, com acesso restrito e auditável.

8.7. Observações Específicas

8.7.1. Será admitida a padronização de equipamentos e serviços desde que tecnicamente justificada.

8.7.2. Poderá ser exigido certificado de conformidade de fabricação e qualidade dos produtos utilizados.

8.7.3. Não será permitida a contratação de um mesmo agente econômico para funções que exijam segregação, como fornecimento e fiscalização.

8.7.4. Excepcionalmente, poderão ser exigidos modelos/marcas específicos quando justificado por compatibilidade, desempenho ou padronização operacional.

8.8. 7.13 Requisitos de integração

8.8.1. Integração com a Arquitetura Tecnológica do Banco da Amazônia:

A solução ofertada deverá apresentar plena compatibilidade com a arquitetura tecnológica vigente, respeitando modularidade, interoperabilidade, segurança e escalabilidade horizontal/vertical.

Deverá garantir integração transparente com sistemas de missão crítica (core bancário), serviços de autenticação e autorização (AD/LDAP/SAML), VPN/IPsec, ambientes de desenvolvimento/homologação, nuvem pública/privada e ferramentas de monitoramento/auditoria.

Todos os elementos tecnológicos (hardware, software, APIs, interfaces de monitoração, motores de correlação, etc.) deverão seguir padrões abertos, aptos à integração com a arquitetura de serviços e microsserviços da **CONTRATANTE**.

8.9. Integração com a Arquitetura de Redes do Banco:

8.9.1. A solução deverá se integrar, de forma nativa, à arquitetura de redes corporativas e aos datacenters, suportando alta disponibilidade, balanceamento, failover e replicação segura.

8.9.2. Todos os componentes ativos (appliances NGIPS/NDR, servidores de gerenciamento, sensores, etc.) deverão interoperar com o backbone e as políticas de segurança existentes, sem degradação de desempenho ou quebra de compatibilidade.

8.9.3. A **CONTRATADA** deverá garantir a correta integração lógica e segura dos componentes (túneis criptografados, políticas, marcações e isolamentos necessários) entre ambientes de produção e contingência, conforme Especificações Técnicas.

8.9.4. Todas as configurações devem respeitar diretrizes internas sobre segregação de redes, endereçamento, autenticação, criptografia, replicação entre datacenters e regras de acesso entre zonas.

8.10. Requisitos funcionais da solução

8.10.1. A solução deverá atender aos requisitos funcionais necessários à sustentação da operação de segurança cibernética, garantindo disponibilidade, integração com ambientes críticos, flexibilidade operacional e aderência às diretrizes de modernização tecnológica.

8.10.2. Capacidade de Suporte à Inovação e Transformação Digital

A infraestrutura deverá ser compatível com as diretrizes de transformação digital, sustentando projetos como canais digitais, inteligência analítica e integração com nuvem, devendo:

- *Suportar múltiplas aplicações e cargas simultâneas em ambientes híbridos;*
- *Possuir flexibilidade para integração com tecnologias emergentes (SD-WAN, SASE, ZTNA, XDR);*
- *Garantir baixa latência e contingência ativa entre datacenters e unidades críticas.*

8.11. Ambiente Tecnológico de Suporte à Inovação Regional

8.11.1. A solução deverá prover base tecnológica para iniciativas de inovação, incluindo:

Acesso seguro à internet e integração com APIs e canais digitais em tempo real;
Apoio a ecossistemas de inovação com segurança e continuidade;
Fortalecimento de um ambiente digital estável para parcerias estratégicas.

8.12. Integração Segura com o Ambiente Corporativo do Banco

8.12.1. A infraestrutura deverá garantir plena integração com a arquitetura atual e futura, considerando:

- *Operação contínua com legados, core bancário, parceiros e plataformas externas (BACEN e congêneres);*
- *Compatibilidade com replicação de dados entre datacenters e serviços cloud híbridos;*
- *Aplicação de boas práticas de segurança e privacidade, com segregação, controle de acesso e registros de logs.*

8.13. Estímulo à Modernização Tecnológica e Eficiência Operacional

8.13.1. A solução deverá incorporar funcionalidades que avancem a gestão da infraestrutura por meio de:

- *Plataforma de monitoração centralizada com automação, alertas inteligentes, dashboards e indicadores (SLM);*
- *Integração com inventário de ativos, métricas de desempenho e disponibilidade;*
- *Ações proativas baseadas em análise comportamental e detecção de anomalias.*

8.14. Conectividade de Alta Performance para Projetos Estratégicos

8.14.1. A solução deverá garantir operação ininterrupta dos ambientes estratégicos do Banco por meio de:

- *Contingência e replicação entre datacenters, com alta disponibilidade dos componentes de segurança;*
- *Integração segura com parceiros, meios de pagamento e órgãos reguladores;*
- *Suporte a unidades em áreas remotas com mecanismos de resiliência e continuidade.*

8.15. Entregas Técnicas e Garantias de Atualização

8.15.1. Todos os elementos (appliances NGIPS/NDR, servidores de gerenciamento, licenças) deverão ser entregues em versões recentes e homologadas pelo fabricante;

8.15.2. Durante toda a vigência, a **CONTRATADA** deverá prover atualizações automáticas de versões, assinaturas e patches de segurança, sem ônus adicional;

8.15.3. Todos os produtos ofertados deverão apresentar compatibilidade plena entre si, com solução funcionalmente integrada;

8.15.4. Em caso de não conformidade técnica, será assegurado o contraditório e ampla defesa à **CONTRATADA**, conforme normativos aplicáveis.

8.16. Necessidade de treinamentos e requisitos para a implementação da solução

8.16.1. Caberá à **CONTRATADA** cumprir, sem ônus adicional, os seguintes requisitos durante a implementação:

Demonstração Técnica Inicial

*Durante a implantação, a **CONTRATADA** deverá apresentar demonstração completa contemplando:*

8.16.1.1. Arquitetura e componentes da plataforma integrada;

8.16.1.2. Mecanismos de alta disponibilidade, resposta a incidentes e atualizações;

8.16.1.3. Operação do gerenciamento centralizado e integrações (SIEM/SOAR);

8.16.1.4. Procedimentos de contingência e escalonamento;

8.16.1.5. Recursos disponíveis nos módulos de Vulnerabilidades, NDR, NGIPS e MDR.

8.17. Treinamento Inicial Obrigatório

8.17.1. A **CONTRATADA** fornecerá treinamento técnico inicial completo aos colaboradores designados;

8.17.2. Fornecimento de Conteúdo Programático Mínimo do Treinamento

8.17.3. Conteúdo obrigatório:

Visão geral da solução;
• Funcionalidades principais (blindagem, NDR, NGIPS, MDR, gestão e relatórios);
• Procedimentos operacionais para ativação, monitoração e troubleshooting;
• Resolução de problemas comuns;
• Melhores práticas para alta disponibilidade e desempenho.

8.18. .Carga Horária e Modalidade

8.18.1. Carga mínima de 40 horas;

8.18.2. Local: sede da **CONTRATANTE** em Belém/PA ou online síncrono com gravação;

8.18.3. Modalidade definida em comum acordo;

8.18.4. Suporte Técnico Pós-Treinamento

8.18.5. Disponibilização, por 90 dias, de suporte complementar (8x5, estendível a 24x7 em caso de impacto relevante), para:

Esclarecimento de dúvidas;
Apoio remoto a incidentes recorrentes;
Acompanhamento de procedimentos críticos em operação assistida.

8.19. Indicação de Eventual Necessidade de Contratações Correlatas ou Interdependentes

8.19.1. Eventuais necessidades técnicas ou logísticas para o correto funcionamento serão de inteira responsabilidade da **CONTRATADA**, sem ônus adicional.

8.19.2. Para garantir operação estável e contínua, a **CONTRATADA** deverá prover:

8.20. Alocação de Profissionais Qualificados

8.20.1. Alocação de profissionais qualificados e certificados para os equipamentos e serviços contratados, com todas as obrigações trabalhistas e previdenciárias.

8.21. Apoio Técnico e Logístico

8.21.1. Apoio completo às atividades de instalação, testes, manutenção, substituições e atualizações.

8.22. Custos Operacionais e Logísticos

8.22.1. Todos os custos necessários à execução serão integralmente absorvidos pela **CONTRATADA**.

8.23. Configurações e Customizações para Alta Disponibilidade

8.23.1. Realização de todas as configurações e customizações necessárias para operação ininterrupta, com mitigação proativa de falhas.

8.24. Execução conforme Normas Técnicas e Fabricantes

8.24.1. Execução conforme normas técnicas, recomendações dos fabricantes e boas práticas de segurança da informação.

8.25. Fornecimento de Ferramental e Documentação Técnica

8.25.1. Fornecimento de ferramental, manuais, guias e kit de ferramentas/testador para instalações em datacenter.

8.25.2. Equipamentos de Proteção

Fornecimento de EPI e EPC quando aplicável.

8.25.3. Suporte Técnico 24x7

Manutenção de infraestrutura de suporte 24x7x365 para ocorrências relativas à prestação dos serviços.

8.25.4. Suporte Técnico Remoto

Suporte remoto por telefone, e-mail e sistema de chamados web, com equipe qualificada.

8.25.5. Suporte Técnico Local

Atendimento on-site quando necessário, observando prazos e níveis de serviço do SLA.

8.25.6. Requisitos técnicos dos profissionais da **CONTRATADA**

8.25.7. Os requisitos dos profissionais estão descritos no **ANEXO I A – Especificações Técnicas da Solução**

9. ESCOLHA DA SOLUÇÃO

9.1. Durante o processo de planejamento da contratação, foram consideradas diversas alternativas tecnológicas e operacionais para atendimento às necessidades institucionais relacionadas à conectividade corporativa do Banco da Amazônia. A análise foi conduzida com base em critérios técnicos, estratégicos, logísticos e econômicos, conforme previsto no Estudo Técnico Preliminar (ETP), especialmente nas seções de **Levantamento de Mercado** e **Justificativas da Escolha da Solução a Contratar**.

9.2. As seguintes alternativas foram analisadas:

9.2.1. **Alternativa 1 –** manutenção do ambiente legado com contratação pontual de ferramentas isoladas (antivulnerabilidade, NDR, NGIPS, MDR em contratos distintos):

Vantagens: menor esforço inicial de transição; reaproveitamento parcial de componentes existentes.

Desvantagens: baixa integração entre camadas; ausência de gestão centralizada; aumento do TCO por sobreposição de contratos; maior risco de incompatibilidades e lacunas de segurança; dificuldade de correlação de eventos e resposta coordenada.

Conclusão: alternativa inadequada ao porte, criticidade e abrangência operacional do Banco, por não garantir visibilidade unificada nem resposta integrada a incidentes.

9.2.2. **Alternativa 2 –** contratação segmentada com múltiplos fornecedores, integrando via equipe interna (multi-vendor):

Vantagens: possibilidade de customização pontual; pluralidade de ofertas.

Desvantagens: complexidade elevada de gestão contratual e técnica; risco de incompatibilidade entre tecnologias e políticas; SLA heterogêneo; maior tempo de implantação e de resposta; perda de governança e de padronização.

Conclusão: alternativa não recomendada diante da necessidade de gestão unificada,

padronização e garantia de níveis mínimos de serviço em todo o ambiente.

9.2.3. **Alternativa 3 –** desenvolvimento/implantação própria de plataforma unificada (in-house), incluindo operação 24x7 e serviços de resposta:

Vantagens: maior controle direto sobre componentes e processos.

Desvantagens: inviabilidade técnica e econômica para sustentação de operação 24x7x365; necessidade de quadro especializado, ferramentas e inteligência de ameaças; prazos e custos incompatíveis com a urgência e com a evolução tecnológica contínua exigida.Conclusão: alternativa inviável, principalmente em função do alto custo, tempo de implantação e exigência de capacidades especializadas de difícil manutenção.

9.2.4. Alternativa 4 – contratação de Solução Integrada de Rede e Segurança em modelo plataforma unificada (full-solution), com gestão centralizada, MDR do fabricante 24x7, NDR, NGIPS e blindagem de vulnerabilidades (modelo proposto neste Termo de Referência):

Vantagens: gestão unificada de todas as camadas; alta disponibilidade e resiliência; padronização tecnológica; suporte especializado; redução de MTTD/MTTR por correlação inteligente; conformidade com LGPD, ISO 27001 e normativos BACEN; integração nativa com nuvem pública e ambientes on-premises; escalabilidade e evolução contínua com atualizações de versões e assinaturas.

Desvantagens: dependência de fabricante/integrador homologado; necessidade de fiscalização técnica contínua.

Conclusão: alternativa mais adequada e vantajosa para o Banco da Amazônia, considerando a criticidade das operações, a necessidade de visibilidade completa e resposta coordenada a incidentes, bem como a governança centralizada e a otimização do custo total de propriedade.

9.2.5. Dessa forma, a Equipe de Planejamento conclui que a contratação integrada da Solução de Rede e Segurança em plataforma unificada (full-solution), com fornecimento de hardware, software, serviços especializados, gerenciamento centralizado e MDR 24x7, é a alternativa mais segura, eficiente e compatível com os objetivos institucionais, assegurando continuidade operacional, conformidade regulatória e evolução tecnológica alinhada ao ETP.

10.PLANO DE SUSTENTAÇÃO (PARA CONTRATAÇÕES DE TECNOLOGIA DE INFORMAÇÃO)

10.1. O presente Plano de Sustentação tem como objetivo garantir a continuidade das operações do Banco da Amazônia durante e após a entrega da Solução Integrada de Rede e Segurança, bem como mitigar riscos relacionados à descontinuidade de serviços após o encerramento contratual. Este plano contempla os recursos materiais e humanos necessários, as precauções operacionais, a estratégia de transição contratual e os mecanismos para evitar dependência técnica da empresa **CONTRATADA**, assegurando autonomia operacional e governança sobre o ambiente implantado.

10.2. Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato

10.2.1. Recursos Materiais a Serem Fornecidos pelo Banco

*Não há previsão de fornecimento de recursos materiais por parte do Banco da Amazônia para a execução contratual da solução. Todos os insumos, appliances, servidores e licenças serão integralmente providos pela **CONTRATADA**, conforme especificações técnicas e quantitativos do Termo de Referência.*

10.2.2. Recursos de TI a Serem Fornecidos pelo Banco

*Disponibilização de acesso remoto seguro aos ambientes corporativos, mediante autenticação multifator (MFA) e controle de privilégios, para suporte técnico e integração com o sistema de gerenciamento da **CONTRATADA**, quando aplicável;*

Fornecimento, de forma controlada, de informações de diretório corporativo (Active Directory/LDAP/SAML) estritamente necessárias para fins de integração e autenticação entre as camadas da solução, garantindo rastreabilidade e conformidade com a LGPD.

10.2.3. Recursos Humanos

10.2.3.1. A **CONTRATADA** deverá disponibilizar equipe técnica qualificada e certificada, composta por, no mínimo, 2 profissionais aptos ao atendimento de chamados de manutenção, suporte técnico, atualização, correção, configuração e sustentação das ferramentas **CONTRATADAS**, conforme os níveis de serviço estabelecidos neste Termo de Referência e em seus anexos.
10.2.3.2. O atendimento será realizado preferencialmente de forma remota, podendo ocorrer de forma presencial quando a natureza do chamado, a criticidade do incidente ou a necessidade técnica assim exigir, mediante solicitação ou autorização da **CONTRATANTE**.
10.2.3.3. A disponibilização desses profissionais não caracteriza dedicação exclusiva de mão de obra, posto de trabalho residente, subordinação direta à **CONTRATANTE** ou controle de jornada pelo Banco da Amazônia, cabendo exclusivamente à **CONTRATADA** a gestão, coordenação, substituição e responsabilidade trabalhista, previdenciária e operacional sobre sua equipe.
10.2.3.4. O Banco da Amazônia designará analistas da área técnica para acompanhamento das atividades, absorção de conhecimento operacional e fiscalização contratual, assegurando a transferência de tecnologia e a autonomia de gestão do ambiente;
10.2.3.5. Ao término da vigência contratual, a **CONTRATANTE** deverá ter definida a estratégia de continuidade da solução — renovação, nova licitação ou absorção parcial pela equipe interna, conforme análise de viabilidade técnica e institucional.

10.2.4. Estratégia de Continuidade Contratual

10.2.4.1.1. Evento: Falência ou Inexecução pela **CONTRATADA**

Será incluída cláusula contratual exigindo da **CONTRATADA** a manutenção de garantia contratual durante todo o período de vigência, nas modalidades previstas na Lei nº 13.303/2016, tais como caução em dinheiro, fiança bancária ou seguro-garantia, de modo a resguardar a **CONTRATANTE** em casos de falência, inexecução parcial ou rescisão unilateral. Adicionalmente, a **CONTRATADA** deverá garantir a transferência de conhecimento e documentação técnica atualizada, mitigando dependência tecnológica e assegurando a continuidade dos serviços.

10.2.5. Plano de Continuidade de Negócios

10.2.5.1. *A **CONTRATADA** deverá possuir e comprovar, sempre que solicitado, um Plano de Continuidade de Negócios (PCN) aplicável à Solução Integrada de Rede e Segurança, com o objetivo de mitigar riscos operacionais que possam comprometer os níveis mínimos de serviço (SLA ≥ 99,7%) exigidos neste contrato.*

10.2.5.2. O PCN deverá contemplar:

- Estratégias de redundância operacional e failover entre datacenters;
- Mecanismos de replicação segura de dados e mitigação de falhas críticas de infraestrutura e segurança;
- Planos de contingência e resposta a incidentes de segurança cibernética com atuação automatizada via MDR;
- Procedimentos de recuperação de desastres (DRP), garantindo continuidade dos serviços

essenciais em caso de incidentes de indisponibilidade prolongada;

- Definição de responsáveis técnicos e fluxos de comunicação para incidentes de segurança e indisponibilidade.

10.2.6. **Ações para Transição e Encerramento Contratual**

*10.2.6.1. Ao final da vigência contratual, deverão ser adotadas pela **CONTRATADA** as seguintes providências, sem qualquer ônus adicional à **CONTRATANTE**:*

- Recebimento formal de comunicado de encerramento do contrato pela área gestora;
- Entrega de relatório técnico de transição, contendo documentação atualizada da solução implantada, configurações lógicas, versões de software, licenças vigentes, acessos administrativos, políticas aplicadas e status operacional de todos os módulos;
- Declaração de inexistência de pendências operacionais ou contratuais, com garantia de integridade dos registros e logs;
- Colaboração plena no processo de substituição ou transição, conforme instruções da **CONTRATANTE**, incluindo suporte à nova empresa ou equipe interna responsável pela continuidade da operação;
- Transferência formal de conhecimento técnico e de documentação (procedimentos de operação, relatórios, manuais e topologias), conforme previsto na estratégia de independência tecnológica do ETP.

11.INDICAÇÃO SE O CONTRATO É COM OU SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA;

11.1. A presente contratação não envolve dedicação exclusiva de mão de obra, uma vez que o objeto refere-se à implantação, operação, manutenção e suporte de solução integrada de rede e segurança, abrangendo hardware, software, licenças, serviços técnicos especializados e atendimento de chamados por equipe técnica da **CONTRATADA** e/ou do fabricante, sem alocação de postos fixos ou profissionais residentes nas dependências da **CONTRATANTE**.

11.2. A eventual atuação presencial de profissionais da **CONTRATADA** ocorrerá de forma pontual, sob demanda, para atendimento técnico específico, não configurando dedicação exclusiva de mão de obra.

11.3. As atividades de monitoramento, detecção e resposta gerenciada (MDR), bem como de suporte técnico, instalação e manutenção preventiva, serão realizadas por profissionais especializados e certificados, sem alocação exclusiva de mão de obra nas dependências da **CONTRATANTE**, não se caracterizando, portanto, vínculo direto ou atividades permanentes nas instalações do Banco da Amazônia.

12.MODELO DE GESTÃO DO CONTRATO

12.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 13.303, de 2016, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

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

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

12.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

12.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa **CONTRATADA** para reunião inicial para apresentação do plano

de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da **CONTRATADA**, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

12.6. **Fiscalização:** A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.

12.6.1. Fiscalização Técnica

O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

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

Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

O fiscal técnico do contrato informará ao gestor do serviço, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do serviço.

O fiscal técnico do contrato comunicará ao gestor do serviço, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

12.6.2. Fiscalização Administrativa

O fiscal administrativo do contrato será responsável por verificar a manutenção das condições de habilitação jurídica, fiscal, trabalhista e técnica da **CONTRATADA**, exigidas durante o processo licitatório, ao longo de toda a vigência contratual, conforme estabelecido na legislação aplicável.

Em caso de descumprimento de obrigações administrativas contratuais, como a ausência de garantias legais, desatualização de certidões, pendências trabalhistas ou descumprimento de cláusulas contratuais não técnicas, o fiscal administrativo atuará tempestivamente na solução do problema, comunicando imediatamente ao gestor do contrato quando as medidas necessárias ultrapassarem sua competência direta.

A fiscalização administrativa, no âmbito desta contratação, deverá obedecer às seguintes rotinas específicas, considerando a natureza estratégica e contínua da prestação dos serviços de conectividade:

12.6.2.1.1. Verificação periódica da validade da documentação de habilitação da **CONTRATADA** (balancetes, certidões negativas, apólices de seguro-garantia etc.);

12.6.2.1.2. Conferência da vigência e regularidade da garantia contratual, nos moldes exigidos pela Lei nº 13.303/2016;

12.6.2.1.3. Monitoramento da regularidade trabalhista e previdenciária dos profissionais alocados, quando aplicável, especialmente para técnicos residentes e equipes de campo que realizem suporte nas dependências do Banco;

12.6.2.1.4. Acompanhamento do cumprimento das obrigações contratuais formais, tais como entrega de relatórios gerenciais, cronogramas de implantação, atas de reuniões técnicas, registros de ocorrências e documentações de visitas técnicas;

12.6.2.1.5. Registro de ocorrências administrativas no histórico do contrato, com descrição precisa das ações adotadas e dos prazos para regularização;

12.6.2.1.6. Apoio ao gestor do serviço na elaboração de notificações formais e aplicação

de penalidades administrativas, quando cabíveis, conforme previsto no instrumento contratual;

12.6.2.1.7. Comunicação prévia à área responsável sempre que forem identificados indícios de inexecução contratual, suspensão das atividades ou risco de descontinuidade dos serviços, especialmente nas localidades de maior criticidade operacional.

12.7. Gestor do Serviço

12.7.1. O gestor do serviço coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

12.7.2. O gestor do serviço acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

12.7.3. O gestor do serviço acompanhará a manutenção das condições de habilitação da **CONTRATADA**, para fins de pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

12.7.4. O gestor do serviço emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e negócios quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

12.7.5. O gestor do serviço tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela área competente para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

12.7.6. O gestor do serviço deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

12.7.7. O gestor do serviço deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

13. ESTIMATIVAS DOS PREÇOS E ORÇAMENTO DETALHADO DO VALOR

13.1.1. Para a contratação, por se tratar de solução integrada de rede e segurança, realizamos pesquisa em diversos bancos públicos, sem encontrar contratos que se assemelhassem às necessidades do Banco. Portanto, realizamos cotação com 5 empresas da área que nos encaminharam 5 propostas, das quais descartamos uma por estar fora da faixa de valores de mercado.

13.1.2. O valor estimado para esta contratação será mantida sob 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, na (s) rubrica (s):

14.1.1. Rubricas orçamentárias

Tipo	Descrição	Conta Contábil
Investimento	Equipamentos de process. De dados	26.165-3 / 4103
Dispêndio	Licença de Uso	27.065-2 / 1
Despesa	Execução de Serviços - S/INSS PJ	82.022-9
Treinamento	DESPESAS DE PROCESSAMENTO - TREINAMENTOS P/IMP. INTR. EXTERNO - S/INSS PJ	82.110-1

14.2. O plano de desembolso da solução foi estruturado de forma linear e previsível ao longo dos cinco anos, permitindo melhor planejamento e alocação dos recursos orçamentários do Banco da Amazônia. **No Ano 1**, devido à necessidade de aquisição inicial de componentes de software e hardware, subscrições, serviços de implantação, configurações e treinamentos indispensáveis à ativação completa da solução. Esse investimento inicial concentra os custos de implementação e estabelece a base tecnológica necessária para os anos seguintes.

14.3. A partir do **Ano 3, 4 e 5**, os valores anuais tornam-se estáveis, permanecendo constantes**.** Essa estabilização ocorre porque, após a implantação concluída no primeiro ano, os custos passam a ser predominantemente operacionais, envolvendo atualizações, subscrições, suporte técnico contínuo e serviços de manutenção das soluções. Esse modelo reforça a economicidade ao diluir o investimento inicial e evitar desembolsos elevados nos anos subsequentes, além de proporcionar maior previsibilidade orçamentária e controle financeiro ao BASA.

14.4. É importante destacar que o item **"Serviço de suporte mensal das soluções CONTRATADAS" (item 12) será pago mensalmente,** por se tratar de um serviço continuado, necessário para garantir o funcionamento ininterrupto, o monitoramento, a aplicação de patches de segurança, a abertura e a resolução de chamados e o suporte especializado às soluções implementadas. Esse formato impede o pagamento antecipado de períodos não executados e está alinhado às melhores práticas de contratação de serviços contínuos na Administração Pública.

14.5. Como se trata de uma nova solução integrada, todos os recursos necessários já estão devidamente contemplados no planejamento orçamentário do Banco, com impacto previsto ao longo dos cinco anos de vigência. O modelo de desembolso anualizado acompanha a estrutura de licenciamento, manutenção e operação da solução, assegurando o equilíbrio financeiro e a compatibilidade com a capacidade orçamentária do BASA.

14.6. O valor mais elevado no primeiro ano reflete os custos típicos de implantação e ativação, enquanto a estabilidade dos valores a partir do segundo ano garante planejamento eficiente e previsibilidade no ciclo plurianual. Qualquer necessidade de substituição, alteração tecnológica ou revisão de escopo deverá ser previamente analisada pela Governança de TI (COGTI), garantindo alinhamento com o Plano Diretor de Tecnologia e com os princípios de economicidade, eficiência e sustentabilidade do investimento.

15. CRITÉRIOS DE ANÁLISE DE EXEQUIBILIDADE DAS PROPOSTAS

15.1. Para fins de análise da exequibilidade, a proposta será avaliada considerando o preço global ofertado para o lote único, os preços unitários e totais de cada item, os quantitativos, o prazo contratual de 60 (sessenta) meses, o cronograma físico-financeiro, a planilha de composição de custos e formação de preços e a compatibilidade da oferta com todas as obrigações previstas neste Termo de Referência e em seus anexos.

15.2. A análise de exequibilidade observará, no mínimo:

a) o valor global ofertado para o lote único;

b) os preços unitários e totais dos itens que compõem a solução;

c) a distribuição anual dos valores propostos ao longo dos 60 (sessenta) meses de vigência contratual;

d) a compatibilidade dos preços com os quantitativos previstos neste Termo de Referência;

e) a compatibilidade dos preços com as especificações técnicas, níveis mínimos de serviço, prazos de implantação, suporte, garantia, atualização de versões e demais obrigações contratuais;

f) a coerência entre os valores atribuídos a hardware, software, subscrições, serviços MDR, implantação, treinamento, suporte técnico, garantia, manutenção, atualizações, logística, tributos e demais custos necessários à execução integral do objeto;

g) a compatibilidade da proposta com os referenciais de mercado, com o orçamento estimado da contratação e com os documentos constantes do processo administrativo.

15.3. Para fins desta contratação, serão consideradas parcelas de maior relevância técnica e/ou econômica, para análise de exequibilidade, os seguintes componentes do objeto:

a) item 1 – Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas;

b) item 2 – Serviço de detecção e resposta (MDR) do fabricante para o item de blindagem de vulnerabilidades;

c) item 3 – Camada lógica para solução de análise de ameaças avançadas;

d) item 4 – Solução de Detecção e Resposta de Rede (NDR);

e) item 5 – Camada de hardware para solução de análise de ameaças avançadas;

f) item 6 – Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas;

g) item 7 – Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS);

h) item 8 – Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS);

i) item 9 – Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração;

j) item 10 – Serviço de instalação das soluções **CONTRATADAS**;

k) item 12 – Serviço de suporte mensal das soluções **CONTRATADAS**.

15.4. Para fins de análise objetiva da exequibilidade, serão considerados indícios de inexequibilidade da proposta, ensejando diligência pela Administração, isolada ou cumulativamente:

a) valor global ofertado inferior a 70% (setenta por cento) do valor global estimado pela Administração para a contratação;

b) preço total de qualquer item classificado como parcela de maior relevância técnica e/ou econômica, nos termos do item 15.3, inferior a 70% (setenta por cento) do respectivo valor estimado pela Administração para o item;

c) valor global ofertado inferior a 50% (cinquenta por cento) do valor global estimado pela Administração, hipótese em que a proposta será considerada como indício grave de inexequibilidade,

exigindo comprovação reforçada, detalhada e documental da viabilidade econômica, técnica e operacional da execução integral do objeto;

d) preço unitário ou total de item essencial cotado com valor igual a zero, simbólico ou manifestamente incompatível com o custo necessário à sua execução;

e) omissão de custos indispensáveis à execução do objeto, tais como licenciamento, subscrições, garantia, suporte do fabricante, atualização de versões, assinaturas, firmware, manutenção, logística, frete, tributos, seguros, implantação, treinamento, equipe técnica, certificações ou atendimento aos níveis mínimos de serviço;

f) distribuição de preços entre os itens que indique concentração artificial de custos em componentes de pagamento inicial, com redução desproporcional dos valores vinculados a suporte, subscrições, MDR, garantia, atualização de versões, manutenção ou operação continuada;

g) incompatibilidade entre os preços ofertados e a obrigação de fornecimento, implantação, integração, sustentação e suporte da solução durante o prazo contratual de 60 (sessenta) meses;

h) divergência relevante entre a proposta comercial e a planilha de composição de custos e formação de preços;

i) ausência de comprovação de que os produtos, licenças, subscrições, serviços MDR, suporte técnico e garantias ofertados terão cobertura integral durante toda a vigência contratual;

j) proposta que transfira indevidamente custos entre itens, etapas ou exercícios financeiros, de modo a comprometer a coerência econômico-financeira da contratação ou dificultar a fiscalização contratual.

15.5. Os percentuais previstos no item 19.10 constituem parâmetros objetivos para identificação de indícios de inexequibilidade e abertura de diligência, não implicando desclassificação automática da proposta.

15.6. Constatado indício de inexequibilidade, o(a) Pregoeiro(a) promoverá diligência para que a **LICITANTE** comprove, de forma objetiva, documental e detalhada, a viabilidade econômica, técnica e operacional da proposta apresentada, em prazo a ser fixado no ato de convocação.

15.7. Na diligência de exequibilidade, a **LICITANTE** deverá apresentar, conforme solicitado pela Administração, no mínimo:

a) planilha detalhada de composição de custos e formação de preços, com memória de cálculo;

b) detalhamento dos custos diretos e indiretos da solução, inclusive tributos, encargos, despesas administrativas, seguros, fretes, logística, implantação, treinamento, suporte técnico, manutenção, garantia, atualizações, assinaturas, subscrições e margem comercial;

c) identificação dos fabricantes, modelos, versões, licenças, subscrições, equipamentos, appliances, módulos, quantitativos e respectivos prazos de cobertura técnica e contratual;

d) comprovação de cobertura das licenças, subscrições, garantias, atualizações, assinaturas, serviços MDR, suporte do fabricante e suporte técnico durante os 60 (sessenta) meses de vigência contratual;

e) declaração ou documento emitido pelo fabricante, distribuidor ou canal autorizado, quando aplicável, que comprove a viabilidade de fornecimento da solução ofertada, a originalidade dos produtos, a disponibilidade de suporte oficial e a cobertura durante a vigência contratual;

f) detalhamento da composição dos preços dos serviços especializados, especialmente implantação, integração, treinamento, suporte técnico, manutenção, operação assistida, atendimento de chamados e serviços continuados vinculados à solução;

g) demonstração da compatibilidade entre a proposta comercial, o cronograma físico-financeiro, a planilha de composição de custos e as obrigações de execução contratual;

h) indicação da equipe técnica, certificações, estrutura de suporte, canais de atendimento, logística e capacidade operacional necessários à execução integral do objeto;

i) demais documentos que a Administração entenda necessários para formação de juízo quanto à exequibilidade da proposta.

15.8. A mera declaração genérica da **LICITANTE** de que sua proposta é exequível não será suficiente para afastar os indícios de inexequibilidade. A comprovação deverá ser específica, consistente, verificável e compatível com as exigências deste Termo de Referência, do Edital e de seus anexos.

15.9. A proposta não será desclassificada exclusivamente por apresentar valor inferior ao orçamento estimado ou aos percentuais previstos neste item, desde que a **LICITANTE** demonstre, de forma satisfatória, a plena viabilidade econômica, técnica e operacional de sua execução.

15.10. Após a diligência, será considerada inexequível e desclassificada a proposta quando ocorrer qualquer das seguintes situações:

a) ausência de apresentação, no prazo fixado, dos documentos solicitados para comprovação da exequibilidade;

b) apresentação de documentação genérica, insuficiente, contraditória ou incompatível com a proposta ofertada;

c) não comprovação da cobertura integral de licenças, subscrições, garantias, atualizações, assinaturas, serviços MDR, suporte do fabricante ou suporte técnico durante os 60 (sessenta) meses de vigência contratual;

d) não comprovação da viabilidade de fornecimento dos produtos, equipamentos, appliances, módulos, softwares, serviços, suporte, manutenção e demais componentes necessários à execução integral do objeto;

e) manutenção de preços unitários ou totais incompatíveis com os custos mínimos necessários à execução do objeto, sem justificativa técnica e econômica idônea;

f) identificação de omissão relevante de custos indispensáveis à execução contratual;

g) identificação de concentração artificial de preços, transferência indevida de custos entre itens ou composição econômico-financeira que comprometa a execução continuada da solução;

h) incompatibilidade entre a proposta, a planilha de custos, os quantitativos, o cronograma de execução, os níveis mínimos de serviço e as obrigações previstas neste Termo de Referência;

i) não comprovação de capacidade técnica, operacional, logística ou de suporte compatível com a execução do objeto pelo prazo contratual;

j) demonstração de que a proposta depende de condição futura, incerta, não prevista no Edital ou incompatível com o regime de execução contratual.

15.11. A desclassificação por inexequibilidade deverá ser devidamente motivada, com indicação dos elementos objetivos analisados, dos documentos apresentados pela **LICITANTE**, das inconsistências identificadas e das razões pelas quais a Administração concluiu pela inviabilidade econômica, técnica ou operacional da proposta.

15.12. A análise de exequibilidade não se limitará ao preço global, podendo alcançar os preços unitários, totais e anuais dos itens, especialmente daqueles classificados como parcelas de maior relevância técnica e/ou econômica, sempre que sua composição indicar risco de inadimplemento, execução inadequada, comprometimento da qualidade da solução, descumprimento dos níveis de serviço ou inviabilidade de sustentação contratual.

15.13. Não serão aceitas propostas que, ainda que apresentem valor global aparentemente regular, revelem composição de custos incompatível com a execução integral do objeto, com o modelo de solução integrada, com o prazo de 60 (sessenta) meses, com a manutenção dos níveis mínimos de serviço ou com as condições estabelecidas neste Termo de Referência e em seus anexos.

16. PRAZO DE VIGÊNCIA

16.1. O prazo de vigência do Contrato será de 60 meses, contados a partir da data de sua assinatura, nos termos do Artigo 71 da Lei nº 13.303/2016.

16.2. Este prazo foi definido com base na análise técnica apresentada no Estudo Técnico Preliminar (ETP), que identificou que a vigência estendida é a mais vantajosa para a administração, considerando:

- A complexidade da solução **CONTRATADA** e o tempo necessário para sua implantação completa em âmbito nacional;
- A criticidade dos serviços de conectividade para a continuidade das operações bancárias, especialmente em regiões remotas da Amazônia Legal;
- A previsibilidade orçamentária e a necessidade de estabilidade contratual para manter níveis elevados de disponibilidade, segurança e desempenho institucional;
- A aderência aos ciclos de planejamento estratégico e tecnológico do Banco da Amazônia.

16.3. Durante o período de vigência, poderão ser formalizados aditivos para ajustes contratuais compatíveis com a legislação, desde que não impliquem transfiguração do objeto contratado nem extrapolem os limites previstos na Lei nº 13.303/2016.

17. DA PARTICIPAÇÃO EM CONSÓRCIOS.

17.1. Fica vedada a participação de empresas em consórcio, em razão da criticidade do objeto, da necessidade de operação integrada e de responsabilização técnica centralizada.

17.2. A exigência de uma única responsável pela implementação, integração e operação mitigará o risco de fragmentação decisória, conflito de responsabilidades ou lacunas de suporte técnico.

18. CONDIÇÕES DE REAJUSTE DE PREÇOS

18.1. Os preços contratados serão reajustados com intervalo mínimo de 12 (doze) meses, contados a partir da data da proposta comercial, conforme disposto no Termo de referência de licitação, utilizando-se como referência o Índice de Custos de Tecnologia da Informação – ICTI/IPEA, por ser o indicador mais aderente ao setor e à natureza dos serviços técnicos especializados objeto da contratação.

18.2. Os reajustes subsequentes observarão, igualmente, o **interregno mínimo de 12 (doze) meses** a contar da **data-base do último reajuste aplicado**, sendo calculados com base na variação acumulada do índice ICTI/IPEA no respectivo período.

19. ALTERAÇÃO DO CONTRATO

19.1. 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.

19.1.1. A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do artigo 81 da Lei nº 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 S.A.

19.1.2. Excepcionalmente a alteração qualitativa não se sujeitará aos limites previstos nos § 1º e 2º do artigo 81 da Lei n. 13.303/2016, desde que observe os seguintes pressupostos:

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 a ser atendido pela obra ou pelo serviço;

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.

19.2. 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 S.A., 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 Serviço do BANCO DA AMAZÔNIA S.A.;

c) submetidas à área jurídica e, quando for o caso, à área financeira do BANCO DA AMAZÔNIA S.A.;

19.3. 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 S.A..

19.4. Não caracterizam alteração do contrato e podem ser registrados por termo de apostilamento, 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**;

20.PAGAMENTO AO FORNECEDOR

20.1. O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados a partir da emissão do Termo de Recebimento Definitivo, emitido pelos fiscais do contrato, que deverá atestar o recebimento do bem e/ou serviço, o cumprimento das obrigações contratuais correspondentes à etapa anual executada e autorizar expressamente a emissão da respectiva nota fiscal. Os pagamentos observarão a distribuição anual prevista na planilha de desembolso e percentuais do contrato, na seguinte forma:

Item	Software	Tipo	Conta	Quantidade	Percentual	Percentual	Percentual	Percentual	Percentual	Valor total
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.	Subscrição	27.065-2 / 1	1.000	20%	20%	20%	20%	20%	100%
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.	Subscrição	27.065-2 / 1	1.000	20%	20%	20%	20%	20%	100%
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Software	26.165-3 / 4103	2	25%	30%	15%	15%	15%	100%
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.	Subscrição	27.065-2 / 1	2	20%	20%	20%	20%	20%	100%
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Hardware	26.165-3 / 4103	2	100%	0%	0%	0%	0%	100%
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses.	Subscrição	27.065-2 / 1	2	20%	20%	20%	20%	20%	100%
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	Software	26.165-3 / 4103	4	20%	35%	15%	15%	15%	100%
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	Hardware	26.165-3 / 4103	4	100%	0%	0%	0%	0%	100%
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.	Subscrição	27.065-2 / 1	4	20%	20%	20%	20%	20%	100%
10	Serviço de Instalação das soluções Contratadas	Serviço	82.022-9	3	100%	0%	0%	0%	0%	100%
11	Serviços de treinamento das soluções contratadas	Treinamento	82.110-1	3	100%	0%	0%	0%	0%	100%
12	Serviço de suporte mensal das soluções contratadas	Serviço	82.022-9	12	20%	20%	20%	20%	20%	100%

a) itens 1, 2, 4, 6, 9 e 12: pagamento anual correspondente a 20% (vinte por cento) do valor total do item em cada um dos 5 (cinco) anos de vigência contratual;

b) item 3: pagamento anual correspondente a 25% (vinte e cinco por cento) no Ano 1, 30% (trinta por cento) no Ano 2 e 15% (quinze por cento) em cada um dos Anos 3, 4 e 5;

c) item 7: pagamento anual correspondente a 20% (vinte por cento) no Ano 1, 35% (trinta e cinco por cento) no Ano 2 e 15% (quinze por cento) em cada um dos Anos 3, 4 e 5;

d) itens 5, 8, 10 e 11: pagamento correspondente a 100% (cem por cento) do valor total do item no Ano 1, após o recebimento definitivo da respectiva entrega ou execução;

e) os pagamentos anuais somente serão devidos após a comprovação da efetiva execução da parcela correspondente de cada item, nos termos do cronograma físico-financeiro e da fiscalização contratual.

20.2. 18.2 As Notas Fiscais referentes às parcelas anuais de cada item não serão aceitas quando emitidas após o dia 25 do mês subsequente ao atesto da respectiva etapa anual de execução, devendo a **CONTRATADA** emiti-las a partir do 1º (primeiro) dia útil do mês subsequente ao recebimento definitivo da parcela correspondente.
20.3. 18.3 No caso de atraso imputável ao **CONTRATANTE**, os valores devidos à **CONTRATADA**, referentes à respectiva parcela anual vencida e não paga, serão atualizados monetariamente entre o termo final do prazo de pagamento e a data de sua efetiva realização, mediante aplicação do índice IPCA/IBGE de correção monetária.

21. Forma de pagamento

21.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

21.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

21.5. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de trinta dias

úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

21.6. Para fins de liquidação, o fiscal técnico deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- o prazo de validade;
- a data da emissão;
- os dados do contrato e do órgão **CONTRATANTE**;
- o período respectivo de execução do contrato;
- o valor a pagar; e
- eventual destaque do valor de retenções tributárias cabíveis.

21.7. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao **CONTRATANTE**;

21.8. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, social e trabalhista, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação estabelecida na contratação.

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

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

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

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

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

22.DA GARANTIA DO CONTRATO

22.1. A **CONTRATADA** se obriga a manter, durante toda a vigência da garantia dos serviços prevista neste Contrato, garantia contratual ao **CONTRATANTE**, em qualquer das modalidades previstas em Lei (caução em dinheiro, fiança bancária ou seguro-garantia), nos termos do Artigo 70 da Lei nº 13.303/16, de acordo com as seguintes condições:

22.2. Garantia contratual de 5% (cinco por cento) do valor anual do Contrato, pelo prazo de toda a execução contratual;

22.3. A garantia oferecida pela **CONTRATADA** deve assegurar o cumprimento tanto do objetivo contratado, quanto das obrigações acessórias, inclusive trabalhistas;

22.4. A **CONTRATADA** deverá providenciar a garantia contratual impreterivelmente em 10 (dez) dias úteis, contados a partir da assinatura do Contrato.

22.5. No caso de CAUÇÃO EM DINHEIRO, o valor depositado será administrado pelo **CONTRATANTE** e devolvido à **CONTRATADA** após o ateste pelo Banco da inexistência de pendências contratuais de qualquer natureza e ainda do término e extinção do Contrato.

22.6. O **CONTRATANTE** reserva-se o direito de utilizar, a qualquer tempo, no todo ou em partes, o valor da garantia para cobrir prejuízos eventualmente apurados, decorrentes de descumprimento de qualquer obrigação contratual ou falha dos serviços ora contratados, inclusive motivados por greve ou atos dos empregados da **CONTRATADA.**

22.7. Utilizada a garantia, por qualquer que seja o motivo, a **CONTRATADA** fica obrigada a integralizá-la no prazo de 05 (cinco) dias úteis contados da data em que for notificada formalmente pelo **CONTRATANTE**, sob pena de rescisão do Contrato.

22.8. A garantia somente será devolvida à **CONTRATADA** quando do término ou rescisão do Contrato, desde que a **CONTRATADA** não possua dívida com o **CONTRATANTE** mediante expressa autorização deste.

22.9. No caso de **SEGURO-GARANTIA** o **CONTRATANTE** deverá ser indicado como beneficiário do seguro garantia e ter prazo de validade de pelo menos 03 (três) meses após o prazo previsto para término do contrato;

22.10. O seguro-garantia deverá assegurar o pagamento de todas as obrigações contratuais previstas.

22.11. A **CONTRATADA** obriga-se a apresentar nova apólice, até 05 (cinco) dias úteis após o vencimento da anterior e a comprovar o pagamento do prêmio respectivo, até 02 (dois) dias úteis após o seu vencimento.

22.12. No caso da **FIANÇA BANCÁRIA** deverão constar do instrumento os seguintes requisitos:

a. Prazo de validade correspondente ao período de vigência do Contrato, acrescentado de 03 (três) meses após o prazo previsto para término do contrato;

b. Expressa afirmação do fiador de que, como devedor solidário e principal pagador,fará o pagamento, ao **CONTRATANTE**, dos prejuízos por este sofridos, em razão do descumprimento das obrigações da **CONTRATADA**, independente de interpelação judicial; e

c. Cláusula que assegure a atualização do valor afiançado.

22.13. A qualquer tempo, mediante prévia comunicação ao **CONTRATANTE**, poderá ser admitida a substituição da garantia, observadas as modalidades (caução em dinheiro, fiança bancária ou seguro-garantia), previstas na legislação em vigor.

22.14. A garantia será liberada após o perfeito cumprimento do Contrato, no prazo de até 30 (trinta) dias, contados da data do seu vencimento, desde que devidamente comprovado que não há pendências contratuais de qualquer natureza, em especial aquelas envolvendo direitos trabalhistas do empregados abrangidos pelo contrato encerado, inclusive quanto às verbas rescisórias, se for o caso, devendo tal condição estar registrada no documento pertinente à garantia, caso está se efetue nas modalidades de seguro-garantia e fiança bancária.

23.DAS OBRIGAÇÕES DA CONTRATADA

23.1. A **CONTRATADA** obriga-se a cumprir integralmente as disposições previstas neste Termo de referência, no contrato e em seus anexos, observando as seguintes obrigações, sem prejuízo de outras que sejam inerentes ao cumprimento do objeto da contratação:

Obrigações Gerais

23.2. Executar o objeto do contrato em conformidade com todas as especificações técnicas, níveis de serviço (SLA), prazos e demais condições estabelecidas neste Termo de Referência, no Estudo Técnico Preliminar e nos seus anexos, garantindo a entrega e operação da Solução Integrada de Rede e Segurança.

23.3. Cumprir rigorosamente todos os prazos de implantação, ativação, homologação, suporte, manutenção e correções, conforme cronograma técnico e marcos contratuais aprovados pela **CONTRATANTE**.

23.4. Prestar, sempre que solicitado, esclarecimentos técnicos e administrativos sobre a execução do contrato, bem como atender tempestivamente a reclamações, notificações e recomendações emitidas pela fiscalização ou gestão contratual.

23.5. Submeter-se à fiscalização técnica e administrativa da **CONTRATANTE**, assegurando livre acesso a instalações, sistemas, equipamentos, consoles de gerenciamento, registros, relatórios e documentos relacionados à execução do objeto.

23.6. Prover todos os meios técnicos, humanos, materiais, logísticos e operacionais necessários à plena operacionalidade da plataforma de segurança integrada, incluindo hardware, software, licenças, suporte técnico, serviços de instalação, configuração, atualização e manutenção preventiva e corretiva.

23.7. Manter sigilo e confidencialidade absolutos sobre dados, documentos, topologias, políticas de segurança, relatórios, acessos e informações técnicas ou estratégicas do Banco da Amazônia, aplicando medidas de proteção física e lógica em conformidade com a Lei nº 13.709/2018 (LGPD), as normas internas e as políticas de segurança da **CONTRATANTE**.

23.8. Executar todas as atividades em conformidade com a legislação brasileira vigente, especialmente a Lei nº 13.303/2016, a Resolução nº 4.893/2021 do Banco Central do Brasil, a Lei Geral de Proteção de Dados (LGPD), bem como as normas de segurança da informação, trabalhistas, fiscais e ambientais aplicáveis.

23.9. Não empregar, direta ou indiretamente, trabalho ilegal, infantil ou análogo à escravidão, devendo garantir que todos os seus fornecedores, subcontratados e prestadores de serviço observem integralmente a legislação trabalhista e de direitos humanos.

23.10. Adotar políticas de equidade e não discriminação no ambiente de trabalho, assegurando respeito à diversidade e à inclusão social, conforme boas práticas corporativas e princípios de responsabilidade social do Banco da Amazônia.

23.11. Executar os serviços com responsabilidade socioambiental, observando a legislação ambiental vigente e as boas práticas de sustentabilidade, incluindo descarte correto de resíduos eletrônicos, redução de impactos ambientais e uso racional de recursos.

23.12. Corrigir imediatamente, sem ônus para a **CONTRATANTE**, quaisquer falhas, deficiências, inconsistências ou desvios técnicos identificados pela fiscalização, dentro dos prazos estabelecidos nas notificações formais.

23.13. Responder civil e administrativamente por eventuais danos causados à **CONTRATANTE** ou a terceiros, decorrentes de ações ou omissões de seus empregados, subcontratados ou prepostos, desde que comprovada culpa ou dolo, inclusive por comprometimento de dados, indisponibilidade de serviços ou falhas de segurança.

Obrigações Específicas Relacionadas à Solução Integrada de Rede e Segurança

23.14. Garantir a alta disponibilidade da infraestrutura **CONTRATADA**, conforme SLA definido em anexo, assegurando monitoramento contínuo 24x7x365, suporte técnico proativo e tempos de resposta e resolução compatíveis com a criticidade dos serviços.

23.15. Monitorar continuamente o desempenho, a integridade e os indicadores da solução por meio da plataforma central de gerenciamento, utilizando inteligência artificial e machine learning para detecção de anomalias, priorização de alertas e geração de relatórios técnicos e executivos periódicos.

23.16. Assegurar a redundância e a resiliência operacional de todos os componentes, incluindo módulos de NDR, NGIPS, blindagem de vulnerabilidades e MDR, mantendo mecanismos automáticos de failover e replicação segura entre datacenters.

23.17. Disponibilizar profissionais qualificados e certificados pelo fabricante para todas as atividades de implantação, configuração, suporte técnico e manutenção da solução, conforme perfis mínimos estabelecidos no Termo de Referência e nos seus anexos**.**

23.18. Garantir compatibilidade plena entre os módulos e equipamentos fornecidos, com atualizações automáticas de firmware, assinaturas, patches de segurança e versões, sem interrupções na operação e sem impacto sobre a disponibilidade dos serviços críticos do Banco.

23.19. Manter infraestrutura técnica, logística e de suporte suficiente para atuação local e remota, conforme os níveis de atendimento definidos em contrato, assegurando resposta imediata a incidentes, inclusive em regiões remotas da Amazônia Legal.

24.DAS OBRIGAÇÕES DO CONTRATANTE

24.1. O Banco da Amazônia, na qualidade de **CONTRATANTE**, compromete-se a cumprir as obrigações a seguir, sem prejuízo de outras previstas em lei, no contrato ou em seus anexos, com vistas a assegurar a boa execução do objeto contratado:

24.2. Exigir o cumprimento integral de todas as obrigações assumidas pela **CONTRATADA**, em conformidade com as cláusulas contratuais, o Termo de Referência, os Anexos Técnicos e a proposta comercial vencedora.

24.3. Designar formalmente os fiscais técnico e administrativo do contrato, os quais exercerão as atividades de acompanhamento e fiscalização da execução dos serviços, conforme previsto no Art. 117 da Lei nº 13.303/2016 e no Art. 99 do Regulamento de Licitações e Contratos do Banco da Amazônia.

24.4. Atuar no controle e validação das entregas contratuais, por meio do atesto técnico das Notas Fiscais/Faturas correspondentes às etapas executadas, condicionando o pagamento à comprovação da conformidade dos serviços e ao cumprimento dos SLA acordados.

24.5. Rejeitar, total ou parcialmente, os serviços prestados em desacordo com as especificações técnicas, padrões de qualidade, cronograma, prazos ou qualquer outra obrigação prevista contratualmente, comunicando formalmente à **CONTRATADA** as não conformidades apuradas.

24.6. Efetuar o pagamento das Notas Fiscais/Faturas apresentadas pela **CONTRATADA**, desde que protocoladas com antecedência mínima de 30 (trinta) dias do vencimento, e que os serviços prestados estejam integralmente atestados pelo setor técnico competente.

24.7. Disponibilizar os meios e recursos mínimos necessários à prestação dos serviços contratados, quando aplicável, incluindo:

- Acesso remoto (VPN) para diagnóstico e suporte;
- Apoio logístico local, mediante solicitação prévia, nas unidades operacionais do Banco;
- Autorização para entrada em ambientes de missão crítica, mediante credenciamento prévio do(s)técnico(s) da **CONTRATADA**.

24.8. Receber e identificar os prepostos da **CONTRATADA**, adotando as providências administrativas necessárias para garantir o acesso autorizado às dependências do Banco, conforme normas de segurança institucional.

24.9. Assegurar que ordens e solicitações relativas à execução dos serviços sejam formalmente encaminhadas ao preposto da **CONTRATADA**, evitando interferência direta nos seus empregados, exceto em situações de emergência ou risco iminente.

24.10. Notificar a **CONTRATADA**, por escrito, sempre que houver constatação de falhas, irregularidades ou infrações contratuais, estabelecendo prazo razoável para a sua correção, bem como aplicar penalidades administrativas, quando cabíveis, observando o contraditório e a ampla defesa.

Obrigações Complementares Específicas ao Objeto

24.11. Disponibilizar, quando necessário, as informações técnicas e operacionais essenciais para viabilizar a correta configuração dos equipamentos e enlaces contratados, sem que isso implique compartilhamento de informações sigilosas ou estratégicas.

24.12. Garantir a interlocução institucional com os demais setores do Banco (como infraestrutura predial, segurança da informação, TI, logística e agências), para assegurar ambiente técnico e organizacional adequado à implantação e operação da solução de Rede.

24.13. Planejar, com a devida antecedência, os procedimentos necessários à renovação, substituição ou nova contratação dos serviços, de forma a evitar descontinuidade na prestação dos serviços de conectividade ao término da vigência contratual.

25.DAS SANÇÕES ADMINISTRATIVAS

25.1. Pela inexecução total ou parcial do objeto, o Banco poderá, garantido o contraditório e a ampla defesa, sem prejuízo das demais cominações previstas no Termo de Referência e na minuta do contrato, aplicar as penalidades previstas nas leis nº 13.303/16:

I – Advertência;

II – Multa de 10% (dez por cento) sobre o valor global da contratação, pela inexecução total do ajuste;

III – Multa diária de 0,2% (dois décimos por cento), calculado sobre o valor da respectiva fatura, quando houver atraso parcial na execução do objeto do contrato enquanto perdurar o inadimplemento;

IV - Suspensão do direito de licitar e de contratar com o Banco pelo prazo de até 2 (dois) anos;

25.2. O atraso na entrega do produto superior a 30 (trinta) dias consecutivos, poderá ensejar, a exclusivo critério do Banco, a rescisão do Contrato.

25.3. A rescisão do contrato provocada pela **CONTRATADA** implicará, de pleno direito, a cobrança pelo Banco de multa equivalente a 10% (dez por cento) do valor total contratado.

25.4. Nenhuma penalidade será aplicada pelo Banco sem o devido processo administrativo, assegurado o contraditório e a ampla defesa, no prazo de 5 (cinco) dias úteis.

25.5. A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança, facultada a defesa prévia, não isentará a obrigação de indenizar eventuais perdas e danos.

25.6. O valor das multas apurado, após o processo administrativo, será descontado dos pagamentos eventualmente devidos ao Banco.

25.7. 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.

25.8. Em não se realizando o pagamento nos termos definidos no item acima, far-se-á a sua cobrança judicialmente.

26.DA SUBCONTRATAÇÃO

26.1. A **CONTRATADA** não poderá subcontratar o núcleo do objeto, compreendendo a operação integrada da solução, a execução dos serviços de NDR, NGIPS, MDR, a gestão centralizada, o suporte técnico especializado e a administração lógica, sob pena de rescisão contratual.

26.2. Será admitida, mediante autorização prévia e expressa da **CONTRATANTE**, a subcontratação de atividades acessórias ou de apoio logístico que não impliquem transferência das responsabilidades principais assumidas.

26.3. A **CONTRATADA** permanecerá responsável, perante a **CONTRATANTE**, pela execução integral do objeto, pelos níveis de serviço, pela segurança da informação e pela conformidade técnica, bem como pelo cumprimento da Lei Geral de Proteção de Dados – LGPD.

27.DA RESCISÃO DO CONTRATO

27.1. A rescisão poderá ocorrer:

I. Mediante distrato pela inexecução total ou parcial das cláusulas contratuais;

II. Por cordo entre as partes, reduzida a termo no processo de contratação desde que haja conveniência para o Banco, precedida de autorização escrita e fundamentada mediante aviso prévio por escrito de 30 (trinta) dias consecutivos, e

III. Judicialmente nos termos da legislação.

27.2. Sem prejuízo de outras sanções, constituem motivos para rescisão do Contrato, oriundo da contratação, as situações descritas nos subitens abaixo:

a) Paralisação injustificada dos serviços;

b) O não cumprimento de cláusulas contratuais, especificações ou prazos;

c) A subcontratação, ainda que parcial, dos serviços objeto do Contrato;

d) A cessão ou transferência do contrato;

e) O desatendimento às determinações da FISCALIZAÇÃO designada para acompanhar e fiscalizar a execução dos serviços;

f) O cometimento reiterado de faltas na execução dos serviços;

g) A decretação de falência, o pedido de recuperação judicial ou extrajudicial;

h) A dissolução da sociedade;

i) A alteração societária que modifique a finalidade ou o controle acionário ou, ainda, a estrutura da **CONTRATADA** que, a juízo da **CONTRATANTE**, inviabilize ou prejudique a execução deste Contrato;

j) A prática de qualquer ato que vise fraudar ou burlar o fisco ou órgão/entidade arrecadador/credor dos encargos sociais e trabalhistas ou de tributos;

k) O descumprimento de quaisquer das condições ajustadas neste Contrato;

l) A utilização pela **CONTRATADA** de mão-de-obra de menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e menores de 16 (dezesseis) anos em qualquer trabalho, salvo na

condição de aprendizes, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal (Emenda Constitucional nº 20, de 1998);

m) O conhecimento, ainda que, "a posteriori", de fato ou ato que afete a idoneidade da **CONTRATADA** ou de seus sócios/cotistas ou de seus gestores ou ainda de seus representantes;

n) Razões de interesse público;

o) Ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução deste Contrato;

p) Deixar de comprovar sua regularidade fiscal, trabalhista, inclusive contribuições previdenciárias e depósitos de FGTS para com seus empregados;

q) Utilizar em benefício próprio ou de terceiras informações sigilosas ás quais tenha acesso por força de suas atribuições.

27.3. O Banco da Amazônia poderá, a qualquer tempo, mediante aviso com antecedência mínima de 30 (trinta) dias, denunciar o Contrato, para efeito de rescisão, sem que, por esse motivo, seja obrigado a suportar ônus de indenização, multa ou pagamento extra de qualquer natureza, salvo previsão em lei.

27.4. Também poderá ocorrer rescisão quando:

a) Não prestar garantia suficiente para assegurar o cumprimento das obrigações contratuais.

b) Deixar de comprovar sua regularidade, trabalhista, fiscal, inclusive contribuições previdenciárias e depósitos do FGTS dos seus funcionários;

c) Vier a ser declarada inidônea por qualquer órgão da Administração Pública;

d) Vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira;

e) Utilizar em benefício próprio ou de terceiros, informações sigilosas às quais tenha acesso por força de suas atribuições contratuais.

27.5. A rescisão acarretará, de imediato execução da garantia, para ressarcimento, ao **CONTRATANTE**, dos valores das multas aplicadas ou de quaisquer outras quantias ou indenizações a ele devidas.

27.6. A rescisão acarretará, de imediato, retenção dos créditos decorrentes deste Contrato, até o limite dos prejuízos causados ao **CONTRATANTE**.

27.7. Na rescisão do Contrato, o **CONTRATANTE** aplicará à **CONTRATADA** multa prevista neste contrato.

27.8. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados à **CONTRATADA** o contraditório e o direito à ampla defesa.

27.9. As responsabilidades imputadas à **CONTRATADA**, por prejuízos decorrentes de ações delitivas perpetradas contra o **CONTRATANTE**, não cessam com a rescisão deste Contrato.

28.DOS CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL, SOCIAL E TRABALHISTA E ECONÔMICA FINANCEIRA

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

Habilitação Jurídica

28.2. Para sua habilitação jurídica, o **LICITANTE** deve comprovar a possibilidade de exercer direitos

e assumir obrigações, devendo comprovar essa condição através por meio de carteira de identificação, contrato social, estatuto social ou outro documento constitutivo compatível com o objeto da contratação, bem como documento que comprova os poderes de seus representantes e decreto de autorização de funcionamento para empresas estrangeiras, conforme exigido neste termo de referência.

28.2.1. Deverá apresentar ainda cópia CPF e RG/CNH dos representantes e/ou procuradores que representarão a propensa **CONTRATADA** no ato de assinatura do contrato.

Habilitação Fiscal, Social e Trabalhista

28.2.2. Para fins de Habilitação fiscal, a **LICITANTE** deverá apresentar a documentação de acordo com as exigências do SICAF, inclusive certidão de regularidade trabalhista ou ainda através das certidões abaixo:

I - a inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ) – Cartão CNPJ;

II - a inscrição no cadastro de contribuintes estadual e municipal, se houver, relativo ao domicílio ou sede do **LICITANTE**, pertinente ao seu ramo de atividade e compatível com o objeto contratual – Comprovante de Inscrição na Fazenda Municipal e Estadual ou Distrital;

III - a regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do **LICITANTE**, ou outra equivalente, na forma da lei – Certidão Negativa ou Positiva com efeito de Negativa de Regularidade perante a Fazenda Federal, Estadual e Municipal ou Distrital;

IV - a regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei - Certidão Negativa ou Positiva com efeito de Negativa de Débitos Relativos a Créditos Tributários Federais e à Divida Ativa da União / Certidão de Regularidade do FGTS (CRF).

V - a regularidade perante a Justiça do Trabalho - Certidão Negativa ou Positiva com efeito de Negativa de Débitos Trabalhistas - **CNDT;**

VI - Declaração de não empregar menor – Art. 7º, inciso XXXIII, CF;

VII - Declaração de Conhecimento do decreto nº 7.203 de 04/06/2010;

*Os documentos referidos neste inciso artigo poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do **LICITANTE**, inclusive por meio eletrônico, desde que por meios legalmente idôneos.*

Habilitação Econômico-Financeira

28.3. Além dos documentos exigidos no Edital, a **LICITANTE** deverá apresentar **patrimônio líquido mínimo equivalente a 10% (dez por cento) do valor anual estimado da contratação**, considerado o valor anualizado de referência adotado pela Administração para fins de habilitação, admitida atualização monetária quando cabível.

27.2.8 A exigência de patrimônio líquido mínimo prevista no subitem anterior justifica-se pela natureza do objeto, que envolve contratação integrada de solução de rede e segurança, com fornecimento de hardware, software, subscrições, serviços de implantação, treinamento, suporte técnico e operação especializada, em ambiente de alta criticidade e com vigência contratual de 60 (sessenta) meses, exigindo capacidade financeira compatível com a execução continuada e com a manutenção dos níveis mínimos de serviço.

27.2.10 As empresas constituídas no exercício em curso ou com menos de 1 (um) ano de existência deverão apresentar:

a) balanço de abertura, na forma da lei;
b) quando houver movimentação contábil, demonstrações intermediárias aptas a evidenciar sua situação econômico-financeira;
c) documentos assinados pelo representante legal e pelo responsável técnico contábil, observadas as

formalidades legais aplicáveis.

27.2.11 As empresas inativas no exercício anterior deverão apresentar:

a) as demonstrações contábeis do último exercício em que estiveram ativas;
b) documento comprobatório da condição de inatividade no período correspondente, quando exigível;
c) documentação contábil superveniente que evidencie sua reativação, quando houver.

27.2.12 A **LICITANTE** em **recuperação judicial ou extrajudicial** poderá participar da presente licitação, desde que comprove, de forma objetiva e suficiente, sua viabilidade econômico-financeira e sua aptidão para executar o objeto contratual, inclusive por meio da documentação contábil exigida neste item e, quando aplicável, por meio de decisão judicial, plano de recuperação aprovado ou outro documento idôneo que evidencie a regularidade de sua condição e a possibilidade de cumprimento das obrigações contratuais.

27.2.13 A Administração poderá promover diligência para verificar a consistência das informações econômico-financeiras apresentadas, inclusive para conferência do índice, do patrimônio líquido, da regularidade formal dos documentos contábeis e da compatibilidade da situação financeira da **LICITANTE** com o porte, a complexidade, a criticidade e a duração da contratação.

27.2.14 Serão aceitos documentos contábeis apresentados por meio do **SPED Contábil**, Junta Comercial competente ou outro meio legalmente admitido, desde que observados os requisitos formais de registro, autenticação e assinatura previstos na legislação aplicável.

27.2.15 As **microempresas e empresas de pequeno porte** deverão atender a todas as exigências de habilitação econômico-financeira previstas neste Edital, sem prejuízo do tratamento favorecido legalmente aplicável nas demais fases do certame.

Outras condições de Habilitação

28.3.1. A propensa **CONTRATADA** deverá apresentar ***"Declaração de conhecimento do Art. 38 da Lei 13.303/16"***, na forma do anexo estabelecido no processo de contratação do Banco;

28.3.2. A propensa **CONTRATADA** deverá apresentar "***Declaração de Inexistência de Fato Impeditivo ou Superveniente",*** na forma do anexo estabelecido no processo de contratação do Banco;

28.3.3. A propensa **CONTRATADA** deverá apresentar "***Declaração de não existência em seu quadro empregado do Banco"***, na forma do anexo estabelecido no processo de contratação do Banco;

28.3.4. A propensa **CONTRATADA** deverá apresentar ***"Declaração de conhecimento da Lei de Improbidade Administrativa"***, na forma do anexo estabelecido no processo de contratação do Banco;

28.3.5. A propensa **CONTRATADA** deverá apresentar "**Declaração de ME e EPP"** na forma do anexo estabelecido no processo de contratação do Banco;

28.3.6. O **CONTRATANTE** realizará consultas à lista restritivas de Prevenção e Lavagem de Dinheiro (PLD), sendo que a **CONTRATADA** não poderá apresentar restrições nas referidas listas, salvo se deliberado pelo comitê competente do **CONTRATANTE**.

29.DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA

29.1.1. A **LICITANTE** deverá comprovar aptidão técnica para o desempenho de atividade pertinente e compatível com o objeto desta contratação, consistente na implantação, integração, operação, suporte e sustentação de solução integrada de rede e segurança, em ambiente corporativo de médio ou grande porte, abrangendo, no mínimo, os componentes de blindagem de vulnerabilidades, detecção e resposta de rede (NDR), prevenção de intrusão de próxima geração (NGIPS) e serviço de detecção e resposta

gerenciada (MDR), observadas as especificações deste **Termo de Referência e do Anexo I A**.

29.1.2. Atestado(s) de Capacidade Técnica

29.1.3. Para comprovação da capacidade técnico-operacional, a **LICITANTE** deverá apresentar, no mínimo, 01 (um) **Atestado de Capacidade Técnica**, emitido por pessoa jurídica de direito público ou privado, em nome da **LICITANTE**, que comprove a execução de serviços compatíveis com o objeto desta contratação.

29.1.4. Serão aceitos tantos atestados quantos forem necessários para a comprovação da capacidade técnica exigida, admitindo-se a soma de quantitativos e escopos complementares, desde que demonstrem, em conjunto, experiência compatível com a implantação e a operação da solução integrada objeto deste certame.

29.1.5. Os atestados deverão referir-se a contratos concluídos ou em execução, desde que, neste último caso, contem com execução mínima de 12 (doze) meses, admitindo-se diligência para verificação das informações prestadas, inclusive mediante solicitação de cópia do instrumento contratual, termos de aceite, ordens de serviço, relatórios de execução ou outros documentos idôneos de suporte.

Deverá ser apresentado em conjunto com os atestados uma planilha que comprove atendimento a todos os itens elencados neste Termo de Referência, bem como correlacionado a um documento oficial do fabricante, citando o mesmo e número da página de atendimento (Planilha ponto-a-ponto).

29.1.6. Os atestados deverão conter, de forma clara e objetiva, no mínimo:

a) identificação da pessoa jurídica emitente;
b) identificação da **LICITANTE** como executora dos serviços;
c) descrição do escopo executado;
d) período de execução;
e) quantitativos relevantes do ambiente atendido, tais como ativos, sensores, links, throughput, módulos implantados ou parâmetro técnico equivalente;
f) indicação da responsabilidade da **LICITANTE** na implantação, integração, operação, suporte ou sustentação da solução.

29.1.7. Definição de serviços similares

29.1.8. Para fins de qualificação técnica, serão considerados **serviços similares** ao objeto da licitação aqueles que demonstrem equivalência técnica e de complexidade, compreendendo, em ambiente corporativo de médio ou grande porte, a implantação e/ou operação integrada de solução de segurança com, no mínimo, os seguintes componentes ou funcionalidades equivalentes:

a) NDR (Network Detection and Response): instalação, configuração, parametrização e integração de sensores ou coletores de rede e console de gestão, com geração, tratamento e correlação de alertas e eventos;

b) NGIPS (Next Generation Intrusion Prevention System): instalação, configuração, ajuste fino de políticas de detecção e prevenção de intrusão, em modo inline e/ou monitoramento, com evidência de operação em produção;

c) Blindagem de vulnerabilidades: execução de processo contínuo de identificação, priorização, mitigação e proteção de vulnerabilidades, incluindo inventário, varredura, hardening, patching, virtual patching ou mecanismos equivalentes, correlacionados aos eventos de segurança da plataforma;

d) Integração obrigatória: comprovação de integração entre os componentes acima, mediante correlação de eventos, encaminhamento para ferramenta corporativa de logs, console centralizada, plataforma de XDR, SIEM ou estrutura equivalente, de modo a caracterizar solução integrada, e não apenas ferramentas isoladas.

e) Serviço de suporte e respostas a incidentes: prestação de serviço de suporte e resposta a incidentes prestados no âmbito das soluções **CONTRATADAS**;

29.1.9. Serão aceitas soluções de fabricantes distintos para fins exclusivos de comprovação de experiência pretérita, desde que comprovem equivalência funcional aos componentes exigidos nesta contratação.

29.1.10. Infraestrutura técnica e capacidade operacional

29.1.11. **A LICITANTE** deverá comprovar que possui, diretamente ou por meio de estrutura contratualmente vinculada, capacidade operacional compatível com a execução do objeto, incluindo equipe técnica qualificada, instalações adequadas, recursos de laboratório, ferramental e suporte técnico necessários ao atendimento da solução ofertada.

29.1.12. A **LICITANTE** deverá comprovar possuir ou ter acesso contratual a estrutura de operação e suporte apta a atender a solução proposta, inclusive, quando aplicável ao escopo contratado, centros de operação de segurança e/ou rede (**SOC/NOC**) em território nacional, com equipe técnica certificada e capacidade de atendimento em regime compatível com os níveis de serviço exigidos no Termo de Referência.

29.1.13. A **LICITANTE** deverá apresentar declaração de capacidade operacional, assinada por seu representante legal, atestando que dispõe de infraestrutura técnica e equipe certificada compatíveis com a execução da solução proposta, inclusive para implantação, configuração, atualização, suporte, operação e atendimento especializado dos módulos de NDR, NGIPS, MDR e blindagem de vulnerabilidades.

29.1.14. **Conformidade do fabricante, originalidade e suporte**

29.1.15. Considerando que o **Anexo I A** exige solução integrada e componentes do mesmo fabricante, a **LICITANTE** deverá apresentar **declaração de conformidade técnica** emitida pelo fabricante da solução ou por integrador autorizado, atestando que a **LICITANTE** está homologada, certificada ou autorizada a implantar, configurar, suportar e operar a tecnologia ofertada.

29.1.16. A **LICITANTE** deverá apresentar declaração de compromisso de suporte técnico do fabricante, assegurando a disponibilidade de atualizações de versões, assinaturas, correções, firmware, patches e suporte oficial durante toda a vigência contratual.

29.1.17. A **LICITANTE** deverá comprovar, mediante documento emitido pelo fabricante ou distribuidor autorizado, que os produtos ofertados são originais, homologados e cobertos por suporte oficial do fabricante, vedada a oferta de itens em condição de **End of Life (EoL)**, **End of Support (EoS)** ou situação equivalente incompatível com o prazo contratual.

29.1.18. **Declarações da LICITANTE**

29.1.19. A **LICITANTE** deverá apresentar declaração formal de que atenderá integralmente às exigências mínimas relativas à implantação, configuração, integração, operação, atualização, suporte técnico, infraestrutura, equipe especializada, equipamentos e demais requisitos indispensáveis ao cumprimento do objeto licitado.

29.1.20. A apresentação da proposta implicará responsabilidade exclusiva da **LICITANTE** pela prévia avaliação das condições técnicas e operacionais necessárias à execução do objeto, não sendo admitidas alegações posteriores de desconhecimento do escopo, das especificações ou das condições de execução.

30.DA OBRIGAÇÃO DE MANUTENÇÃO DOS CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL,

TRABALHISTA E ECONÔMICO FINANCEIRO E QUALIFICAÇÃO TÉCNICA EXIGIDAS

30.1. A **CONTRATADA** obriga-se em manter durante a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na presente contratação.

31. DAS GARANTIAS DOS MATERIAIS E SERVIÇOS

31.1. A **CONTRATADA** obriga-se a dar garantia aos serviços e equipamentos conforme este termo de referência pelo prazo de no mínimo de 60 meses, a contar da data da assinatura do contrato, contra qualquer defeito de fabricação, incluindo avarias no transporte até o local de entrega, mesmo depois de ocorrida sua aceitação pelo **CONTRATANTE**. Durante esse período de garantia, a **CONTRATADA** prestará manutenção ao bem, de acordo com o seguinte esquema:

I. Durante o período da garantia, a **CONTRATADA** providenciará a reparação de eventual defeito ou substituição, no prazo máximo de 10 (dez) dias contado da data de notificação do defeito, sem ônus para o **CONTRATANTE**, seja com transporte do bem, peças, ferramentas, diárias de mão-de-obra, hospedagem e alimentação de técnicos, seguros, embalagem;

II. Findo tal prazo, sem a devida reparação do serviços e equipamentos conforme este termo de referência, a **CONTRATADA** deverá substituir, em 24 (vinte e quatro) horas, por outro novo e original, entregando-a no mesmo local da anterior, tudo sem ônus, inclusive despesas com transporte, substituição e entrega;

III. A **CONTRATADA** deverá apresentar listagem das empresas credenciadas para prestação de assistência técnica corretiva durante todo o período da garantia, compreendendo no mínimo de 1 (uma) empresa credenciada em cada local para onde serviços e equipamentos conforme este termo de referência serão destinados.

IV. Se o defeito encontrado não for resultante de mau uso ou negligência por parte de prepostos do **CONTRATANTE**, este nada pagará pelo conserto/substituição do equipamento;

V. Se o bem entregue ao **CONTRATANTE** apresentar qualquer tipo de defeito ou não estiver em conformidade com as especificações deste Termo, o mesmo deverá ser substituído no prazo máximo de 15 (quinze) dias consecutivos;

VI. Toda e qualquer despesas decorrentes da execução dos Serviços de Garantia aqui descritos, inclusive as substituições de produtos e/ou seus componentes, ficarão inteiramente a cargo da **CONTRATADA**, bem como a responsabilidade dos produtos e/ou seus componentes que estiverem sob sua guarda, ou sob a guarda de sua Assistência Técnica credenciada, arcando com quaisquer danos.

VII. O fornecedor vencedor, deverá apresentar um termo de garantia técnica por escrito com prazo de 30 dias após a assinatura do contrato.

32. DO SIGILO E RESTRIÇÕES

32.1. É responsabilidade do **CONTRATADO** garantir absoluto sigilo sobre todos os processos, fórmulas, rotinas, objetos, informações, documentos e quaisquer outros dados que venham a ser disponibilizados pelo **CONTRATANTE** ao mesmo, em razão da execução do Contrato, oriundo desta contratação.

32.2. É responsabilidade da **CONTRATADA** garantir absoluto sigilo e confidencialidade sobre todos os processos, fórmulas, rotinas, objetos, informações, documentos, dados técnicos, comerciais e quaisquer outros elementos disponibilizados pelo **CONTRATANTE**, em razão da execução do contrato decorrente desta contratação.

32.3. A **CONTRATADA** deverá observar integralmente os quesitos da Lei nº 13.709/2018 – Lei Geral

de Proteção de Dados Pessoais (LGPD), responsabilizando-se pela proteção dos dados pessoais tratados no âmbito da execução contratual, de acordo com os princípios da finalidade, necessidade, adequação, segurança, prevenção e responsabilização.

32.4. A observância à LGPD e às normas complementares será regida pelo **ANEXO VII** Tratamento de Dados.

32.5. A **CONTRATADA** compromete-se a adotar todas as medidas técnicas e administrativas necessárias para prevenir incidentes de segurança da informação e vazamento de dados, incluindo controles de acesso, criptografia, segregação de funções e registros de auditoria.

32.6. É vedada à **CONTRATADA** a utilização das informações disponibilizadas pelo **CONTRATANTE** para qualquer outra finalidade que não seja a execução do objeto contratual, sob pena de aplicação das sanções previstas em contrato, sem prejuízo das responsabilidades civis, administrativas e penais cabíveis.

33.FISCALIZAÇÃO DO CONTRATO

33.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o cumprimento do ajuste, e serão exercidos por um ou mais representantes da **CONTRATANTE**.

33.2. A fiscalização da entrega do objeto da contratação será realizada pela Gerência de Produção e Infraestrutura (GPROD) que designará representante da Administração para o gerenciamento do cumprimento das obrigações previstas neste contrato.

33.3. A ausência ou omissão da Fiscalização do **CONTRATANTE** não eximirá a **CONTRATADA** das responsabilidades previstas neste Contrato.

33.4. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência e na proposta.

34.MATRIZ DE RISCO

34.1. Fica consignado para presente contratação a divisão dos riscos conforme Matriz de Riscos constante no **Anexo X**, repartindo os riscos assumidos por cada uma das partes na celebração da presente contratação**.**

35.DAS VEDAÇÕES

35.1. O instrumento de contrato objeto da presente contratação não poderão ser, no todo ou em parte, objeto de cessão ou transferência.

35.2. Nos termos do art. 7º do Decreto nº 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da administração pública federal, também é vedado ao **CONTRATADO** utilizar, durante toda a vigência do Contrato, mão de obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º (terceiro) grau, de empregado do **CONTRATANTE** que exerça cargo em comissão ou função de confiança.

36.DA INTEGRIDADE, DA CONDUTA ÉTICA E DOS PROCEDIMENTOS ANTICORRUPÇÃO

36.1. O contrato oriundo da presente contratação deverá prever que as Partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa - Lei nº 8.429, de 02 de junho de 1992 e a Lei Anticorrupção - Lei nº 12.846, de 01 de agosto de 2013 e seus regulamentos e 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, as Partes declaram que tem e manterão até o final da vigência do contrato, oriundo desta contratação, 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 códigos de ética e conduta, ambas as Partes desde já se obrigam, 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;

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;

III. Respeitar e exigir que seus empregados respeitem, no que couber, os princípios éticos e os compromissos de conduta definidos no Código de Conduta Ética do **BASA**, cujo teor poderá ser acessado no site www.bancoamazonia.com.br/index.php/obanco-codigodeetica.

36.2. A comprovada violação de quaisquer das obrigações previstas nesta contratação é causa para a rescisão unilateral do Contrato, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

36.3. A aplicação das sanções previstas na Lei n° 12.84, de 2013 não afeta os processos de responsabilização e aplicação de penalidades decorrentes de atos ilícitos.

37. DOS CRITÉRIOS DE SUSTENTABILIDADE

37.1. A **CONTRATADA** se compromete a atender 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 a Política Geral de Contratações, disponível em https://www.bancoamazonia.com.br/component/edocman/politica-geral-de-contratacoes/viewdocument/5727, considerando os requisitos a seguir:

- Não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;

- Não empregar menores de 18 anos para trabalho noturno, perigoso ou insalubre, e menores de dezesseis anos para qualquer trabalho, com exceção a categoria de Menor Aprendiz;

- Não permitir a prática ou a manutenção de discriminação limitativa ao acesso na relação de emprego, ou negativa com relação a sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar ou estado gravídico, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

- Respeitar o direito de formar ou associar-se a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias;

- Proteger e preservar o meio ambiente, bem como buscar prevenir e erradicar práticas que lhe sejam danosas, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos às áreas de meio ambiente, emanadas das esferas federal, estaduais e municipais e implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;

- Desenvolver suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados a proteções dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se: a) “Condições ultrajantes”: condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo. b) “Condições sub-humanas”: tudo que está abaixo da

condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano, situação abaixo da linha da pobreza.
c) “Condições degradantes de trabalho”: condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão;

- Atender à Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), observando quanto ao descarte adequado e ecologicamente correto;

- Apresentar conformidade com a legislação e regulamentos que disciplinam sobre a prevenção e combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo;

- Não ter sofrido sanções que implicam na restrição de participar de licitações ou de celebrar contratos com a Administração Pública, não constar registro da empresa e/ou sócios e representantes no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), atendendo às diretrizes anticorrupção;

- Adotar práticas e métodos voltados para a preservação da confidencialidade e integridade, atentando à Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018;

- O Banco da Amazônia poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia defesa, caso se comprove que a **CONTRATADA**, subcontratados ou fornecedores utilizam-se de trabalho em desconformidade com as condições referidas nas cláusulas supracitadas.

38.FORO

38.1. Fica eleito o Foro de Belém, capital do Estado do Pará, com renúncia a qualquer outro, por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução desta contratação.

E por estarem de pleno acordo as Partes reconhecem e concordam expressamente que a inserção de sua senha pessoal e/ou a utilização de outras formas de assinatura eletrônica. Inclusive biométricas, em plataformas digitais, como a “Certisign”, constitui forma legítima e suficiente para a confirmação de seus dados, comprovação de sua identidade e validade de sua declaração de vontade para assinar e celebrar a presente contratação para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

ANEXO I A

ESPECIFICAÇÕES TÉCNICAS

1.1. PLATAFORMA DE CIBERSEGURANÇA – Plataforma de segurança unificada para extensão de visibilidade do ambiente, quantificação de risco, baseado na identificação e mapeamento da superfície de ataque.

1.1.1. Para atender a integridade da solução e facilitar a gestão do ambiente, todas as soluções devem ser do mesmo fabricante;

1.2. COMPOSIÇÃO DA SOLUÇÃO

ITEM	DESCRIÇÃO DO ITEM
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.
3	Camada Lógica para solução de inspeção de rede contra ameaças avançadas, incluindo atualização de versão por 60 meses.
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.
5	Camada de hardware para solução de inspeção de rede contra ameaças avançadas, incluindo atualização de versão por 60 meses.
6	Serviço de detecção e resposta (MDR) do fabricante para o item de inspeção de rede contra ameaças avançadas pelo período de 60 meses.
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS).
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS).
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.
10	Serviço de instalação das soluções **CONTRATADAS**.
11	Serviços de treinamento das soluções **CONTRATADAS**.
12	Serviço de suporte mensal das soluções **CONTRATADAS**.

DESCRIÇÕES TÉCNICAS:

1. **Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses:**
   1.1. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

   1.2. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, Microsoft Azure, Amazon Web Services e Google Cloud Platform.

   1.3. A console de administração deverá permitir o envio de notificações via SMTP;

   1.4. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

   1.5. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

   1.6. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

1.7. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

1.8. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

1.9. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

1.10. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

1.11. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

1.12. A solução de segurança ter a capacidade de identificar ataques em estruturas de container.

1.13. Deve ser possível customizar os privilégios de administração da solução:

1.14. Acesso total;

1.15. Acesso somente leitura;

1.16. Deve ser possível assignar políticas de segurança em máquinas específicas, grupos estáticos e dinâmicos;

1.17. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

1.18. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

1.19. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

1.20. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

1.21. Windows Server 2000;

1.22. Windows Server 2003 SP1 e 2003 R2 SP2;

1.23. Windows Server 2008 e 2008 R2;

1.24. Windows Server 2012 e 2012 R2;

1.25. Windows Server 2016;

1.26. Windows Server 2019;

1.27. Windows Server 2022;

1.28. Windows XP e 7;

1.29. Red Hat Enterprise 5, 6, 7 e 8;

1.30. CentOS 5, 6, 7 e 8;

1.31. AIX 6.1, 7.1 e 7.2;

1.32. Oracle Linux 5, 6, 7 e 8;

1.33. SUSE Linux Enterprise Server 10, 11, 12 e 15;

1.34. Ubuntu 10, 12, 14, 16, 18 e 20;

1.35. Debian 6, 7, 8, 9 e 10;

1.36. Rocky Linux 8;

1.37. AlmaLinux 8;

1.38. Cloud Linux 5, 6, 7 e 8;

1.39. Amazon Linux 2 (x64)

1.40. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

1.41. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

1.42. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

1.43. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

1.44. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

1.45. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

1.46. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

1.47. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

1.48. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

1.49. A solução deverá mostrar quais máquinas estão usando determinada política;

1.50. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

1.51. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

1.52. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

1.53. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

1.54. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

1.55. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

1.56. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

1.57. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

1.58. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, HPArcSight e IBMQradar, de modo a permitir enviar os seus logs para essas soluções;

1.59. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

1.60. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

1.61. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

1.62. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

1.63. Após a atualização deve ser informado o que foi modificado ou adicionado;

1.64. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

1.65. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

1.66. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

1.67. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

1.68. No gerenciamento de licenças, deve ser informada quantidade **CONTRATADA** e quantidade em utilização de clientes;

1.69. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

1.70. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

1.71. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

1.72. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

1.73. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

1.74. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

1.75. A solução deve possuir API documentada para integração na esteira de automação;

1.76. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

1.77. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

1.78. A solução deve permitir desabilitar os módulos individualmente;

1.79. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

1.80. A console deverá possibilitar a integração com o Microsoft Active Directory, listando as máquinas e grupos existentes na estrutura;

1.81. Em caso da solução ser ofertada em nuvem, deve ser compliance com ISO 27001, ISO 27014, ISO 27017 e SOC 2;

1.82. Os ambientes em nuvem providos pelo fabricante devem passar por testes de penetração de forma recorrente como para garantir a segurança da solução provida.

1.83. Deverá possuir funcionalidade de Antimalware;

1.84. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

1.85. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

1.86. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

1.87. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

1.88. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

1.89. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

1.90. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

1.91. A solução deverá oferecer escanear processos em memória em busca de Malware;

1.92. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

1.93. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;

1.94. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

1.95. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

1.96. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

1.97. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

1.98. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

1.99. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

1.100. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

1.101. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

1.102. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

1.103. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

1.104. Proteção Contra URLs Maliciosas

1.105. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

1.106. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

1.107. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

1.108. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

1.109. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

1.110. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

1.111. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

1.112. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

1.113. Deverá possuir funcionalidade de Firewall de host;

1.114. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

1.115. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

1.116. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

1.117. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

1.118. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

1.119. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

1.120. Precisa ter a capacidade de definição de regras para contextos específicos;

1.121. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

1.122. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

1.123. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

1.124. O firewall deverá ser stateful bidirecional;

1.125. O firewall deverá permitir liberar ou apenas logar eventos;

1.126. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

1.127. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

1.128. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

1.129. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

1.130. Deverá realizar pseudo stateful em tráfego UDP;

1.131. Deverá logar a atividade stateful;

1.132. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

1.133. Deverá permitir limitar o número de meias conexões vindas de um computador;

1.134. Deverá prevenir ack storm;

1.135. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

1.136. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;

1.137. Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;

1.138. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

1.139. Proteção contra Vulnerabilidades de Sistemas Operacionais e Aplicações

1.140. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

1.141. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do Sistema Operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

1.142. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;

1.143. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

1.144. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

1.145. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

1.146. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

1.147. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

1.148. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

1.149. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

1.150. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

1.151. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

1.152. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

1.153. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

1.154. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

1.155. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

1.156. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

1.157. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

1.158. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

1.159. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

1.160. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

1.161. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

1.162. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

1.163. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

1.164. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

1.165. As regras devem ser atualizadas automaticamente pelo fabricante;

1.166. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

1.167. Monitoramento De Integridade para Servidores

1.168. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

1.169. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

1.170. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

1.171. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

1.172. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

1.173. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

1.174. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

1.175. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

1.176. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;

1.177. Deverá logar e colocar em relatório todas as modificações que ocorram;

1.178. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

1.179. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

1.180. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

1.181. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

1.182. Deverá possuir capacidade de Inspeção de Logs para Servidores

1.183. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

1.184. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

1.185. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

1.186. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

1.187. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

1.188. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

1.189. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

1.190. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

1.191. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

1.192. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

1.193. As regras poderão ser modificadas por severidade de ocorrência de eventos;

1.194. As regras devem se atualizar automaticamente pelo fabricante;

1.195. Permitir modificação pelo administrador em regras para adequação ao ambiente.

1.196. Deverá possuir capacidades de Controle De Aplicações

1.197. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

1.198. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

1.199. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

1.200. A console deverá exibir eventos de no mínimo 30 dias;

1.201. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

1.202. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

1.203. Deverá possuir funcionalidades de de Detecção e Resposta;

1.204. solução deve possuir módulo de investigação, detecção integrados;

1.205. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

1.206. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

1.207. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

1.208. O módulo de detecção e resposta deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

1.209. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

1.210. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

1.211. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

1.212. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

1.213. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

1.214. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

1.215. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

1.216. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

1.217. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

1.218. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

1.219. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

1.220. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

1.221. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de detecção e resposta do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;

1.222. Esta conexão deverá garantir, sem qualquer configuração local, que o sensor de detecção e resposta esteja ativo e envie telemetria a plataforma;

1.223. **xxx**

2. **Serviço de detecção e respota (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo perído de 60 meses:**
   2.1. O Serviço de Monitoramento avançado é aquele resultante de vários serviços de cibersegurança prestados em conjunto com o objetivo de oferecer observabilidade e respostas aos alertas gerados de potenciais ameaças e ataques cibernéticos
   2.2. O serviço de monitoramento avançado é composto de equipes técnicas especializadas em cibersegurança, atendimento de requisições e respostas a incidentes, e soluções de tecnologia.
   2.3. A solução deverá possuir monitoramento avançado da plataforma de detecção e resposta estendida em modo 24x7.
   2.4. O serviço deve operar na modalidade 24 horas 7 dias por semana, baseado na plataforma de Detecção e Resposta Estendida (XDR);
   2.5. Deve auxiliar a **CONTRATANTE** no processo de implantação das soluções, de forma a balizar tais ações com base nas melhores práticas do fabricante, acompanhamento de instalações das soluções em fases de homologação e apoio nas configurações necessárias;
   2.6. Deve ser elencado o panorama de vulnerabilidades existentes no ambiente da **CONTRATANTE**, apresentando recomendações para aplicação de patchs;
   2.7. Apoio na criação e customização dos playbooks de resposta automatizada da solução;
   2.8. Deve prover celeridade na resolução de chamados de suporte técnico, atuando com SLO de até 1 Hora;
   2.9. Deve fornecer acesso a um gestor de serviços do fabricante, para comunicações gerais acerca do ambiente e das entregas **CONTRATADAS**, agindo como um ponto único de contato;
   2.10. O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato;
   2.11. O serviço de monitoramento avançado deve validar a ingestão de logs pelos sensores da plataforma de Detecção e Resposta Estendida;
   2.12. Quando necessário, a **CONTRATANTE** poderá solicitar aconselhamento sobre processos de melhoria, atualização ou migração das soluções atuais para o gestor de serviços do fabricante;

2.13. O serviço em questão deve estar atrelado diretamente às tecnologias **CONTRATADAS** neste processo a fim de facilitar a correlação das informações e dar uma rápida resposta, a saber:
2.14. Plataforma de detecção e resposta estendida - XDR;
2.15. Sensores de detecção e resposta para Endpoint - EDR;
2.16. Sensor de detecção e resposta para e-mail;
2.17. Os relatórios dos incidentes analisados e reportados devem ser fornecidos com frequência mínima mensal para o ambiente;
2.18. O serviço deve dispor de ações de caça de ameaças com base nos alertas gerados pela plataforma de Detecção e Resposta Estendida;
2.19. O time de monitoramento do fabricante deve atuar com análise dos indicadores de ameaças e campanhas de malware identificadas no ambiente;
2.20. Deverá monitorar os alertas gerados pela plataforma de detecção e resposta estendida – XDR em regime 24 horas por dia e 7 dias por semana;
2.21. Os alertas gerados deverão ser analisados e categorizados segundo criticidade: Alta, Média e Baixa, os quais devem ser informados a **CONTRATANTE** para ações particulares;
2.22. Deve ser possível, em comum acordo com a **CONTRATANTE**, que sejam tomadas ações de remediação em casos de detecção de ameaças eminentes, via time de monitoramento do fabricante;
2.23. Deve prover análise de possíveis incidentes, mapeando o ponto de entrada do ataque, escopo afetado, recomendações de contenção e melhorias futuras;
2.24. O fabricante deverá analisar os alertas gerados na plataforma e deverá reportar em casos de possíveis indícios de fases iniciais ou em curso de ataques cibernéticos;
2.25. Deve identificar, perante os alertas gerados pela plataforma, a cadeia de causa raiz e determinar o perfil da ameaça, informando tais análises a **CONTRATANTE**;
2.26. Deve ocorrer buscas de novos IOCs identificados no ambiente, com base na inteligência de ameaças do fabricante;
2.27. O fabricante deverá aplicar análises de configurações detalhadas das soluções com base na documentação de melhores práticas da plataforma;
2.28. Ao final de cada validação de saúde das soluções o fabricante deverá apresentar um relatório detalhado;
2.29. O fabricante deverá disponibilizar ao menos 40 hrs por ano de serviços especializados de análise profunda de incidentes de segurança e respostas a incidente, durante a vigência do contrato;
2.30. A **CONTRATADA** deve identificar o momento oportuno apara acionamento do serviço de resposta a incidentes;
2.31. A atuação do time de resposta a incidentes do fabricante deve ocorrer de maneira única, cobrindo as 40hrs, dentro o contrato de 60 meses;
2.32. Ao final das atividades de incidente e resposta o fabricante deverá apresentar relatório conclusivo sobre as atividades realizadas, incluindo escopo identificado do incidente, causa raiz quando aplicável, medidas de contensão e recomendações de melhores práticas contra fragilidades identificadas;

3. Camada Lógica para solução de inspeção de rede contra ameaças avançadas, incluindo atualização de versão por 60 meses:

3.1. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da **CONTRATANTE**, inspecionando o tráfego de rede, independente de agentes instalados;
3.2. A solução deverá prover inspeção avançada de tráfego de rede para detecção de ameaças conhecidas e desconhecidas, com capacidade de análise em múltiplos protocolos e formatos de arquivo, e ser integrada a uma console única de XDR (Extended Detection and Response) para gestão centralizada e correlação de eventos de segurança.
3.3. Todos os eventos e alertas devem ser enviados e correlacionados em uma console única de XDR, permitindo visão unificada de incidentes e resposta coordenada.

3.4. Integração com plataforma de XDR para correlação de dados provenientes de endpoints, e-mail, rede e servidores.O sensor avançado de análise de rede deve ser licenciado a fim de inspecionar o Throughput total informado pela **CONTRATANTE**;
3.5. Deve atuar com a inspeção de rede da **CONTRATANTE**, estendendo visibilidade sob tráfego leste-oeste e norte-sul;
3.6. A solução inspeciona tráfego norte-sul e leste-oeste por meio de sensores físicos, virtuais e em nuvem, sem necessidade de agentes, garantindo cobertura total.
3.7. A solução deve ser instalado de modo a detectar ameaças avançadas no ambiente da **CONTRATANTE**, inspecionando o tráfego de rede, independente de agentes instalados;
3.8. A solução deve ser instalado a fim de detectar ameaças avançadas no ambiente da **CONTRATANTE**, inspecionando o tráfego de rede, independente de agentes instalados;
3.9. A solução deve aplicar técnicas de análise de tráfego avançadas baseadas em aprendizagem de máquina;
3.10. A solução deve atuar com técnicas de detecção e resposta específicos para modelos de detecção focados em rede, de forma a identificar comportamentos maliciosos;
3.11. A solução deve permitir que seja implantado em linha com o tráfego de rede e em modo de espelhamento de rede;
3.12. Caso seja implementada em linha na rede da **CONTRATANTE**, o sensor deve permitir a criação de regras de by-pass para casos de falhas de interface;
3.13. Deve suportar o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;
3.14. Durante a inspeção do tráfego de rede em tempo real, o sensor deverá ser capaz de identificar anomalias na rede e gerar alertas em casos de tráfego suspeito;
3.15. Deve implementar características de Network Detection and Response baseado em comportamento;
3.16. Quando implantada em linha com a rede da **CONTRATANTE**, o sensor deve ter a capacidade de analisar tráfego TLS, sem necessidade de licenciamento adicional;
3.17. Deve identificar ameaças direcionadas avançadas e persistentes (APT);
3.18. Deve analisar possíveis fases de um ataque direcionado, identificando tentativas de coletas de informação, movimentação lateral, exfiltração de dados, descoberta de dispositivos e comunicações de comando e controle (C&C);
3.19. Deve identificar e mapear possíveis pontos de entrada na rede que possam ser exploradas por atacantes;
3.20. Deve prover automatizações para bloqueio de ameaças identificadas a partir da inspeção de rede;
3.21. A solução deve inspecionar a rede a fim de analisar, no mínimo os protocolos: HTTP, HTTPS, LDAP, FTP, Telnet, WebSocket, SMTP, POP3, DNS, SMB, RDP, Kerberos, IRC, VNC, SQL, MYSQL e ARP.
3.22. Deve permitir análise de arquivos em sandbox, permitindo identificar ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, vulnerabilidades conhecidas e arquivos maliciosos no tráfego de rede, de forma automática e quando aplicável;
3.23. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos executáveis (scripts), PDF´s, executáveis, PPTX, DOCX, XLSX, LNK, ELF, CHM, RTF, ODP, DLLs, JAR, ZIP e RAR;
3.24. A solução de inspeção de rede, deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Linux nas distribuições (CentOS), Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019;
3.25. Deve suportar a criação de sandboxes que repliquem os sistemas operacionais e aplicações da **CONTRATANTE**, para avaliação do real impacto da ameaça no ambiente;
3.26. Possibilitar a predefinição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;

3.27. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em único ponto;
3.28. Deve possuir atualização automática de regras, sendo que estas devem ser disponibilizadas via internet pelo fabricante da solução;
3.29. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;
3.30. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;
3.31. Deve possuir interface web para busca e investigação local de incidentes;
3.32. Capacidade de detectar ameaças web derivadas de vulnerabilidades e downloads de conteúdo malicioso;
3.33. A solução deve ser capaz de analisar protocolos mascarados ou tunelados em ICMP, IP, UDP e TCP;
3.34. Deve ser capaz de detectar ameaças desconhecidas, ataques dirigidos e ameaças de dia zero, sendo que este módulo majoritariamente deve pertencer ao mesmo fabricante;
3.35. Deve permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo, múltiplas camadas de empacotamento e arquivos comprimidos;
3.36. Deve suportar o monitoramento de múltiplas interfaces de rede conectadas a diferentes VLANs e Switches;
3.37. Deve permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;
3.38. Deve possibilitar que modelos de detecção a nível de rede sejam customizados de acordo com as necessidades da **CONTRATANTE**;
3.39. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e escaneamentos de porta;
3.40. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de Servidor SMTP não autorizado e Servidor Proxy não autorizado;
3.41. Deve possuir regras que identifiquem comunicações streaming de mídia, peer-to-peer e instant messengers;
3.42. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:
3.43. Sumário das detecções;
    3.43.1. Visão Geral dos Incidentes de Segurança;
    3.43.2. Discriminação dos Tipos de Incidentes;
    3.43.3. Top Ameaças Analisadas;
    3.43.4. Top Hosts Infectados;
    3.43.5. Recomendações de Segurança;
    3.43.6. Executivos;
3.44. Deve possuir detalhes técnicos dos incidentes detectados;
3.45. Deve possuir estatística do tráfego analisado;
3.46. Deve possuir indicadores de risco do ambiente;
3.47. Recomendações de Segurança.
3.48. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e atualizada dinamicamente, hosts com alto nível de risco, classificando os tipos de eventos detectados;
3.49. Deve permitir o upgrade e downgrade de versão de firmware;
3.50. Deve ser capaz de identificar ameaças que afetam dispositivos móveis, especificamente aqueles baseados em IOS e Android;
3.51. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns e tunelamento de protocolo;
3.52. Deve ser capaz de detectar tentativas de escaneamento de rede;Deve ser capaz de detectar propagação de malwares na rede;
3.53. Deve ser capaz de detectar tentativas de força bruta em credenciais;
3.54. Deve ser capaz de detectar tentativas de roubo de informação;
3.55. Deve ser capaz de detectar ameaças que se replicam na rede;

3.56. Deve ser capaz de detectar Exploits na rede;
3.57. Deve replicar a comunicação captada por interface gráfica interativa, a fim de facilitar a compreensão dos alertas gerados;
3.58. Deve possuir interface gráfica que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas etc.;
3.59. Deve apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboard;
3.60. Deve permitir busca por informações de destino e origem de comunicações, incluindo: endereço IP, endereço MAC, domínio, protocolo e grupo de rede;
3.61. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;
3.62. Capacidade de salvar uma investigação antes de ser finalizada;
3.63. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;
3.64. Capacidade de gerar relatórios baseados nas investigações;
3.65. Deve permitir exportar sob demanda os logs padrões CSV ou PDF;
3.66. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;
3.67. Deve ser totalmente integrado com a console de gerência da plataforma do próprio fabricante, com objetivo de correlacionar as detecções do sensor de rede com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e gateway seguro;
3.68. Deverá ser capaz de identificar ameaças evasivas em tempo real atuando com análise profunda e inteligência para identificar e prevenir ataques;
3.69. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;
3.70. A solução de inspeção de rede deve ter a capacidade de integrar-se com a plataforma de gerência centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;
3.71. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:
    3.71.1. Uso de CPU
    3.71.2. Uso de Disco;
    3.71.3. Uso de Memória;
    3.71.4. Tráfego malicioso analisado;
    3.71.5. Todo o tráfego analisado.
3.72. A solução deverá ter integração com ferramentas de SIEM com pelo menos uma dessas soluções de mercado:NetWitness, Qradar, Splunk e Chronicle;
3.73. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:
3.74. Deverá suportar ao menos a integração com dois servidores syslogs;
3.75. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.
3.76. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;
3.77. A solução deve ter capacidade de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;
3.78. Deverá listar os 10 hosts mais críticos do ambiente da **CONTRATANTE**, de forma a categorizá-los de acordo com a severidade atual baseada em número e criticidade das detecções, segundo:
    3.78.1. Nível Crítico
    3.78.2. Nível Alto
    3.78.3. Nível Médio

3.78.4. Nível Baixo

3.79. Deverá correlacionar cada host listado a um alerta de investigação, quando aplicável;

3.80. As detecções de cada host listado deverão ser apresentadas com detalhes para devida investigação;

3.81. Deverá apresentar os logs de rede de maneira evidente e destaca por meio de rótulo e cor, a fim de diferenciar dos demais logs de outros sensores;

3.82. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

3.82.1. Computadores infectados;
3.82.2. Origem de infecções;
3.82.3. Estatísticas de ameaças;
3.82.4. Riscos potenciais de segurança;
3.82.5. Riscos de perda de informações;
3.82.6. Risco de sistema comprometido;
3.82.7. Risco de disseminação de ameaças;
3.82.8. Infecções de malware
3.82.9. Eventos suspeitos;

3.83. Deve permitir a configuração de alarmes personalizados, com base em investigações;

3.84. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

3.85. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado

3.86. A solução deve possuir recurso de prevenção de ameaças avançadas, com capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK MITRE Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução;

3.87. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

3.88. A partir de um alerta do sensor de rede, deve ser possível o bloqueio dos IPs e URLs envolvidos no contexto da detecção;

3.89. Deve mapear os métodos de requisições detectados ao longo de uma comunicação inspecionada, listando ao menos:

3.89.1. Requisições GET
3.89.2. Requisições POST
3.89.3. Requisições MOVED
3.89.4. Requisições NOT FOUND

3.90. A partir dos alertas gerados, deve correlacionar as máquinas, IPs e Hashs envolvidos, apontando possíveis indicadores de comprometimento (IOCs) ao ambiente da **CONTRATANTE**;

3.91. Os relatórios e logs deverão ser exportados nos formatos PDF, TXT ou CSV;

3.92. A solução deve por meio da integração com a plataforma de detecção e resposta, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos: Fortinet, Palo Alto ou Checkpoint;

4. Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses:

4.1. A solução deve fornecer uma console única para gerenciamento dos serviços de segurança, integrando-se com os outros componentes;

4.2. Capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

4.3. A console de administração deverá permitir o envio de notificações via SMTP

4.4. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

4.5. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
4.6. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
4.7. Deverá orquestrar todas as funcionalidades descritas;
4.8. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;
4.9. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;
4.10. Prover nota de risco para o ambiente de TI da **CONTRATANTE**, baseada em diversos fatores e comparável com a de outras organizações da mesma região, indústria ou tamanho;
4.11. Deve suportar integração com os seguintes serviços de diretório:
4.12. Microsoft Active Directory;
4.13. Azure Active Directory;
4.14. Open LDAP;
4.15. A nota de risco deve ser calculada continuamente e deve ser possível analisar seu comportamento ao longo do tempo de forma gráfica;
4.16. As fontes de dados para cálculo do risco não devem se limitar àquelas desenvolvidas pelo FABRICANTE, sendo aceitas soluções de terceiros;
4.17. Deve prover um sumário dos itens referentes ao escopo de risco cibernético mapeado, apresentando as ações a serem executadas, a fim de diminuir o valor numérico do risco;
4.18. Deve apresentar alertas de possíveis comprometimentos de contas;
4.19. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
4.20. Suporte a atribuição de papéis funcionais, para implantação de política de controle de acesso baseada em papéis (RBAC - Role-based access control);
4.21. A console de administração deve metrificar o nível de risco cibernético do ambiente, baseando-se na telemetria gerada pelas demais soluções citadas nos itens 1.1, 1.2, 1.3,1.4 e 1.5;
4.22. Deve mapear as vulnerabilidades existentes nas máquinas, elencando quanto ao nível de CVSS score e impacto no ambiente, apresentando as vulnerabilidades que estão sofrendo algum tipo de exploração a nível das máquinas e da rede;
4.23. Deve apontar as vulnerabilidades com o maior índice de risco presentes no ambiente;
4.24. Deve apresentar os alertas de ameaças direcionadas, suspeitas, e de dia zero, a fim de identificar possíveis ações maliciosas no ambiente da **CONTRATANTE**;
4.25. Tais alertas devem apresentar:
4.26. A relação entre máquinas e IPs;
4.27. Requisições de rede;
4.28. URLs e Hashs;
4.29. Usuários e domínios;
4.30. Deve ser possível customizar os modelos de detecção, a fim de atender as necessidades da **CONTRATANTE**;
4.31. Deve ser possível criar exceções para os modelos de detecção;
4.32. A solução deve ser baseada em inteligência artificial e aprendizagem de máquina, a fim de potencializar os níveis de detecção de comportamentos anômalos;
4.33. Deve possuir rede global de inteligência de ameaças;
4.34. Deve apresentar alertas caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais;
4.35. Deve possuir módulo de pesquisa forense de ameaças, possibilitando a coleta de logs remotamente;
4.36. Deve suportar conexões remotas via agente da solução, sendo possível:
    4.36.1. Coleta de evidências forenses;
    4.36.2. Isolar a máquina;
    4.36.3. Terminar processo;
    4.36.4. Dump de memória;

4.36.5. Listar as portas abertas na máquina;
4.36.6. Listar configurações de rede;
4.36.7. Listar os diretórios;
4.36.8. Deletar arquivo ou diretório;

4.37. Enumerar a superfície de ataque da **CONTRATANTE**, dependendo das fontes de dados conectadas, compreendendo:

4.38. As estações de trabalho, os servidores e os dispositivos móveis da **CONTRATANTE**;

4.39. Os usuários da **CONTRATANTE**, apontando inclusive aqueles que detêm poderes administrativos;

4.40. As aplicações acessadas por usuários e dispositivos da **CONTRATANTE**, apontando inclusive aquelas que passaram por recente vazamento de dados;

4.41. Os ativos mantidos pela **CONTRATANTE** sob custódia de Provedores de Serviços em Nuvem;

4.42. Os domínios da **CONTRATANTE**, suportando ao menos 10 domínios diferentes;

4.43. Os subdomínios da **CONTRATANTE**;

4.44. Os IPs Públicos associados à **CONTRATANTE** e seus respectivos hosts;

4.45. As portas de comunicação/serviços abertos em cada host público;

4.46. Deve mapear via rede da **CONTRATANTE** os dispositivos existentes e apontar aqueles que não são gerenciados pelos agentes da solução;

4.47. Deve apresentar a relação de máquinas que o usuário acessou;

4.48. Deve listar os alertas identificados no ambiente e correlacionar com técnicas, táticas e procedimentos do framework MITRE ATT&CK;

4.49. Tais alertas devem seguir o seguinte escopo de severidade quanto ao nível de risco:

4.49.1. Risco Crítico;
4.49.2. Risco Alto;
4.49.3. Risco Médio;
4.49.4. Risco Baixo.

4.50. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

4.51. Deve haver correlação entre eventos de detecção, a fim de apresentar um possível incidente de segurança;

4.52. Deve suportar que o usuário manualmente correlacione alertas em um incidente;

4.53. Deve possibilitar que um usuário atribua o alerta a outro usuário;

4.54. Deve possuir campo para observações e notas;

4.55. Cada alerta deverá ser listado com um status de:

4.55.1. Novo alerta;
4.55.2. Alerta sendo tratado;
4.55.3. Falso Positivo
4.55.4. Fechado;
4.55.5. Verdadeiro Positivo.

4.56. Deve listar todos as ações de resposta executadas, apresentando o status de cada uma;

4.57. Deve possuir lista customizável de indicadores de comprometimento e objetos suspeitos;

4.58. Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;

4.59. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos.

4.60. Deve informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

4.61. A solução deve mostrar, pelo menos, o timestamp e objetos envolvidos (comandos, processos, usuários, servidores);

4.62. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
4.63. Para a integração com o sensor de inspeção de rede, a solução deverá receber os alertas advindos do sensor de inspeção de rede, processá-los e analisá-los, a fim de identificar os riscos de segurança existentes;
4.64. Com base na telemetria do sensor de inspeção de rede, deverá replicar a sequência de requisições ocorridas dentre as máquinas da rede da **CONTRATANTE** e endereços externos, a fim de apresentar eventos correlacionados para permitir investigações forenses;
4.65. Deverá correlacionar os logs do sensor de inspeção de rede e indicar quais vulnerabilidades existentes nas máquinas estão sofrendo tentativas de exploração;
4.66. A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deverá ser capaz de disponibilizar as regras de proteção indicadas;
4.67. Deverá ser capaz de automaticamente enviar as regras de proteção frente as vulnerabilidades por meio da console do gerenciamento e aplicá-las diretamente no appliance de Prevenção de Intrusão de rede de 2º Geração, sem necessidade de ação manual;
4.68. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;
4.69. Com base na telemetria gerada, deve apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;
4.70. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
4.71. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
4.72. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
4.73. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
4.74. Deve ser capaz de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
4.75. Capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;
4.76. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;
4.77. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
4.78. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
4.79. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
4.80. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;
4.81. Reagir programaticamente, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da **CONTRATANTE**;
4.82. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
4.83. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;
4.84. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;
4.85. Deve elencar o nível de risco cibernético dos usuários da **CONTRATANTE**, identificando os que apresentem comportamentos anômalos de:
4.85.1. Comprometimento de credencial;

4.85.2. Ataque de força bruta;
4.85.3. Login atípico ou impossível;
4.85.4. Login via IPs suspeitos;
4.85.5. Múltiplas tentativas de login com sucesso e insucesso;

4.86. A partir da dos alertas de risco dos usuários, deve ser possível enviar ações de mitigação de risco:
4.86.1. Forçar reset de senha;
4.86.2. Desabilitar conta do usuário no serviço de diretório;
4.86.3. Forçar sign-out do usuário;

4.87. Deverá centralizar as ações e estender a visibilidade sob todas as funcionalidades, sendo elas:
4.88. inspeção de rede contra ameaças avançadas com detecção e resposta;
4.89. Detecção e resposta para Servidores e cargas de trabalho;
4.90. Detecção e resposta para estações de trabalho;
4.91. Controle de acesso a aplicações internas, externas e na nuvem;
4.92. Prevenção de Intrusão de rede;
4.93. A solução deverá prover relatórios contendo no mínimo as seguintes informações:
4.93.1. Top Ameaças;
4.93.2. Top usuários com risco;
4.93.3. Top vulnerabilidades identificadas;
4.93.4. Top Hosts com detecções;
4.93.5. Sumário de tráfego de rede inspecionado;

5. Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses:

5.1. O appliance físico deve ter capacidade de monitorar tráfego de até 40 Gbps.
5.2. Deve suportar inspeção de tráfego em tempo real com capacidade mínima de 10 Gbps.
5.3. Processamento otimizado para análise de ameaças avançadas e inspeção de múltiplos protocolos.
5.4. Suporte a análise de tráfego inline e out-of-band.
5.5. O hardware deve suportar pelo menos 25 sandboxes customizadas para análise de ameaças.
5.6. Não serão aceitos appliances de Unified Threat Management (UTM) ou Next-Generation Firewall (NGFW) para monitoramento de tráfego, mesmo que possuam recursos/licenciamento para análise de ameaças em rede.
5.7. Deve suportar o uso de portas espelhadas de switch (mirror port) para monitoramento e detecção de riscos à segurança.
5.8. Deve suportar o monitoramento de múltiplas interfaces de rede conectadas a diferentes VLANs e switches.
5.9. Deve possuir interface de gerenciamento 1 GbE de cobre ou de até 25 GbE SFP28.
5.10. Múltiplas interfaces de rede 1GbE e 10GbE, com suporte a agregação de links.
5.11. Formato 2U para montagem em rack.
5.12. Processador multi-core de alto desempenho, otimizado para cargas de segurança de rede.
5.13. Memória RAM mínima de 160 GB para processamento simultâneo de múltiplas sessões.
5.14. Armazenamento interno em SATA com capacidade mínima de 2 TB para retenção de dados e logs.
5.15. Ventilação e refrigeração adequadas para operação contínua em ambientes de datacenter.
5.16. Duas fontes de alimentação redundantes (1+1), hot-swap, garantindo alta disponibilidade.
5.17. Suporte a alimentação elétrica de 100 VAC a 240 VAC.
5.18. Suporte a alimentação em corrente contínua de 40 VDC a 60 VDC.
5.19. Inicialização segura (Secure Boot) e firmware assinado digitalmente.
5.20. Proteção contra acesso físico não autorizado.
5.21. Suporte a criptografia de dados em repouso e em trânsito.

5.22. Atender a padrões internacionais de segurança e interoperabilidade (CE, FCC, RoHS).
5.23. Compatibilidade com políticas corporativas de segurança e privacidade.

6. Serviço de detecção e resposta (MDR) do fabricante para o item de inspeção de rede contra ameaças avançadas pelo período de 60 meses:

6.1. A solução deverá possuir monitoramento avançado da plataforma de detecção e resposta estendida em modo 24x7.
6.2. O Serviço de Monitoramento avançado é aquele resultante de vários serviços de cibersegurança prestados em conjunto com o objetivo de oferecer observabilidade e respostas aos alertas gerados de potenciais ameaças e ataques cibernéticos.
6.3. serviço de monitoramento avançado é composto de equipes técnicas especializadas em cibersegurança, atendimento de requisições e respostas a incidentes, e soluções de tecnologia.
6.4. O serviço deve operar na modalidade 24 horas 7 dias por semana, baseado na plataforma de Detecção e Resposta Estendida (XDR).
6.5. Deve auxiliar a **CONTRATANTE** no processo de implantação das soluções, de forma a balizar tais ações com base nas melhores práticas do fabricante, acompanhamento de instalações das soluções em fases de homologação e apoio nas configurações necessárias;
6.6. Deve ser elencado o panorama de vulnerabilidades existentes no ambiente da **CONTRATANTE**, apresentando recomendações para aplicação de patchs;
6.7. Apoio na criação e customização dos playbooks de resposta automatizada da solução;
6.8. Deve prover celeridade na resolução de chamados de suporte técnico, atuando com SLO de até 1 Hora;
6.9. Deve fornecer acesso a um gestor de serviços do fabricante, para comunicações gerais acerca do ambiente e das entregas **CONTRATADAS**, agindo como um ponto único de contato;
6.10. O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato;
6.11. O serviço de monitoramento avançado deve validar a ingestão de logs pelos sensores da plataforma de Detecção e Resposta Estendida;
6.12. Quando necessário, a **CONTRATANTE** poderá solicitar aconselhamento sobre processos de melhoria, atualização ou migração das soluções atuais para o gestor de serviços do fabricante;
6.13. O serviço em questão deve estar atrelado diretamente às tecnologias **CONTRATADAS** neste processo a fim de facilitar a correlação das informações e dar uma rápida resposta, a saber:
6.13.1. Plataforma de detecção e resposta estendida - XDR;
6.13.2. Sensor de inspeção avançada de rede com detecção e resposta - NDR;
6.14. Os relatórios dos incidentes analisados e reportados devem ser fornecidos com frequência mínima mensal para o ambiente;
6.15. O serviço deve dispor de ações de caça de ameaças com base nos alertas gerados pela plataforma de Detecção e Resposta Estendida;
6.16. O time de monitoramento do fabricante deve atuar com análise dos indicadores de ameaças e campanhas de malware identificadas no ambiente;
6.17. Deverá monitorar os alertas gerados pela plataforma de detecção e resposta estendida – XDR em regime 24 horas por dia e 7 dias por semana;
6.18. Os alertas gerados deverão ser analisados e categorizados segundo criticidade: Alta, Média e Baixa, os quais devem ser informados a **CONTRATANTE** para ações particulares;
6.19. Deve ser possível, em comum acordo com a **CONTRATANTE**, que sejam tomadas ações de remediação em casos de detecção de ameaças eminentes, via time de monitoramento do fabricante;
6.20. Deve prover análise de possíveis incidentes, mapeando o ponto de entrada do ataque, escopo afetado, recomendações de contenção e melhorias futuras;
6.21. O fabricante deverá analisar os alertas gerados na plataforma e deverá reportar em casos de possíveis indícios de fases iniciais ou em curso de ataques cibernéticos;

6.22. Deve identificar, perante os alertas gerados pela plataforma, a cadeia de causa raiz e determinar o perfil da ameaça, informando tais análises a **CONTRATANTE**;
6.23. Deve ocorrer buscas de novos IOCs identificados no ambiente, com base na inteligência de ameaças do fabricante;
6.24. O fabricante deverá aplicar análises de configurações detalhadas das soluções com base na documentação de melhores práticas da plataforma;
6.25. Ao final de cada validação de saúde das soluções o fabricante deverá apresentar um relatório detalhado;
6.26. O fabricante deverá disponibilizar ao menos 40 hrs por ano de serviços especializados de análise profunda de incidentes de segurança e respostas a incidente, durante a vigência do contrato;
6.27. A **CONTRATADA** deve identificar o momento oportuno apara acionamento do serviço de resposta a incidentes;
6.28. A atuação do time de resposta a incidentes do fabricante deve ocorrer de maneira única, cobrindo as 40hrs, dentro o contrato de 60 meses;
6.29. Ao final das atividades de incidente e resposta o fabricante deverá apresentar relatório conclusivo sobre as atividades realizadas, incluindo escopo identificado do incidente, causa raiz quando aplicável, medidas de contensão e recomendações de melhores práticas contra fragilidades identificadServiço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses:

7. Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS):

7.1. A solução ofertada deverá ser entregue como appliance do próprio fabricante, não sendo aceitos virtual appliances de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da solução-software e do hardware são empresas diferentes);
7.2. A fim de priorizar performance na entrega do sistema de inspeção de instrução de rede, não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede;
7.3. O NGIPS deverá suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, onde o arquivo padrão SNORT deverá ser importado e convertido para o padrão utilizado pela solução ofertada;
7.4. Para atendimento do bypass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de bypass, que poderá ser embutido ou externo;
7.5. O equipamento NGIPS deve atender às seguintes especificações:
7.6. Cada IPS deverá estar licenciado para inspecionar throughput de 10 Gbps;
7.7. Deverá gerar latência igual ou inferior a 40 Microsegundos;
7.8. Deverá suportar pelo menos 650.000 novas conexões por segundo;
7.9. Deverá suportar pelo menos 120 milhões de sessões concorrentes;
7.10. Deverá suportar pelo menos 5700 novas conexões SSL por segundo;
7.11. Deverá suportar inspeção de tráfego SSL de até 8 Gbps;
7.12. A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);
7.13. Os filtros providos pelo NGIPS deverão permitir a seleção de ações de resposta.
7.14. As ações deverão possibilitar: Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Captura de Pacotes), além de ações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados tráfegos / ataques de acordo com condições encontradas no ambiente como, por exemplo, permitir as 1000 primeiras conexões de um único IP para determinado tráfego de rede em um período de 15 minutos. Após a conexão 1001 na mesma janela de tempo, a ação deverá ser alternada para bloqueio;

7.15. A solução NGIPS deverá suportar assinaturas de IPS para proteger contra-ataques, detectar exploits, detectar roubo de informações, detecção de virus, detecção de spywares, detectar tentativas de reconhecimento de rede, possuir regras que ajudem a controlar comportamentos de rede (exemplo: permitir ou bloquear resposta de comandos ping, detectar falhas de autenticação no MS SQL Server), possuir regras que blindem equipamentos de rede contra ataques que explorem vulnerabilidades, regras que efetuem a normalização de tráfego, ou seja, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como youtube, skype, TOR e facebook;

7.16. Os filtros do NGIPS precisam estar segmentados por categorias, com o objetivo de facilitar o gerenciamento da solução. Deverão existir pelo menos as seguintes categorias: Políticas de Segurança, Exploits, Normalização de Tráfego, Vírus, Reconhecimento de Rede, P2P e Vulnerabilidades;

7.17. O total de filtros disponíveis na solução (não necessariamente para uso simultâneo) não deve ser inferior a 16.000;

7.18. A solução NGIPS deverá ser capaz de permitir a criação e uso de políticas de segurança granulares baseados nos seguintes métodos:

7.19. Por NGIPS (todos os segmentos de rede de um IPS);

7.20. Por segmento físico, podendo selecionar o modo bi-direcional ou unidirecional (permitindo ativar a política de segurança nos sentidos de comunicação de A > B e de B > A [na mesma política de segurança]. Ou com política de segurança dedicada de A > B e de B > A);

7.21. Por TAG de VLAN (802.1Q), de forma direcional e bi-direcional;

7.22. Por CIDR (Range de endereços IP);

7.23. Baseado no horário do dia.

7.24. A solução NGIPS deverá ser capaz de detectar e bloquear ataques de reconhecimento de rede;

7.25. A solução NGIPS deverá prover filtros de detecção de aplicações tais como P2P, Online Games, permitindo a ativação de controles de banda;

7.26. A Inspeção de rede com o NGIPS deverá cobrir o throughput real do ambiente da **CONTRATADA**;

7.27. Deverá possuir ferramenta para criação de filtros customizados, sendo que estes deverão permitir a customização de parâmetros tais como:

7.28. Nome do filtro;

7.29. Descrição do filtro;

7.30. Protocolo, permitindo a criação de filtros de proteção baseados nos protocolos IPv4, ICMPv4, UDP, TCP, HTTP, IPv6 e ICMPv6;

7.31. Severidade do filtro, devendo possuir pelo menos 4 níveis;

7.32. Customização da categoria do filtro;

7.33. Classe do filtro (devendo possuir pelo menos as classes DoS, Exploit, Virus e Acesso);

7.34. Gatilhos de acionamento (triggers), onde parâmetros ou informações/dados contidos no streaming de rede serão utilizados como gatilho para validação de parâmetros adicionais da regra;

7.35. Detecção de payload, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede;

7.36. Detecção de payload dentro do protocolo HTTP, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também deverá permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload;

7.37. Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP;

7.38. A solução NGIPS ofertada deverá suportar processamento de tráfego assimétrico;

7.39. Deverá ser possível colocar a solução em modo bypass total forçado;

7.40. A solução NGIPS deverá possuir Machine Learning, ou seja, deverá possuir filtros que implementem Machine Learning na detecção de, por exemplo, conteúdo obfuscado em HTML associado/relacionado a exploit kits;

7.41. Deverá possuir filtros de gerenciamento de tráfego, ou seja, deverá ser possível criar regras para controlar o tráfego no sentido de A para B, de B para A, liberando o tráfego (com inspeção de riscos de segurança), liberando o tráfego (sem inspecioná-lo, confiando na conexão), bloqueando o tráfego, e permitindo a criação de políticas de controle de banda, permitindo limitar, por exemplo, determinado fluxo de dados de rede a 100kbps;
7.42. A solução de NGIPS deverá possuir controles de proteção contra-ataques de DDOS, atuando como um SYN PROXY;
7.43. A solução de NGIPS deverá possuir filtros que detectem a tentativa de uso de TOR, TeamViewer;
7.44. A solução de NGIPS deverá detectar e bloquear tráfego Skype;
7.45. A solução de NGIPS deverá detectar e permitir o bloqueio de tunelamento de conexões DNS;
7.46. A solução de NGIPS deverá possuir assinatura que permita a validação de requisições HTTP 2.0;
7.47. A solução de NGIPS deve bloquear nativamente a transferência de arquivos maliciosos via FTP;
7.48. A solução deve detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos.
7.49. solução de NGIPS ofertada precisa entregar detalhes sobre a cobertura para vulnerabilidades Microsoft reportadas nos últimos 12 meses;
7.50. O fabricante da solução NGIPS deve prover estatísticas do número de vulnerabilidades de dia zero descobertas nos últimos 5 anos.;
7.51. O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research);
7.52. A solução NGIPS deverá suportar atualizações automáticas dos filtros/assinaturas, possuindo frequência de atualizações mínima semanal (fabricante deverá entregar 1 atualização por semana);
7.53. Sempre que a solução NGIPS atualizar-se, o novo pacote de atualizações deverá conter descritivo visualizável na própria solução (console local do NGIPS ou gerenciamento centralizado), indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos. O mesmo deve ocorrer para os filtros de ameaças (malwares), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução.
7.54. Correlação de Informações e Consultas em Nuvem;
7.55. Reputação de Endereços IP, DNS e URLs;
7.56. A solução NGIPS ofertada precisa permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de DNS e URLs;
7.57. O serviço de reputação deverá contar com categorias tais como: Malware, Botnet, Spyware, SPAM, TOR, Web, Application Attackers, P2P e Network Worm;
7.58. Deverá ser possível criar exceções baseadas em domínio e endereços IP, assim como deverá ser possível estabelecer as políticas de reputação individuais para cada perfil de segurança em uso no ambiente;
7.59. A base de reputação IP deverá suportar IPv4 e IPV6;
7.60. A base de reputação IP deverá ser baseada em informações do próprio fabricante, e permitir o uso de bases terceiras;
7.61. Os filtros de reputação de IP deverão atuar tanto no sentido inbound quanto outbound;
7.62. As políticas de reputação deverão permitir a customização de ações tanto para bloquear ou permitir determinados acessos;
7.63. Deverá ser possível criar filtros de controle de acesso inbound e outbound baseados em geolocalização.
7.64. Deverá possuir módulos que atuem com proteção avançada contra ameaças;

7.65. A solução NGIPS deverá possuir funcionalidade que permita a identificação e proteção contra atividades maliciosas relacionadas a virus e spywares, no sentido inbound e outbound;
7.66. A solução NGIPS deverá possuir assinaturas de proteção contra malwares;
7.67. As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de comando e controle através da inspeção do tráfego de rede;
7.68. A solução deverá ser capaz de interromper atividades maliciosas tais como ransomware, fuga de dados, click fraud, etc;
7.69. Deverá bloquear ameaças do tipo drive-by-downloads;
7.70. Deverá detectar atividades de comunicação com servidores de comando e controle de botnets;
7.71. Os filtros de malware deverão ser atualizados de forma regular pelo fabricante da solução.
7.72. Deverá atuar com alta disponibilidade aderente a estrutura da **CONTRATANTE**;
7.73. A solução de NGIPS deve suportar a operação de forma redundante, com possíveis cenários de operação Ativo-Passivo e Ativo-Ativo;
7.74. A gerência da solução deve permanecer ativa em caso de indisponibilidade dos NGIPS e possui cenários de alta disponibilidade;
7.75. A solução NGIPS deverá suportar software bypass;
7.76. Em caso de atualizações ou reinicializações do NGIPS, a solução não deverá gerar nenhuma interrupção de rede.
7.77. A solução NGIPS precisa suportar ser gerenciada de maneira centralizada por solução fornecida pelo mesmo fabricante;
7.78. A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 2 sensores de NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS;
7.79. A solução de gerenciamento centralizado necessita operar em modo alta disponibilidade, sendo que se o primeiro servidor falhar, o segundo deverá continuar operando normalmente sem prejuízos ao gerenciamento do ambiente;
7.80. A solução de gerenciamento centralizado deverá possuir um painel de monitoramento de eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques, etc;
7.81. A solução de gerenciamento centralizado deverá possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução NGIPS, devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e permitindo adicionar e remover endereços IP suspeitos da quarentena dos NGIPS;

8. Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS):

8.1. O equipamento deve realizar bloqueio inline de ameaças, garantindo inspeção e resposta em tempo real.
8.2. O hardware deve possuir capacidade de ativar funcionalidades de NDR (Network Detection and Response) para análise aprofundada de tráfego que não corresponde a regras previamente definidas.
8.3. O equipamento deve permitir escalabilidade em modo stacking, suportando até 200 Gbps de throughput agregado.
8.4. Em formato 1U, o hardware deve ser capaz de realizar análise de tráfego de até 40 Gbps.
8.5. O equipamento deve possuir mecanismos de fail-open, permitindo a passagem do tráfego em caso de falhas internas.
8.6. Deve possuir duas fontes de alimentação redundantes (1+1), hot-swap, garantindo alta disponibilidade.
8.7. O hardware deve incluir bypass embutido, assegurando continuidade do tráfego em situações críticas.

8.8. A arquitetura do equipamento deve ser modular e hot-swap, permitindo substituição rápida de interfaces em caso de falha, sem necessidade de troca completa do equipamento.
8.9. O equipamento deve permitir bypass interno via backbone a través da gerencia remota, facilitando processos de troubleshooting.
8.10. Todas as interfaces (fibra e cobre) devem possuir bypass automático, garantindo continuidade do tráfego em caso de falha elétrica ou de hardware.
8.11. O equipamento deve suportar implementação em links redundantes, operando em modo ativo-ativo ou ativo-passivo.
8.12. Deve ser capaz de analisar tráfego assimétrico, mantendo visibilidade e controle.
8.13. O hardware deve suportar no mínimo 1.000.000 de novas conexões por segundo.
8.14. Deve suportar até 300.000.000 de conexões simultâneas.
8.15. A latência máxima do equipamento deve ser inferior a 60 microssegundos.
8.16. Deve suportar no mínimo 20.000 novas conexões TLS por segundo.
8.17. Deve suportar até 250.000 conexões TLS simultâneas.
8.18. Deve ser capaz de armazenar até 2.500 certificados digitais.
8.19. Deve possuir interface de gerenciamento 1 GbE de cobre ou de até 25 GbE SFP28
8.20. Deve disponibilizar duas interfaces QSFP28-DD dedicadas para stacking.
8.21. As dimensões máximas do equipamento devem ser: 18,54” (L) x 28,90” (P) x 1,73” (A).
8.22. Deve suportar alimentação elétrica de 100 VAC a 240 VAC.
8.23. Deve suportar alimentação em corrente contínua de 40 VDC a 60 VDC.
8.24. O consumo máximo de energia deve ser de 1.000 W.
8.25. O equipamento deve operar com frequência de alimentação elétrica entre 47 Hz e 63 Hz, com tolerância nominal de 50 Hz a 60 Hz.
8.26. Deve possuir ventiladores hot-swap, permitindo manutenção sem interrupção.
8.27. A faixa de temperatura operacional deve ser de 0 °C a 40 °C.
8.28. O HW debe suportar humidade relativa desde 5% a 95% sem condensação
8.29. O HW deve estar em conformidade com as seguintes normas de emissões eletromagnéticas: EN55032:2014/A11:2020 e CISPR 32:2015
8.30. O HW deve estar em conformidade com as seguintes normas de inmunidade eletromagnética: EN55035:2017/A11:2020 e CISPR 35:2015
8.31. O HW deve estar em conformidade com as seguintes normas de harmônicos de corrente e flutuações de tensão: EN61000-3-2:2014 e EN61000-3-3:2013/A1:2019
8.32. O HW deve estar em conformidade com a norma de segurança elétrica IEC 62368-1 (edições de 2014 ou 2018). Alternativamente, será aceita a norma IEC 60950-1:2005, com as emendas AMD1:2009 e AMD2:2013, desde que acompanhada de documentação técnica que comprove certificação válida e compatibilidade com os requisitos de segurança exigidos.
8.33. O equipamento deve operar normalmente em altitudes de até 2.000 metros acima do nível médio do mar (MSL), sem prejuízo de desempenho ou segurança.
8.34. O equipamento deve apresentar um MTBF (Mean Time Between Failures) mínimo de 150.000 horas a 25 °C, comprovado por testes ou certificações de confiabilidade que garantam a robustez e a durabilidade do produto em operação contínua.

9. Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses:

9.1. A solução deverá possuir monitoramento avançado da plataforma de detecção e resposta estendida em modo 24x7.
9.2. O Serviço de Monitoramento avançado é aquele resultante de vários serviços de cibersegurança prestados em conjunto com o objetivo de oferecer observabilidade e respostas aos alertas gerados de potenciais ameaças e ataques cibernéticos.

9.3. serviço de monitoramento avançado é composto de equipes técnicas especializadas em cibersegurança, atendimento de requisições e respostas a incidentes, e soluções de tecnologia.
9.4. O serviço deve operar na modalidade 24 horas 7 dias por semana, baseado na plataforma de Detecção e Resposta Estendida (XDR).
9.5. Deve auxiliar a **CONTRATANTE** no processo de implantação das soluções, de forma a balizar tais ações com base nas melhores práticas do fabricante, acompanhamento de instalações das soluções em fases de homologação e apoio nas configurações necessárias;
9.6. Deve ser elencado o panorama de vulnerabilidades existentes no ambiente da **CONTRATANTE**, apresentando recomendações para aplicação de patchs;
9.7. Apoio na criação e customização dos playbooks de resposta automatizada da solução;
9.8. Deve prover celeridade na resolução de chamados de suporte técnico, atuando com SLO de até 1 Hora;
9.9. Deve fornecer acesso a um gestor de serviços do fabricante, para comunicações gerais acerca do ambiente e das entregas **CONTRATADAS**, agindo como um ponto único de contato;
9.10. O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato;
9.11. O serviço de monitoramento avançado deve validar a ingestão de logs pelos sensores da plataforma de Detecção e Resposta Estendida;
9.12. Quando necessário, a **CONTRATANTE** poderá solicitar aconselhamento sobre processos de melhoria, atualização ou migração das soluções atuais para o gestor de serviços do fabricante;
9.13. O serviço em questão deve estar atrelado diretamente às tecnologias **CONTRATADAS** neste processo a fim de facilitar a correlação das informações e dar uma rápida resposta, a saber:
9.14. Plataforma de detecção e resposta estendida - XDR;
9.15. Sensor de inspeção avançada de rede com detecção e resposta - NDR;
9.16. Os relatórios dos incidentes analisados e reportados devem ser fornecidos com frequência mínima mensal para o ambiente;
9.17. O serviço deve dispor de ações de caça de ameaças com base nos alertas gerados pela plataforma de Detecção e Resposta Estendida;
9.18. O time de monitoramento do fabricante deve atuar com análise dos indicadores de ameaças e campanhas de malware identificadas no ambiente;
9.19. Deverá monitorar os alertas gerados pela plataforma de detecção e resposta estendida – XDR em regime 24 horas por dia e 7 dias por semana;
9.20. Os alertas gerados deverão ser analisados e categorizados segundo criticidade: Alta, Média e Baixa, os quais devem ser informados a **CONTRATANTE** para ações particulares;
9.21. Deve ser possível, em comum acordo com a **CONTRATANTE**, que sejam tomadas ações de remediação em casos de detecção de ameaças eminentes, via time de monitoramento do fabricante;
9.22. Deve prover análise de possíveis incidentes, mapeando o ponto de entrada do ataque, escopo afetado, recomendações de contenção e melhorias futuras;
9.23. O fabricante deverá analisar os alertas gerados na plataforma e deverá reportar em casos de possíveis indícios de fases iniciais ou em curso de ataques cibernéticos;
9.24. Deve identificar, perante os alertas gerados pela plataforma, a cadeia de causa raiz e determinar o perfil da ameaça, informando tais análises a **CONTRATANTE**;
9.25. Deve ocorrer buscas de novos IOCs identificados no ambiente, com base na inteligência de ameaças do fabricante;
9.26. O fabricante deverá aplicar análises de configurações detalhadas das soluções com base na documentação de melhores práticas da plataforma;
9.27. Ao final de cada validação de saúde das soluções o fabricante deverá apresentar um relatório detalhado;
9.28. O fabricante deverá disponibilizar ao menos 40 hrs por ano de serviços especializados de análise profunda de incidentes de segurança e respostas a incidente, durante a vigência do contrato;

9.29. A **CONTRATADA** deve identificar o momento oportuno apara acionamento do serviço de resposta a incidentes;

9.30. A atuação do time de resposta a incidentes do fabricante deve ocorrer de maneira única, cobrindo as 40hrs, dentro o contrato de 60 meses;

9.31. Ao final das atividades de incidente e resposta o fabricante deverá apresentar relatório conclusivo sobre as atividades realizadas, incluindo escopo identificado do incidente, causa raiz quando aplicável, medidas de contensão e recomendações de melhores práticas contra fragilidades identificada. Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses:

10. Serviço de Instalação das soluções CONTRATADAS:

10.1. Nesta etapa, compreende-se a instalação e configuração da solução **CONTRATADA**, contados a partir da emissão da Ordem de Serviço (OS);

10.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução **CONTRATADA**, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

10.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para a instalação, a configuração e a entrega da solução **CONTRATADA**. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

10.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós-instalação da solução, matriz de responsabilidade, plano de comunicação;

10.5. Durante esta etapa, a equipe da **CONTRATADA** deverá estar presente nos horários de instalação definidos pelo **CONTRATANTE**. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

10.6. O **CONTRATANTE** disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

11. Serviços de treinamento das soluções CONTRATADAS:

11.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

11.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

11.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos: a) Instalação do módulo de gerenciamento central; b) Instalação do software de Endpoint Protection em estações de trabalho e servidores; c) Descrição e configuração de todas as funcionalidades **CONTRATADAS** da solução; d) Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

11.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A **CONTRATADA** é responsável por fornecer

apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

11.5. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

12. Serviço de suporte mensal das soluções CONTRATADAS:

O serviço de suporte proativo, corretivo e para resposta a incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.

12.1. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

12.2. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada.

12.3. Deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

12.4. Suporte Proativo

12.4.1. O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente.

12.4.2. A **CONTRATADA** deverá notificar a **CONTRATANTE** sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos.

12.4.3. Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas os produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro.

12.4.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e ontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos.

12.4.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas.

12.4.6. A **CONTRATADA** deverá apresentar relatório contendo as ações adotadas para a solução do problema.

12.5. Suporte Corretivo

12.5.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional.

12.5.2. Serviço Especializado de Suportes corretivo para xx(xxxx) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução.

12.5.3. A **CONTRATADA** deverá: a) Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte; b) Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento; c) Garantir disponibilidade 24/7 para responder a incidentes crítico.

12.5.4. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

12.6. Resposta a Incidentes

12.6.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. Deverá ser realizada por profissionais especializados e certificados pelo fabricante.

12.6.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança.

12.6.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes.

12.6.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

PREGÃO ELETRÔNICO 90008/2026

ANEXO I B

DEMANDA DE SERVIÇOS

Item	Software	Quant.
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.	1.000
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.	1.000
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	2
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.	2
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	2
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses.	2
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	4
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	4
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.	4
10	Serviço de Instalação das soluções **CONTRATADAS**	3
11	Serviços de treinamento das soluções **CONTRATADAS**	3
12	Serviço de suporte mensal das soluções **CONTRATADAS**	60

PREGÃO ELETRÔNICO 90008/2026

ANEXO I C

ACORDO DE NIVEIS DE SERVIÇO E INTERRUPÇÃO DE SERVIÇO

1. SLA (Service Level Agreement)

1.1. Para fins deste Acordo, considera-se **Tempo de Detecção (MTTD)** o intervalo decorrido entre o início de um evento de segurança relevante e sua **primeira correlação/elevação de alerta no** console central da solução.

1.1.1. O MTTD máximo admitido para **eventos de alta criticidade** (ex.: exploração ativa, beaconing/C&C, ransomware em propagação, exfiltração) será de **até 5 (cinco) minutos**.
1.1.2. O MTTD máximo admitido para **eventos de média criticidade** será de **até 15 (quinze) minutos**.

1.2. Considera-se **Tempo de Resposta (MTTR)** o intervalo entre a abertura do incidente (registro do alerta como incidente) e a **aplicação da ação de contenção** (ex.: bloqueio de assinatura/regra, quarentena, segmentação ou playbook SOAR/MDR concluído).

1.2.1. O MTTR máximo para **incidentes de alta criticidade** será de **até 30 (trinta) minutos**.
1.2.2. O MTTR máximo para **incidentes de média criticidade** será de **até 2 (duas) horas**.

1.3. Disponibilidade do Serviço é o índice que mede o percentual de tempo em que cada **componente essencial** da solução permaneceu operacional no mês-calendário, nas condições normais de funcionamento:

a) **Plataforma de Gerenciamento (console, correlação, atualização de assinaturas)**: disponibilidade mínima de **99,7%** por mês;

b) **Módulos de Inspeção/Prevenção (NGIPS) em HA**: disponibilidade mínima de **99,7%** por mês;

c) **Sensores/Coletas NDR e conectores de telemetria**: disponibilidade mínima de **99,3%** por mês;

d) **Serviço MDR (24x7)**: disponibilidade mínima de **99,9%** para recepção, análise e triagem (triage) de alertas.

1.4. O serviço será considerado **indisponível** quando, verificada por registros da **CONTRATADA** ou da **CONTRATANTE**, ocorrer ao menos uma das seguintes situações até seu total restabelecimento e certificação:

1.4.1. Console inacessível ou sem capacidade de correlação/visualização;
1.4.2. Paralisação de inspeção/mitigação em NGIPS que afete tráfego protegido (modo inline) sem failover;
1.4.3. Perda de ingestão de telemetria NDR superior a 15 minutos para enlaces/segmentos críticos;
1.4.4. Inoperância do MDR 24x7 para abertura/triagem de incidentes.

1.5. A disponibilidade mensal, por componente, será calculada por:

$$D = (\frac{T_0 - T_i}{T_0}) \times 100$$

Onde: **D** = disponibilidade; **T_0** = total de minutos do mês; **T_i** = minutos de indisponibilidade no mês.

1.6. No cálculo de disponibilidade **não** serão computadas interrupções **programadas** (janela de manutenção) ou **de urgência justificada**, bem como eventos **sem responsabilidade** da **CONTRATADA**.

1.6.1. Paralisação programada (manutenção preventiva/atualização): comunicação com **5 (cinco) dias úteis** de antecedência; limites por componente:

a) **Duração máxima**: **até 180 (cento e oitenta) minutos** por componente/mês;
b) **Frequência máxima**: **1 (uma) ocorrência** a cada **30 (trinta) dias**, não cumulativa;
c) Para ações nas dependências da **CONTRATANTE**, é obrigatório **agendamento prévio** com o preposto;
d) Se não houver comunicação prévia nos termos acima, a paralisação **contará como indisponibilidade**.

1.7. Paralisação de urgência: intervenção para prevenir risco imediato à segurança/continuidade (ex.: falha crítica, correção emergencial de assinaturas). Deve ser **comunicada** à **CONTRATANTE** com antecedência mínima de **2 (duas) horas** por relatório técnico. Ausente a comunicação, **contará** no cômputo de indisponibilidade.

1.8. Serão consideradas como **não atribuíveis à CONTRATADA** as paralisações decorrentes de **caso fortuito/força maior** (ex.: eventos naturais), bem como de **ato/omissão da CONTRATANTE** ou falhas em **ativos sob responsabilidade** da **CONTRATANTE**.

1.9. Quando os **níveis de disponibilidade ou tempos MTTD/MTTR** estabelecidos não forem atendidos, aplicar-se-ão os **descontos e penalidades** previstos no item 2 e/ou item 3 deste Anexo.

2. INTERRUPÇÃO DE SERVIÇO

2.1. Na ocorrência de **interrupções não programadas** ou **paralisações de urgência** que não atendam aos critérios deste Anexo, a **CONTRATADA** ficará sujeita a **descontos/multas** conforme abaixo:
2.1.1. Os **descontos** por interrupção serão aplicados na fatura do **mês subsequente** ao da ocorrência, quando a causa **não** for atribuível à **CONTRATANTE**.

2.2. Para efeito de descontos, o tempo será considerado entre o **registro da ocorrência** (na gerência/supervisão da **CONTRATADA**, SIEM/monitoramento da **CONTRATANTE**, ou abertura de chamado) e a **plena normalização** informada à **CONTRATANTE**.

2.3. O **período mínimo** a considerar é de **30 (trinta) minutos consecutivos**;
2.4. Períodos adicionais contam como **módulos integrais de 30 minutos**.

2.5. O **valor do desconto** incidirá na fatura imediatamente subsequente, tomando por base o **valor mensal do componente** afetado no mês da ocorrência.

2.6. Não haverá descontos quando o evento decorrer de **operação inadequada da CONTRATANTE**, falha de sua infraestrutura ou **rede elétrica** interna/externa.

2.7. Não incidem multas por **manutenções programadas** e **paralisações de urgência justificadas**, ou por eventos **sem responsabilidade** da **CONTRATADA**, nos termos deste Anexo.

2.8. O **valor do desconto (VD)** será obtido por:

$$VD = VM \times \frac{N}{1440}$$

Onde: **VM** = **Valor Mensal** do componente afetado; **N** = **quantidade de períodos** de 30 minutos de interrupção no mês (N = minutos de interrupção / 30).

2.9. A **CONTRATADA** deverá garantir **suporte operacional** em todas as localidades abrangidas, por equipe técnica qualificada, para restabelecimento célere dos serviços.

2.10. Em falhas **atribuíveis à CONTRATADA** que afetem componentes críticos (console, NGIPS em HA, MDR 24x7), poderá ser aplicada multa adicional "**pro rata die**", limitada a **10% do valor mensal do contrato**, sem prejuízo dos descontos calculados por indisponibilidade.

2.11. A **CONTRATANTE** realizará **mensalmente** a apuração de **multas e descontos** e encaminhará à **CONTRATADA** para ciência e **eventual contestação única** referente ao mês avaliado. Após aceite, não caberá nova contestação, devendo a **CONTRATADA** proceder ao pagamento/compensação.

2.12. A **CONTRATANTE** poderá utilizar a **planilha de acompanhamento de SLA** (ANEXO I-F) para registro e auditoria dos indicadores.

3. MULTAS E PENALIDADES PARA O ACORDO DE NÍVEL DE SERVIÇOS – SLA

3.1. Pelo não cumprimento do SLA por incidente/chamado, o Banco poderá, **garantidos o contraditório e a ampla defesa**, aplicar as penalidades previstas na **Lei nº 13.303/2016** e demais normas aplicáveis, sem prejuízo das disposições editalícias e contratuais. As classificações e multas seguem:

Classificação – Descrição – Multa/Penalidade

- **Muito Alta** – Indisponibilidade ou degradação de **funções vitais** da solução (console central inacessível; NGIPS sem failover; MDR inoperante) – **1,0%** sobre o **valor global**.
- **Alta** – Indisponibilidade/degradação de **funções não vitais de alta importância** (ex.: perda de ingestão NDR por mais de 60 min em segmento crítico; atraso >MTTR p/ alta criticidade) – **0,5%** sobre o **valor global**.
- **Média** – Indisponibilidade/degradação de **funções não vitais** (ex.: atraso >MTTR p/ média criticidade; degradação de relatório/visibilidade sem impacto em mitigação) – **0,3%** sobre o **valor global do lote**.
- **Baixa** – Chamados de **impacto nulo/baixo** – **advertência** ou **0,1%** sobre o **valor global do lote**.

3.2. As penalidades podem ser **cumulativas** com outras sanções e **não** possuem caráter compensatório, não isentando a **CONTRATADA** de **indenizar perdas e danos**.

3.3. Nenhuma multa será aplicada sem **processo administrativo** prévio, assegurando-se contraditório e ampla defesa no prazo de **5 (cinco) dias úteis** a partir da notificação.

3.4. Constatada a responsabilidade da **CONTRATADA**, o valor das multas poderá ser **descontado da garantia**, **compensado em fatura**, **cobrado diretamente** ou **judicialmente**.

3.5. Se a multa superar o valor da **garantia**, além da perda desta, a **CONTRATADA** responderá pela **diferença**, a ser descontada de pagamentos devidos ou cobrada por via própria.

3.6. Inexistindo pagamentos devidos ou sendo estes insuficientes, a **CONTRATADA** deverá efetuar o **pagamento** no prazo máximo de **10 (dez) dias consecutivos** da confirmação da multa, por **depósito em conta** indicada pela **CONTRATANTE**.

3.7. O **descumprimento** de instruções normativas do BANCO, após **30 (trinta) dias** da ciência, implicará multa de **0,2% ao dia** sobre o valor total do contrato, por item/alínea/tema em não conformidade.

3.8. O **descumprimento de prazos** relativos à execução de serviços, bem como a **não realização de ações de contingência** que assegurem a continuidade durante a garantia, implicará multa de **3% ao dia**.

3.9. A **violação de confidencialidade** e do **sigilo** de quaisquer dados/processos/informações do BANCO implicará multa compensatória de **5%** sobre o valor total do contrato, sem prejuízo de demais sanções e da **rescisão**.

3.10. As multas contratuais poderão ser **descontadas da garantia** após devido processo; excedendo-a, aplicam-se os mecanismos de cobrança previstos em lei e no contrato.

GARANTIA E ASSISTÊNCIA TÉCNICA

1. **GARANTIA E ASSISTÊNCIA TÉCNICA**

1.1. A **CONTRATADA** deverá disponibilizar, nas dependências da sede da **CONTRATANTE**, em Belém/PA, um profissional técnico responsável pela interface operacional e coordenação técnica durante toda a vigência contratual, com capacidade para esclarecer questionamentos, intervir tecnicamente (quando necessário) e coordenar ações conjuntas para resolução de incidentes relacionados à solução integrada de rede e segurança.

1.2. A **CONTRATADA** deverá prestar suporte operacional especializado à **CONTRATANTE**, abrangendo todas as localidades com infraestrutura crítica, por meio de equipe técnica certificada e centros de operações (SOC/NOC) devidamente estruturados.

1.3. Em razão da natureza corporativa e crítica dos serviços da **CONTRATANTE**, todos os atendimentos deverão assegurar a integridade, confidencialidade e disponibilidade dos dados, conforme padrões de segurança da informação e em conformidade com a Lei nº 13.709/2018 (LGPD).

1.4. A Central de Assistência Técnica/SOC da **CONTRATADA** deverá operar de forma contínua (24x7x365), disponível todos os dias do ano, para o recebimento, registro e acompanhamento de incidentes, alertas e chamados técnicos da **CONTRATANTE**.

1.5. O canal de atendimento deverá permitir comunicação telefônica gratuita (ex.: 0800) e atendimento em língua portuguesa, além de canal eletrônico via e-mail corporativo e portal web (Service Desk) com registro de ticket e rastreabilidade.

1.6. As ocorrências registradas deverão ser tratadas pelos Centros de Serviço/SOC da **CONTRATADA**, que deverão dispor de estrutura técnica e de gestão de incidentes (ITSM/SIEM), acionando automaticamente as equipes responsáveis pela mitigação, contenção e recuperação da normalidade operacional.

1.7. A **CONTRATADA** deverá apresentar à **CONTRATANTE**, na fase inicial de implantação, um Manual de Suporte e Escalonamento, contendo fluxos de acionamento, contatos técnicos, níveis de priorização e tempos de resposta.

1.8. A **CONTRATADA** não será responsável por incidentes originados na infraestrutura interna da **CONTRATANTE** que não estejam sob escopo do contrato, salvo quando comprovada relação direta com falha de componentes fornecidos ou serviços contratados.

1.9. A manutenção corretiva dos equipamentos e serviços deverá ser executada em regime contínuo (24x7), incluindo feriados e finais de semana, sempre que houver impacto na operação da solução.

1.10. Os atendimentos que necessitarem ser realizados nas dependências da **CONTRATANTE** deverão ocorrer conforme agendamento prévio, em dias e horários definidos pela **CONTRATANTE**.

1.11. Caso ocorra impedimento de acesso aos técnicos da **CONTRATADA** por motivos atribuíveis à **CONTRATANTE**, o tempo de impedimento não será computado no cálculo de indisponibilidade.

1.12. Intervenções programadas (para atualizações de firmware, substituições preventivas ou melhorias) deverão ocorrer preferencialmente entre 21h30 e 04h00 (horário de Brasília), mediante comunicação prévia com 5 (cinco) dias úteis de antecedência à **CONTRATANTE**.

1.13. Quando a antecedência mínima de comunicação não for observada, ou a **CONTRATANTE** não for formalmente informada, a interrupção será computada no cálculo

de indisponibilidade e sujeita aos descontos previstos no **SLA (Anexo I C).**

1.14. A **CONTRATANTE** poderá, a qualquer tempo, solicitar ajustes de configuração, ampliação ou readequação técnica da solução, mediante termo aditivo contratual, sem prejuízo das garantias de continuidade e suporte.

1.15. Cada visita técnica deverá ser formalizada mediante Relatório de Execução de Atividades, contendo data, horário, técnicos envolvidos, descrição dos serviços executados, equipamentos afetados e assinatura digital ou física do responsável técnico da **CONTRATADA**.

1.16. O atraso no início dos serviços em qualquer dependência da **CONTRATANTE** implicará multa de 1% (um por cento) ao dia, calculada sobre o valor mensal proporcional ao serviço correspondente.

1.17. O atraso superior a 30 (trinta) dias consecutivos poderá ensejar, a critério do Banco da Amazônia, a rescisão contratual e aplicação de multa compensatória equivalente a 1 (um) mês do valor global contratado.

1.18. Os prazos máximos de atendimento técnico presencial serão os seguintes, contados a partir do registro técnico do incidente no Service Desk/SOC da **CONTRATADA**:

1.18.1. Site Central (Datacenter Principal): até 1 (uma) hora;

1.18.2. O descumprimento dos prazos definidos no item anterior sujeitará a **CONTRATADA** à incidência de multa compensatória, equivalente a 5 (cinco) dias de prestação do serviço por dia de atraso, calculada “pro rata die”, contada desde a interrupção até o completo restabelecimento do serviço.

REQUISITOS TÉCNICOS DE SUPORTE DE REDES E SEGURANÇA DA INFORMAÇÃO

1. OBJETO

O presente anexo tem por objetivo a descrição dos requisitos técnicos para a contratação de empresa especializada para prestação de serviços técnicos continuados de suporte à infraestrutura de redes de dados e resposta a incidentes de segurança da informação, com alocação presencial de profissionais qualificados no período de 07h às 20h, em regime de escala de 8 (oito) horas diárias, e atendimento remoto após este horário, conforme demanda da CONTRATANTE. Os serviços abrangem o gerenciamento, a manutenção, o monitoramento e o atendimento a incidentes nos ambientes de redes e segurança da informação.

2. JUSTIFICATIVA

A criticidade da infraestrutura de redes e a complexidade dos atuais cenários de segurança cibernética exigem profissionais de alto nível técnico, aptos a operar ambientes robustos, tomar decisões rápidas diante de falhas ou ataques, e garantir a resiliência do ecossistema digital da CONTRATANTE. A demanda por qualificação exclui funções de nível básico (N1), priorizando profissionais com formação sólida e experiência prática relevante, assegurando maior eficiência na entrega de resultados e redução de riscos operacionais.

3. ESCOPO DOS SERVIÇOS

Os profissionais alocados deverão atuar nas seguintes frentes:

- Administração de redes LAN, WAN, WLAN, MPLS, SD-WAN, links de internet e VPNs;
- Gerenciamento de ativos como switches, roteadores, firewalls e balanceadores;
- Identificação, análise e resposta a eventos e incidentes de segurança;
- Operação de ferramentas de monitoramento de redes (NMS) e segurança (SIEM, IDS/IPS);
- Aplicação de correções, hardening e mitigação de vulnerabilidades;
- Análise forense de incidentes e geração de relatórios técnicos;
- Atendimento de requisições e incidentes, com registro detalhado e documentação;
- Recomendação de melhorias de segurança, desempenho e conformidade.

4. PERFIS PROFISSIONAIS EXIGIDOS

4.1 Analista de Redes Pleno

- Formação: Curso superior completo em Ciência da Computação, Redes, Engenharia de Computação ou áreas correlatas;

- Experiência mínima: 3 anos em administração de redes corporativas;
- Conhecimentos exigidos:
    - Protocolos de roteamento dinâmico (OSPF, BGP, EIGRP);
    - Gerenciamento de VLANs, STP, RSTP, Port Security;
    - Troubleshooting com ferramentas como Wireshark, traceroute, iperf;
    - Monitoramento de rede com Zabbix, LibreNMS, ou equivalentes;
    - VPNs (SSL/IPSec), MPLS e ambientes multihoming;
- Certificações desejáveis: CCNA, JNCIA, ou equivalente.

4.2 Analista de Segurança da Informação Pleno

- Formação: Curso superior completo em Segurança da Informação, Engenharia da Computação, Ciência da Computação ou áreas correlatas;
- Pós-graduação: Segurança da informação ou área correlata;
- Experiência mínima: 3 anos atuando com segurança ofensiva e defensiva;
- Conhecimentos exigidos:
    - Operação de SIEM (ex: IBM QRadar, Splunk, ArcSight);
    - Análise de logs, tráfego suspeito e indicadores de comprometimento (IoCs);
    - Firewalls NGFW (FortiGate, Palo Alto, Check Point), regras de filtragem, NAT, DPI;
    - Resposta a incidentes com base em frameworks NIST 800-61, MITRE ATT&CK ou SANS;
    - Vulnerability Management e aplicação de patches emergenciais;
- Certificações desejáveis: CompTIA Security+, CEH, Fortinet NSE 4 ou equivalente.

5. JORNADA DE TRABALHO E ESCALA

Horário de atendimento presencial: das 07h às 20h, em regime de escala de 8 (oito) horas diárias por profissional;

- Atendimento remoto: a partir das 20h até 07h do dia seguinte, com acionamento sob demanda (plantão remoto), mediante celular corporativo e/ou sistema de chamados;
- A escala deve ser gerida pela contratada de forma a garantir cobertura integral presencial no horário definido, com pelo menos 1 profissional de redes e 1 de segurança da informação por turno.

6. NÍVEIS DE ATENDIMENTO (N2 e N3)

Nível	Descrição	Tempo de Resposta	Tempo de Solução
N2	Profissional alocado localmente	Até 15 Minutos	Até 4 horas

N3	Apoio remoto especializado (caso necessário)	Até 1 hora	Até 12 horas

Incidentes críticos (impacto direto em sistemas de produção ou segurança) deverão ser tratados como prioridade máxima, com atuação imediata.

7. OBRIGAÇÕES DA CONTRATADA

- Disponibilizar profissionais qualificados, conforme perfis exigidos;
- Gerenciar escala de modo que não haja descontinuidade na cobertura presencial;
- Garantir substituição de profissional ausente em até 2 (dois) dias úteis;
- Manter base de backup de profissionais certificados disponíveis para eventual substituição;
- Garantir disponibilidade de atendimento remoto após o horário presencial;
- Fornecer relatório mensal com as atividades realizadas, incidentes tratados e SLA cumprido;
- Manter todos os profissionais com termos de confidencialidade assinados e atualizados.

8. OBRIGAÇÕES DA CONTRATANTE

- Disponibilizar infraestrutura física e lógica necessária para atuação presencial;
- Fornecer acesso aos sistemas de gerenciamento de chamados e logs;
- Designar um fiscal técnico para acompanhar a execução dos serviços;
- Avaliar o desempenho técnico dos profissionais e solicitar substituições se necessário.

10. DISPOSIÇÕES FINAIS

Todas as atividades deverão observar as boas práticas de segurança da informação, padrões técnicos de redes e normas de compliance aplicáveis. A contratada responderá integralmente por qualquer falha operacional, técnica ou de segurança causada por seus profissionais, inclusive podendo incorrer em sanções contratuais.

PREGÃO ELETRÔNICO 90008/2026

ANEXO I F

MATRIZ DE TESTES DA PROVA DE CONCEITO (PoC)
SOLUÇÃO INTEGRADA DE REDE E SEGURANÇA

1. OBJETO

1.1. O presente Anexo estabelece os critérios, procedimentos, casos de teste, forma de avaliação, registro de evidências e condições de aprovação ou reprovação da Prova de Conceito (PoC) da Solução Integrada de Rede e Segurança.
1.2. A PoC será realizada com a **LICITANTE** provisoriamente classificada em primeiro lugar, após a fase de julgamento e antes da adjudicação do objeto, nos termos do Edital, do Termo de Referência e de seus anexos.
1.3. A PoC terá por finalidade comprovar, de forma prática, objetiva, verificável e mensurável, a aderência da solução ofertada aos requisitos técnicos essenciais previstos no Edital, no Termo de Referência, no Anexo I A – Especificações Técnicas e neste Anexo.
1.4. A PoC constitui etapa de validação técnica da solução ofertada, não se confundindo com apresentação comercial, exposição institucional, demonstração meramente conceitual, declaração de intenção, roadmap de produto ou promessa de implementação futura.
1.5. A solução demonstrada na PoC deverá corresponder à solução ofertada na proposta comercial e técnica da **LICITANTE**, incluindo arquitetura, módulos, componentes essenciais, console de gerenciamento, modelo de integração, serviços associados e demais elementos necessários à execução do objeto.

2. FINALIDADE DA PoC

2.1. A Prova de Conceito tem por finalidade validar, em ambiente controlado, a capacidade da solução ofertada de atender aos requisitos críticos da contratação, especialmente quanto a:
a) arquitetura integrada e operação em plataforma unificada;
b) gerenciamento centralizado em console única;
c) integração nativa ou funcional entre as camadas da solução;
d) correlação de eventos entre camadas de proteção, detecção, prevenção e resposta;
e) visibilidade operacional e investigativa do ambiente;
f) geração, classificação, priorização e tratamento de alertas;
g) integração entre módulos de blindagem de vulnerabilidades, inspeção avançada de rede, NDR e NGIPS;
h) emissão de relatórios, trilhas de auditoria, notificações e mecanismos de resposta;
i) integração com diretórios, sistemas corporativos, SIEM, Syslog ou mecanismos equivalentes, quando previstos nas especificações técnicas;
j) aderência aos requisitos funcionais, não funcionais e de integração previstos no Edital, no Termo de Referência e no Anexo I A;
k) aderência aos serviços MDR do fabricante, quando aplicável ao escopo da solução ofertada.
2.2. A PoC será orientada pelos requisitos críticos da contratação, considerando que o objeto compreende solução integrada de rede e segurança com monitoramento contínuo, correlação de eventos, prevenção e resposta a incidentes, atualização contínua, suporte técnico especializado e serviços associados à solução ofertada.
2.3. A PoC deverá permitir a verificação objetiva da capacidade da solução de operar de forma integrada, reduzindo riscos de incompatibilidade técnica, fragmentação operacional, ausência de rastreabilidade, perda de governança centralizada ou insuficiência de resposta a incidentes.

3. CONVOCAÇÃO E CONDIÇÕES DE REALIZAÇÃO

3.1. A **LICITANTE** provisoriamente classificada em primeiro lugar será convocada pelo Pregoeiro para realização da PoC, após a fase de julgamento e antes da adjudicação do objeto.
3.2. A convocação indicará, no mínimo:
a) data, horário e local da realização;
b) prazo para início da PoC;
c) duração estimada da sessão;
d) composição da comissão técnica avaliadora;
e) roteiro de testes a ser executado;
f) requisitos que serão validados;
g) critérios objetivos de aprovação e reprovação;
h) orientações quanto ao acesso dos demais **LICITANTES**, na condição de ouvintes.
3.3. A PoC poderá ser realizada nas dependências da **CONTRATANTE**, em ambiente por ela disponibilizado, em ambiente controlado da **LICITANTE** ou em ambiente remoto, desde que previamente aceito pela comissão técnica e que não comprometa a isonomia, a auditabilidade, a segurança da informação e a objetividade da avaliação.
3.4. A definição do ambiente de realização da PoC deverá considerar a proteção das informações da **CONTRATANTE**, a viabilidade técnica dos testes, a rastreabilidade das evidências e a possibilidade de acompanhamento pela comissão técnica.
3.5. A **LICITANTE** convocada deverá disponibilizar, sem ônus para a **CONTRATANTE**, todos os recursos necessários à execução da PoC, inclusive:
a) licenças temporárias;
b) equipamentos, appliances, imagens, módulos e acessos;
c) ambiente de demonstração funcional;
d) credenciais e perfis de acesso necessários aos testes;
e) equipe técnica qualificada;
f) documentação técnica;
g) evidências de suporte do fabricante ou integrador autorizado, quando aplicável;
h) integrações, templates, bases de teste, datasets ou mecanismos equivalentes necessários à validação dos cenários;
i) demais recursos indispensáveis à execução do roteiro de testes.
3.6. A solução apresentada na PoC deverá corresponder à mesma arquitetura, módulos, componentes essenciais, integrações e modelo operacional constantes da proposta apresentada pela **LICITANTE**.
3.7. Não será admitida, durante a PoC, substituição de fabricante, troca de componentes essenciais, alteração substancial da arquitetura ofertada, modificação do console de gerenciamento, substituição de módulos principais ou uso de solução diversa daquela apresentada na proposta.
3.8. Serão admitidos apenas ajustes meramente operacionais relacionados ao ambiente de testes, desde que previamente aceitos pela comissão técnica, devidamente registrados no relatório da PoC e sem alteração substancial da solução ofertada.
3.9. A aceitação de ajustes operacionais não poderá prejudicar a isonomia entre os **LICITANTE**s, a vinculação ao instrumento convocatório, a objetividade da avaliação ou a rastreabilidade das evidências.
3.10. Os demais **LICITANTE**s poderão acompanhar a realização da PoC na condição de ouvintes, vedada qualquer interferência na condução dos testes, formulação de questionamentos diretos à **LICITANTE** avaliada ou prática de qualquer ato que prejudique a sessão.
3.11. Eventuais manifestações dos **LICITANTE**s ouvintes deverão observar os meios e momentos próprios previstos no Edital e na legislação aplicável, não sendo admitida intervenção durante a execução dos testes.

4. COMISSÃO TÉCNICA DE AVALIAÇÃO

4.1. A PoC será conduzida e avaliada por comissão técnica formalmente designada pela **CONTRATANTE**.
4.2. A comissão técnica será composta por representantes das áreas técnica e demandante, podendo contar com apoio da área de segurança da informação, da fiscalização contratual ou de outros profissionais tecnicamente habilitados.
4.3. Compete à comissão técnica:
a) conduzir a sessão de PoC;
b) verificar o atendimento aos casos de teste;
c) solicitar demonstrações complementares estritamente vinculadas ao roteiro;
d) registrar evidências, inconsistências, ocorrências e resultados;
e) avaliar cada caso de teste com resultado expresso de “ATENDE” ou “NÃO ATENDE”;
f) assegurar que a avaliação observe critérios objetivos, previamente definidos;
g) elaborar relatório circunstanciado de aprovação ou reprovação da solução ofertada.
4.4. A comissão técnica poderá solicitar esclarecimentos técnicos durante a sessão, desde que vinculados aos requisitos previstos no Edital, no Termo de Referência, no Anexo I A e neste Anexo.
4.5. Não caberá à comissão técnica alterar os requisitos do Edital, flexibilizar critérios de julgamento, aceitar funcionalidade futura ou permitir substituição substancial da solução ofertada.

5. REGRAS DE AVALIAÇÃO
5.1. Cada caso de teste previsto neste Anexo será avaliado com resultado expresso de:
a) ATENDE; ou
b) NÃO ATENDE.
5.2. Não serão admitidos resultados intermediários, subjetivos, condicionados ou genéricos.
5.3. A validação ocorrerá exclusivamente com base no que for efetivamente demonstrado durante a sessão da PoC, vedada a aceitação, para fins de aprovação, de:
a) declaração unilateral sem comprovação funcional;
b) roadmap de produto;
c) funcionalidade futura;
d) customização não implementada;
e) promessa de desenvolvimento;
f) material comercial desacompanhado de demonstração funcional;
g) correção posterior de requisito crítico não atendido na sessão.
5.4. Serão considerados requisitos críticos aqueles relacionados à arquitetura integrada, console de gerenciamento, correlação de eventos, visibilidade centralizada, geração de alertas, investigação, resposta, integração entre camadas, trilhas de auditoria, integrações corporativas e aderência aos serviços do fabricante, quando aplicável.
5.5. A PoC será considerada aprovada somente se a **LICITANTE** atender, cumulativamente:
a) a 100% (cem por cento) dos casos de teste classificados como CRÍTICOS; e
b) a, no mínimo, 90% (noventa por cento) do total dos casos de teste previstos neste Anexo.
5.6. O não atendimento de qualquer caso de teste classificado como CRÍTICO implicará reprovação da PoC e consequente desclassificação da **LICITANTE** provisoriamente classificada em primeiro lugar.
5.7. O não atendimento de caso de teste classificado como COMPLEMENTAR não implicará, isoladamente, reprovação da PoC, desde que a **LICITANTE** atenda a todos os casos críticos e alcance o percentual mínimo global de aprovação previsto no item 5.5.
5.8. A comissão técnica deverá registrar, para cada caso de teste, a evidência apresentada e a justificativa objetiva para o resultado atribuído.
5.9. A avaliação deverá observar os princípios do julgamento objetivo, da vinculação ao instrumento convocatório, da isonomia, da competitividade, da transparência e da seleção da proposta mais vantajosa.

6. MATRIZ DE TESTES

6.1. Casos de teste obrigatórios:

Caso 1

Requisito a validar: Arquitetura integrada da solução ofertada, observadas as exigências do Anexo I A quanto a fabricante, módulos, integrações e console de gerenciamento.
Evidência esperada: Comprovação documental e funcional da arquitetura ofertada, demonstrando a integração entre os componentes essenciais da solução.
Forma de validação: Conferência documental e demonstração funcional.
Classificação: CRÍTICO.

Caso 2

Requisito a validar: Console única centralizada para gerenciamento e operação da solução.
Evidência esperada: Painel único de gerenciamento e operação, com visibilidade dos módulos, eventos, alertas, relatórios e elementos administráveis.
Forma de validação: Demonstração navegada na console.
Classificação: CRÍTICO.

Caso 3

Requisito a validar: Integração entre blindagem de vulnerabilidades, inspeção avançada de rede, NDR e NGIPS.
Evidência esperada: Eventos consolidados, relacionados ou correlacionados em ambiente unificado, conforme arquitetura ofertada.
Forma de validação: Simulação funcional ou demonstração assistida.
Classificação: CRÍTICO.

Caso 4

Requisito a validar: Integração com plataforma centralizada de correlação e gerenciamento da solução ofertada, inclusive XDR quando expressamente exigido nas especificações técnicas.
Evidência esperada: Recepção, consolidação e correlação de alertas em console centralizada.
Forma de validação: Demonstração de fluxo de evento.
Classificação: CRÍTICO.

Caso 5

Requisito a validar: Correlação entre usuários, IPs, servidores, processos, arquivos, URLs, domínios e demais objetos monitorados.
Evidência esperada: Tela investigativa ou relatório técnico com objetos relacionados ao alerta ou incidente.
Forma de validação: Investigação assistida.
Classificação: CRÍTICO.

Caso 6

Requisito a validar: Geração, categorização e priorização de alertas por criticidade.
Evidência esperada: Alertas classificados em níveis de severidade, criticidade ou prioridade.
Forma de validação: Simulação de detecção ou consulta a evento previamente carregado no ambiente de teste.
Classificação: CRÍTICO.

Caso 7

Requisito a validar: Correlação com MITRE ATT&CK ou estrutura equivalente de classificação de táticas, técnicas e procedimentos de ataque.
Evidência esperada: Associação do alerta ou incidente a tática, técnica, procedimento ou categoria de ataque.
Forma de validação: Consulta em incidente ou alerta.
Classificação: CRÍTICO.

Caso 8

Requisito a validar: Linha do tempo do ataque, alerta ou incidente.
Evidência esperada: Visualização cronológica dos eventos correlacionados.

Forma de validação: Demonstração funcional.
Classificação: CRÍTICO.
Caso 9
Requisito a validar: Registro de trilhas de auditoria.
Evidência esperada: Log de ações administrativas, alterações de configuração, acessos ou eventos relevantes.
Forma de validação: Execução de ação administrativa e consulta ao log.
Classificação: CRÍTICO.
Caso 10
Requisito a validar: Perfis de acesso e segregação de permissões.
Evidência esperada: Perfis distintos de administração, operação, investigação ou visualização, conforme funcionalidades disponíveis.
Forma de validação: Teste com usuários ou perfis distintos.
Classificação: CRÍTICO.
Caso 11
Requisito a validar: Integração com diretório ou mecanismo corporativo de autenticação.
Evidência esperada: Demonstração de integração, sincronização ou autenticação com AD, Azure AD, LDAP, SAML ou mecanismo equivalente previsto na especificação técnica.
Forma de validação: Demonstração de integração ou evidência técnica verificável.
Classificação: CRÍTICO.
Caso 12
Requisito a validar: Envio de notificações.
Evidência esperada: Geração de notificação por e-mail, SMTP, webhook, API, ferramenta corporativa ou mecanismo equivalente previsto na especificação técnica.
Forma de validação: Geração de alerta e conferência da notificação.
Classificação: CRÍTICO.
Caso 13
Requisito a validar: Emissão de relatórios.
Evidência esperada: Relatórios técnicos ou executivos emitidos sob demanda, em formato compatível com as especificações.
Forma de validação: Geração de relatório em sessão.
Classificação: CRÍTICO.
Caso 14
Requisito a validar: Agendamento de relatórios.
Evidência esperada: Configuração de geração ou envio automático de relatórios.
Forma de validação: Demonstração de agendamento.
Classificação: COMPLEMENTAR.
Caso 15
Requisito a validar: Integração com SIEM, Syslog ou mecanismo equivalente de encaminhamento de logs.
Evidência esperada: Configuração e evidência de envio ou disponibilização de logs para destino externo.
Forma de validação: Configuração e apresentação da evidência.
Classificação: CRÍTICO.
Caso 16
Requisito a validar: Pesquisa investigativa avançada.
Evidência esperada: Busca por IOC, IP, hash, domínio, usuário, host, arquivo, URL ou outro objeto monitorado.
Forma de validação: Consulta assistida na console.
Classificação: CRÍTICO.
Caso 17
Requisito a validar: Classificação, marcação ou etiquetagem de eventos.

Evidência esperada: Uso de tags, categorias, status, falso positivo ou mecanismo equivalente para organização de eventos.
Forma de validação: Demonstração funcional.
Classificação: COMPLEMENTAR.
Caso 18
Requisito a validar: Detecção comportamental em rede.
Evidência esperada: Identificação de anomalia, tráfego suspeito, comportamento incomum ou comunicação atípica.
Forma de validação: Simulação controlada, consulta a dataset ou demonstração funcional.
Classificação: CRÍTICO.
Caso 19
Requisito a validar: Detecção de comando e controle, exploração ou ameaça avançada.
Evidência esperada: Alerta correlacionado com atividade maliciosa, suspeita ou técnica de ataque.
Forma de validação: Simulação, dataset ou demonstração em ambiente controlado.
Classificação: CRÍTICO.
Caso 20
Requisito a validar: Identificação de exploração de vulnerabilidade ou tentativa de exploração.
Evidência esperada: Correlação entre tentativa de exploração, vulnerabilidade e ativo afetado, quando aplicável à solução ofertada.
Forma de validação: Simulação funcional ou consulta a evento de teste.
Classificação: CRÍTICO.
Caso 21
Requisito a validar: Execução de ação de resposta.
Evidência esperada: Bloqueio de IP, URL, domínio, IOC, contenção, quarentena, criação de regra ou ação equivalente compatível com a solução ofertada.
Forma de validação: Demonstração sobre alerta ou incidente.
Classificação: CRÍTICO.
Caso 22
Requisito a validar: Investigação remota ou ação sobre host, quando aplicável à arquitetura ofertada.
Evidência esperada: Recurso funcional de investigação, coleta, contenção ou resposta sobre host ou ativo monitorado.
Forma de validação: Demonstração em console.
Classificação: COMPLEMENTAR.
Caso 23
Requisito a validar: Dashboards customizáveis.
Evidência esperada: Inclusão, remoção, ajuste ou personalização de visualizações, indicadores ou painéis.
Forma de validação: Ajuste em tempo real.
Classificação: COMPLEMENTAR.
Caso 24
Requisito a validar: Score, nota de risco ou priorização do ambiente, host, usuário, ativo ou evento.
Evidência esperada: Painel, lista, indicador ou métrica de risco cibernético.
Forma de validação: Demonstração funcional.
Classificação: COMPLEMENTAR.
Caso 25
Requisito a validar: Identificação de ativos, hosts, usuários ou elementos de maior risco.
Evidência esperada: Lista priorizada de ativos críticos, vulneráveis, comprometidos ou com maior exposição.
Forma de validação: Consulta na console.

Classificação: COMPLEMENTAR.
Caso 26
Requisito a validar: Atualização de assinaturas, regras, inteligência de ameaças, firmware, patches ou componentes equivalentes.
Evidência esperada: Histórico, tela, relatório ou visualização de atualização.
Forma de validação: Demonstração técnica ou evidência documental verificável.
Classificação: COMPLEMENTAR.
Caso 27
Requisito a validar: Controle de versão, rollback ou mecanismo equivalente de gestão de atualização.
Evidência esperada: Evidência de versão, política de atualização, rollback ou controle de mudanças.
Forma de validação: Demonstração funcional ou evidência técnica.
Classificação: COMPLEMENTAR.
Caso 28
Requisito a validar: API documentada ou mecanismo de integração documentado.
Evidência esperada: Exemplo funcional, documentação técnica ou tela de integração.
Forma de validação: Apresentação e validação da documentação ou exemplo.
Classificação: COMPLEMENTAR.
Caso 29
Requisito a validar: Disponibilidade de logs e eventos para investigação histórica.
Evidência esperada: Consulta a eventos históricos relevantes, logs armazenados ou registros de investigação.
Forma de validação: Pesquisa em console ou relatório.
Classificação: COMPLEMENTAR.
Caso 30
Requisito a validar: Aderência do MDR do fabricante ou serviço equivalente exigido nas especificações técnicas.
Evidência esperada: Fluxo de monitoramento, análise, categorização, resposta, comunicação e relatório do serviço MDR.
Forma de validação: Evidência operacional, demonstração do fluxo, documentação técnica e modelo de relatório.
Classificação: CRÍTICO.

7. ROTEIRO MÍNIMO DE EXECUÇÃO

7.1. A **LICITANTE** deverá executar a PoC em sequência lógica, demonstrando, no mínimo, os seguintes blocos funcionais:

I – Arquitetura e Gestão Centralizada
a) apresentação da arquitetura ofertada;
b) comprovação da integração entre os componentes essenciais;
c) demonstração da console centralizada;
d) demonstração de perfis de acesso e controles administrativos;
e) demonstração de trilhas de auditoria.

II – Detecção, Correlação e Investigação
a) geração de alertas;
b) categorização e priorização por criticidade;
c) correlação com MITRE ATT&CK ou estrutura equivalente;
d) linha do tempo do incidente;
e) pesquisa investigativa avançada;
f) causa raiz e objetos correlacionados;
g) identificação de IOCs, IPs, hashes, domínios, URLs, usuários, hosts ou processos relacionados.

III – Integrações Corporativas

a) integração com diretório, autenticação ou mecanismo corporativo equivalente;
b) integração com SIEM, Syslog, API ou mecanismo equivalente;
c) envio de notificações;
d) geração, exportação e agendamento de relatórios, quando aplicável.

IV – Segurança de Rede e Resposta

a) visibilidade de tráfego leste-oeste e norte-sul, quando aplicável à arquitetura ofertada;
b) detecção de anomalia, ameaça, exploração ou comportamento suspeito;
c) identificação de tentativa de exploração de vulnerabilidade;
d) execução de ação de resposta sobre IOC, IP, URL, domínio, evento ou elemento equivalente.

V – Serviços do Fabricante e Sustentação

a) comprovação da aderência do MDR do fabricante ou serviço equivalente exigido nas especificações técnicas;
b) demonstração do fluxo de monitoramento, análise e categorização;
c) evidência de procedimento de resposta e comunicação;
d) apresentação de modelo de relatório periódico;
e) evidência de atualização de assinaturas, regras, inteligência de ameaças ou componentes equivalentes.

7.2. A comissão técnica poderá ajustar a ordem de execução dos blocos funcionais, desde que todos os casos de teste aplicáveis sejam avaliados e que a alteração não comprometa a objetividade, a isonomia ou a rastreabilidade da avaliação.

7.3. A **LICITANTE** poderá utilizar massa de dados, ambiente controlado, simulações, datasets, eventos previamente gerados ou mecanismos equivalentes, desde que aceitos pela comissão técnica e suficientes para demonstrar funcionalmente o atendimento ao requisito avaliado.

7.4. A utilização de simulação, dataset ou evento previamente gerado não dispensa a demonstração funcional da solução, nem autoriza a substituição por mera apresentação comercial ou documentação genérica.

8. REGISTRO DAS EVIDÊNCIAS

8.1. A comissão técnica registrará, para cada caso de teste:
a) o número e a descrição do caso de teste;
b) o requisito avaliado;
c) o resultado obtido;
d) a evidência apresentada;
e) eventual observação técnica;
f) a conclusão quanto ao atendimento.

8.2. Poderão ser utilizados como evidência:
a) capturas de tela;
b) relatórios emitidos pela solução;
c) logs gerados durante a PoC;
d) demonstrativos extraídos da console;
e) registros de configuração;
f) resultados de simulação ou dataset;
g) documentação técnica apresentada durante a sessão;
h) evidências de integração com ferramentas, diretórios, sistemas ou serviços corporativos;
i) modelo de relatório do MDR ou serviço equivalente, quando aplicável.

8.3. As evidências deverão ser suficientes para permitir a rastreabilidade da avaliação e a motivação da conclusão da comissão técnica.

8.4. O relatório da PoC integrará os autos do processo licitatório.

9. REPROVAÇÃO E EFEITOS

9.1. Será reprovada a **LICITANTE** que:

a) deixar de comparecer à sessão de PoC;
b) não disponibilizar os recursos necessários à realização da prova;
c) deixar de demonstrar os requisitos exigidos;
d) não atender a qualquer caso de teste classificado como CRÍTICO;
e) não alcançar o percentual mínimo global de aprovação definido neste Anexo;
f) apresentar solução diversa daquela constante da proposta;
g) substituir componente essencial, fabricante, arquitetura, console de gerenciamento ou módulo principal em desacordo com o Edital, o Termo de Referência e este Anexo;
h) impedir ou prejudicar a condução objetiva dos testes;
i) deixar de apresentar evidências mínimas suficientes para validação dos requisitos.
9.2. Em caso de reprovação, a **LICITANTE** provisoriamente classificada em primeiro lugar será desclassificada, convocando-se a **LICITANTE** subsequente, observada a ordem de classificação, para submissão ao mesmo procedimento, em iguais condições.
9.3. A reprovação da PoC deverá ser motivada pela comissão técnica, com indicação dos casos de teste não atendidos e das respectivas evidências ou ausência de evidências.
9.4. A desclassificação decorrente da reprovação na PoC observará o rito previsto no Edital e no procedimento licitatório, sem prejuízo dos meios de manifestação e recurso cabíveis.

10. RELATÓRIO FINAL

10.1. Ao término da PoC, a comissão técnica elaborará relatório circunstanciado, contendo, no mínimo:
a) identificação da **LICITANTE** avaliada;
b) data, horário e local da sessão;
c) identificação dos membros da comissão técnica;
d) relação dos testes executados;
e) resultado individual de cada caso de teste;
f) evidências produzidas;
g) requisitos atendidos e não atendidos;
h) ocorrências relevantes registradas durante a sessão;
i) conclusão fundamentada quanto à aprovação ou reprovação da solução ofertada.
10.2. O relatório final servirá de fundamento técnico para a aceitação ou rejeição da solução ofertada, observados os princípios do julgamento objetivo, da vinculação ao instrumento convocatório, da isonomia, da competitividade e da seleção da proposta mais vantajosa.
10.3. O relatório final deverá integrar os autos do processo licitatório.

11. DISPOSIÇÕES FINAIS

11.1. A realização da PoC não afasta a obrigação da **LICITANTE** de atender integralmente a todas as exigências previstas no Edital, no Termo de Referência, no Anexo I A – Especificações Técnicas e nos demais anexos da contratação.
11.2. A aprovação na PoC não exime a futura **CONTRATADA** do cumprimento integral das obrigações contratuais, dos níveis de serviço, dos prazos de implantação, das garantias, das atualizações, do suporte técnico e das demais condições estabelecidas no instrumento convocatório e no contrato.
11.3. A PoC não poderá ser utilizada para alterar a proposta, substituir solução, reduzir escopo, modificar obrigação técnica ou flexibilizar requisito previsto no Edital, no Termo de Referência ou nos anexos.
11.4. Eventuais situações não previstas neste Anexo serão decididas de forma motivada pela comissão técnica e pelo Pregoeiro, conforme suas competências, observados o Edital, o Termo de Referência, a Lei nº 13.303/2016, o regulamento interno aplicável e os princípios do julgamento objetivo, da isonomia, da vinculação ao instrumento convocatório e da seleção da proposta mais vantajosa.

REGÃO ELETRÔNICO 90008/2026

ANEXO II

MODELO DE APRESENTAÇÃO DE PROPOSTA

Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação n.90008/2026
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)....., 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 a execução dos serviços objeto desta licitação.

Item	Descrição	Tipo	Fabricante	Modelo	Part-number/SKU	Quantidade	V. Unitário	Valor total
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.	Subscrição				1.000		
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.	Subscrição				1.000		
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Software				2		
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.	Subscrição				2		
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo	Hardware				2		

	atualização de versão por 60 meses.							
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses.	Subscrição				2		
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	Software				4		
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	Hardware				4		
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.	Subscrição				4		
10	Serviço de Instalação das soluções Contratadas	Serviço				3		
11	Serviços de treinamento das soluções contratadas	Treinamento				3		
12	Serviço de suporte mensal das soluções contratadas	Serviço				60		
VALOR GLOBAL DA PROPOSTA								

A LICITANTE deverá apresentar, juntamente com sua proposta comercial, o detalhamento dos componentes da solução ofertada, indicando as seguintes informações, conforme o modelo acima.

2. No valor total proposto estão englobados todos os custos e despesas previstos no Edital n. ...../....., 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 a composição de preços:

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, a BANCO DA AMAZÔNIA S.A. 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. Os pagamentos serão efetuados em conformidade com as condições estabelecidas na Minuta do Contrato. 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 90008/2026

ANEXO III

DECLARAÇÃO DE CONFORMIDADE AOS ARTIGOS 38 E 44 DA LEI N. 13.303/2016

Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação N. 90008/2026
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 nos artigos 38 e 44 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;

(ix) que tenha elaborado o termo de referência, anteprojeto ou o projeto básico da licitação;

(x) que integrou consórcio responsável pela elaboração do termo de referência, anteprojeto ou do projeto básico da licitação;

(xi) da qual o autor do termo de referência, anteprojeto ou do projeto básico da licitação seja administrador, controlador, gerente, responsável técnico, subcontratado ou sócio, neste último caso quando a participação superar 5% (cinco por cento) do capital votante.

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 90008/2026

ANEXO IV

MINUTA DE DECLARAÇÃO DE CONHECIMENTO DO TEOR DO DECRETO Nº 7.203, DE 04.06.2010

Para participar do Pregão Eletrônico nº 90008/2026 cujo objeto é a contratação de ....., de acordo com os critérios, termos, cronograma e condições estabelecidas neste Edital e seus anexos, 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**.

********* (UF), ******** de 20****.

_____

assinatura do(a) declarante

PREGÃO ELETRÔNICO 90008/2026

ANEXO V

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 90008/2026, cujo objeto é ..... de acordo com os critérios, termos, cronograma e condições estabelecidas neste Edital 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 90008/2026

ANEXO VII

MINUTA DO INSTRUMENTO CONTRATUAL

Contrato n. ...../.....

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS 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 Diretor 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 da Diretoria do **CONTRATANTE**, datada de **.**.2024, ajustam o presente Contrato, nos termos do Edital do Pregão Eletrônico nº 90008/2026, sujeitando, ainda, as partes às disposições da Lei 13.303/16, de 30.06.2016, do Decreto nº 8.945/2026 e do Regulamento de Licitações e Contratos do Banco da Amazônia S/A . e suas alterações, bem como as cláusulas e condições seguintes.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem como objeto o fornecimento de solução integrada de rede e segurança voltada à proteção de servidores e cargas de trabalho híbridas, pelo período de 60 (sessenta) meses, abrangendo hardware, software e serviços especializados para implantação de plataforma unificada de proteção cibernética com monitoramento contínuo, detecção, prevenção e resposta a incidentes. A solução deverá integrar, de forma centralizada, camadas de blindagem de vulnerabilidades, análise de ameaças avançadas, detecção e resposta de rede (NDR) e prevenção de intrusão de próxima geração (NGIPS), complementadas por serviço de detecção e resposta gerenciada (MDR) do fabricante. Estão incluídos, ainda, os serviços de instalação, configuração, treinamento operacional e suporte técnico mensal de todas as soluções **CONTRATADAS**, com garantia e atualização contínua de versões, observada as condições estabelecidas no Termo de Referência, adendo deste contrato.

1.2. O presente contrato decorre do processo n. ...../....., realizado pelo **Edital de Licitação n° 90008/2026**.

2. CLÁUSULA SEGUNDA – ADENDOS

2.1. Fazem parte integrante do presente contrato, como se nele estivessem transcritos, os seguintes adendos:

Anexo 1 – Termo de Referência e seus anexos.
Anexo 2 – Termo de Compromisso de Política Anticorrupção
Anexo 3 – Termo de Confidencialidade e Sigilo de Dados e Informações
Anexo 4 – Matriz de Risco

2.2. A contradição involuntária entre, por um lado, as condições dispostas neste contrato, e, de outro, as condições licitadas, configuradas pelo Edital PE 90008/2026 e seus demais anexos, e a proposta apresentada pelo contratado, resolvem-se em prol das condições licitadas no PE 90008/2026 preservado o princípio da boa-fé objetiva.

3. CLÁUSULA TERCEIRA – PRAZOS

3.1. O prazo para início de execução do objeto desta contratação será o 1º dia útil após a assinatura do contrato, conforme descrito **no item 4, Anexo I – Termo de Referência, deste contrato**, e o prazo de vigência é de 05 (CINCO) anos, contados a partir da data da assinatura deste contrato.

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 Anual de R$ [====], e o Valor Global para 05 (cinco) anos é de R$ [====], com os valores conforme abaixo:

Item	Software	Tipo	Quantidade	V. Unitário	Valor total
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.	Subscrição	1.000		
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.	Subscrição	1.000		
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Software	2		
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.	Subscrição	2		

5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Hardware	2		
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses.	Subscrição	2		
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	Software	4		
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	Hardware	4		
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.	Subscrição	4		
10	Serviço de Instalação das soluções **CONTRATADAS**	Serviço	3		
11	Serviços de treinamento das soluções **CONTRATADAS**	Treinamento	3		
12	Serviço de suporte mensal das soluções **CONTRATADAS**	Serviço	60		
				Total	

4.2. 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 **CONTRATANTE** de quaisquer ônus adicionais.

4.3. Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto deste contrato estão previstos no orçamento do Banco da Amazônia nas seguintes rubricas:

Tipo	Descrição	Conta Contábil
Investimento	Equipamentos de process. De dados	26.165-3 / 4103
Dispêndio	Licença de Uso	27.065-2 / 1
Despesa	Execução de Serviços - S/INSS PJ	82.022-9
Treinamento	DESPESAS DE PROCESSAMENTO - TREINAMENTOS P/IMP. INTR. EXTERNO - S/INSS PJ	82.110-1

5. CLÁUSULA QUINTA - GARANTIA

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 anual 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 QUINTA – EXECUÇÃO DO CONTRATO

6.1. O objeto deverá ser fornecido rigorosamente conforme estabelecido no Edital e seus Anexos, em especial **Anexo I – Termo de Referência**, sendo que a inobservância de qualquer condição poderá acarretar a não aceitação dos mesmos, sem qualquer ônus para o **CONTRATANTE**.

6.1.1. A **CONTRATADA** deverá fornecer os serviços especificados no objeto deste instrumento de Contrato, cumprindo todas as obrigações e responsabilidades a si indicadas no **Anexo I – Termo de Referência**, deste contrato.

6.1.2. O **CONTRATANTE** deverá acompanhar e assegurar as condições necessárias para o fornecimento dos serviços, cumprindo rigorosamente todas as obrigações e responsabilidades a si indicadas no **Anexo I – Termo de Referência**, deste contrato.

6.2. A **CONTRATADA** é responsável pelos danos causados direta ou indiretamente ao **CONTRATANTE** ou a terceiros em razão da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo **CONTRATANTE**.

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, 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 **CONTRATANTE**, por escrito, todas as medidas que lhe parecerem oportunas, com vistas a reduzir ou eliminar as dificuldades encontradas, bem como os custos envolvidos. O **CONTRATANTE** 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 **CONTRATANTE**S 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 algumas 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 consecutivos 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 **CONTRATANTE**s, 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 **CONTRATANTE**, das respectivas ordens de fornecimento.

7. CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. O **CONTRATANTE**, por meio do agente de fiscalização técnica, deve receber o objeto do presente Contrato na forma do **Anexo I – Termo de Referência**, deste contrato.

a) provisoriamente: ao final de cada período mensal, o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à **CONTRATADA**, registrando em relatório a ser encaminhado ao gestor do contrato.

b) definitivamente: Os serviços serão recebidos definitivamente no prazo de até 30 dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os procedimentos descritos no Termo de Referência – Adendo I deste contrato:

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. 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 mediante a apresentação de Nota Fiscal/Fatura 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.

8.2. O pagamento seguirá o seguinte critério:

Item	Software	Tipo	Quant.	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	total
1	Solução de blindagem de vulnerabilidades para servidores e cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 60 meses.	Subscrição	1.000	20%	20%	20%	20%	20%	100%
2	Serviço de detecção e resposta (MDR) do fabricante para o item de Blindagem de vulnerabilidades pelo período de 60 meses.	Subscrição	1.000	20%	20%	20%	20%	20%	100%
3	Camada Lógica para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Software	2	25%	30%	15%	15%	15%	100%
4	Solução de Detecção e Resposta de Rede (NDR), incluindo atualização de versão por 60 meses.	Subscrição	2	20%	20%	20%	20%	20%	100%
5	Camada de Hardware para solução de análise de ameaças avançadas, incluindo atualização de versão por 60 meses.	Hardware	2	100%	0%	0%	0%	0%	100%
6	Serviço de detecção e resposta (MDR) do fabricante para o item de análise de ameaças avançadas pelo período de 60 meses.	Subscrição	2	20%	20%	20%	20%	20%	100%
7	Camada lógica para solução de prevenção de intrusão de próxima geração (NGIPS)	Software	4	20%	35%	15%	15%	15%	100%
8	Camada de hardware para solução de prevenção de intrusão de próxima geração (NGIPS)	Hardware	4	100%	0%	0%	0%	0%	100%
9	Serviço de detecção e resposta (MDR) do fabricante para o item de prevenção de intrusão de próxima geração pelo período de 60 meses.	Subscrição	4	20%	20%	20%	20%	20%	100%
10	Serviço de Instalação das soluções **CONTRATADAS**	Serviço	3	100%	0%	0%	0%	0%	100%
11	Serviços de treinamento das soluções **CONTRATADAS**	Treinamento	3	100%	0%	0%	0%	0%	100%

12	Serviço de suporte mensal das soluções **CONTRATADAS**	Serviço	60	20%	20%	20%	20%	20%	100%

8.2.1. O prazo para pagamento é de, no máximo, 30 (trinta) dias úteis, a contar do recebimento definitivo, condicionado à apresentação à unidade de gestão de contrato do Banco da Amazônia da Nota Fiscal/Fatura.

8.2.2. Para efeito do pagamento, a **CONTRATADA** deverá manter apresentar juntamente com as Notas Fiscais discriminativas com os documentos a seguir relacionados, caso não estejam disponíveis no Cadastro Único de Fornecedores (SICAF):

8.2.2.1. certidão negativa ou positiva com efeitos de negativa de débitos relativos aos tributos federais, inclusive contribuições previdenciárias, e à dívida ativa da União emitida pela Secretaria da Receita Federal;

8.2.2.2. certidão negativa ou positiva com efeitos de negativa de débitos emitida pelas Fazendas Estadual e Municipal do domicílio ou sede da **CONTRATADA**;

8.2.2.3. Certificado de Regularidade do FGTS (CRF);

8.2.2.4. certidão negativa de débitos trabalhistas (CNDT); e

8.2.2.5. atestado, se for o caso, de optante pelo SIMPLES (ANEXO I-AV da Instrução Normativa SRF n.º 480, de 15.12.2004);

8.2.3. 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.

8.2.4. As faturas que apresentarem erros devem ser devolvidas à **CONTRATADA** pela unidade de gestão de contrato do Banco da Amazônia para a correção ou substituição. O BANCO DA AMAZÔNIA, 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.

8.3. 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.

8.4. É vedado o pagamento antecipado.

8.5. É permitido ao Banco da Amazônia descontar dos créditos da **CONTRATADA** qualquer valor relativo à multa, ressarcimentos e indenizações, sempre observado o contraditório e a ampla defesa.

8.6. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo Banco da Amazônia, 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:

$$EM = I \times VP \times N$$

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. A **CONTRATADA** não poderá subcontratar o núcleo do objeto, compreendendo a operação integrada da solução, a execução dos serviços de NDR, NGIPS, MDR, a gestão centralizada, o suporte técnico especializado e a administração lógica, sob pena de rescisão contratual.
9.2. Será admitida, mediante autorização prévia e expressa da **CONTRATANTE**, a subcontratação de atividades acessórias ou de apoio logístico que não impliquem transferência das responsabilidades principais assumidas.
9.3. A **CONTRATADA** permanecerá responsável, perante a **CONTRATANTE**, pela execução integral do objeto, pelos níveis de serviço, pela segurança da informação e pela conformidade técnica, bem como pelo cumprimento da Lei Geral de Proteção de Dados – LGPD.

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 reajuste deve ser concedido de ofício pelo Banco da Amazônia e deve observar o descrito no Adendo 1 – Termo de Referência, item 18, pelo índice ICTI/IPEA, apurado no período.

11.3. O reajuste deverá ser precedido de solicitação formal da **CONTRATADA**, acompanhada de demonstração analítica da alteração dos custos, por meio da apresentação da Planilha de Custos e Formação de Preço.

11.4. Os reajustes a que a **CONTRATADA** fizer jus e que não forem solicitados durante a vigência do contrato, serão objeto de preclusão com o encerramento do contrato.

11.5. Em caso de ocorrência de deflação ou qualquer outro evento que implique redução do valor contratual, o reajuste será provocado pelo **CONTRATANTE**.

11.6. 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.

11.6.1. 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.

11.6.2. 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 **CONTRATANTE**, reduzindo-se o preço.

11.6.3. 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 **CONTRATANTE** 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**.

11.7. Os pedidos de revisão serão decididos em decisão fundamentada no prazo máximo de 60 (sessenta) dias contados da formalização do requerimento.

11.7.1. O **CONTRATANTE** 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 – RESCISÃO

12.1. 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 5 (cinco) dias úteis para eventual manifestação.

12.2. 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.

12.3. Aplica-se a teoria do adimplemento substancial, devendo as partes **CONTRATANTE**s 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.

12.4. 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.

12.4.1. Na hipótese deste subitem, o **CONTRATANTE** 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. CLÁUSULA DÉCIMA TERCEIRA – SANÇÕES ADMINISTRATIVAS

13.1. Pela inexecução total ou parcial do Contrato, o **CONTRATANTE** poderá, garantida a prévia defesa, de acordo com o processo administrativo preceituado no artigo 109 do Regulamento, aplicar a **CONTRATADA** as sanções de:

13.1.1. Advertência;

13.1.2. Suspensão;

13.1.3. Multa;

13.2. Suspensão temporária de participação em licitação e impedimento de contratar com o **CONTRATANTE** por prazo não superior a 2 (dois) anos, que podem ser cumuladas com multa.

13.3. 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;

f) Comportar-se com má-fé ou cometer fraude fiscal.

g) Praticar atos ilícitos visando a frustrar os objetivos da licitação.

13.4. 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.

13.4.1. 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 **CONTRATANTE**.

13.4.2. 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 **CONTRATANTE**;

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.

13.4.3. 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.

13.5. A **CONTRATADA**, para além de hipóteses previstas no presente Contrato, estará sujeita à multa conforme previsto no **Adendo I – Termo de Referência,** do Edital:

12.5.1. Multa de 10% (dez por cento) sobre o valor global do contrato pela inexecução total do ajuste;

12.5.2. Multa de 0,2% (dois décimos por cento) calculado sobre o valor da respectiva fatura, quando houver atraso parcial na execução do objeto do contrato enquanto perdurar o inadimplemento;

12.5.3. Se a multa moratória alcançar o seu limite e a mora não se cessar, o Contrato pode ser rescindido, salvo decisão em contrário, devidamente motivada, do gestor do Contrato.

12.5.4. Acaso a multa não cubra os prejuízos causados pela **CONTRATADA**, o **CONTRATANTE** pode exigir indenização suplementar, valendo a multa como mínimo de indenização, na forma do preceituado no parágrafo único do artigo 416 do Código Civil Brasileiro.

12.5.5. A multa aplicada pode ser descontada da garantia, dos pagamentos devidos à **CONTRATADA** em razão do Contrato em que houve a aplicação da multa ou de eventual outro Contrato havido entre o **CONTRATANTE** e a **CONTRATADA**, aplicando-se a compensação prevista nos artigos 368 e seguintes do Código Civil Brasileiro.

12.6. O atraso na entrega do produto superior a 30 (trinta) dias consecutivos, poderá ensejar, a exclusivo critério do Banco, a rescisão do Contrato.

12.7. A rescisão do contrato provocada pela **CONTRATADA** implicará, de pleno direito, a cobrança pelo Banco de multa equivalente a 10% (dez por cento) do valor total contratado.

12.8. Nenhuma penalidade será aplicada pelo Banco sem o devido processo administrativo, assegurado o contraditório e a ampla defesa, no prazo de 10 (dez) dias úteis conforme artigo 83 da Lei nº 13.303/2016.

12.9. A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança, facultada a defesa prévia, não isentará a obrigação de indenizar eventuais perdas e danos.
12.10. O valor das multas apurado, após o processo administrativo, será descontado dos pagamentos eventualmente devidos ao Banco.

12.11. 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.
12.12. Em não se realizando o pagamento nos termos definidos no item acima, far-se-á a sua cobrança judicialmente.

13. CLÁUSULA DÉCIMA TERCEIRA – RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO **CONTRATANTE**

13.1. Com fundamento no artigo 5º da Lei n. 12.846/2013, constituem atos lesivos ao **CONTRATANTE** 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.

13.2. A prática, pela **CONTRATADA**, de atos lesivos ao **CONTRATANTE**, 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.

13.2.1. 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).

13.2.2. 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.

13.2.3. 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.

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

13.3. A prática de atos lesivos ao **CONTRATANTE** 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.

13.3.1. 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.

13.3.2. 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.

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

13.3.4. 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.

13.3.5. 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, inclusive suas eventuais alterações, sem prejuízo ainda da aplicação do ato de que trata o artigo 21 do Decreto n. 11.129/2022.

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

13.5. 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.

13.6. 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.

14. CLÁUSULA DÉCIMA QUARTA – PUBLICIDADE E CONFIDENCIALIDADE

14.1. 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 **CONTRATANTE**. Para os efeitos desta Cláusula, deve ser formulada a solicitação, por escrito, ao **CONTRATANTE**, informando todos os pormenores da intenção da **CONTRATADA**, reservando-se, ao **CONTRATANTE**, o direito de aceitar ou não o pedido, no todo ou em parte.

15. CLÁUSULA DÉCIMA QUINTA – POLÍTICA DE RELACIONAMENTO E ANTICORRUPÇÃO

15.1. 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 assinar o **Termo de Compromisso de Política Anticorrupção – Adendo II**, e **Termo de Confidencialidade e Sigilo de Dados e Informações – Adendo III**, que integra o presente Contrato.

15.2. O **CONTRATANTE** 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 **CONTRATANTE** dentro de 5 (cinco) dias uteis, a contar de sua solicitação.

16. CLÁUSULA DÉCIMA SEXTA – DAS OBRIGAÇÕES

16.1. DAS OBRIGAÇÕES DA CONTRATADA

16.1.1. A **CONTRATADA** obriga-se a cumprir integralmente as disposições previstas neste Termo de referência, no contrato e em seus anexos, observando as seguintes obrigações, sem prejuízo de outras que sejam inerentes ao cumprimento do objeto da contratação:

Obrigações Gerais

16.1.1.1. Executar o objeto do contrato em conformidade com todas as especificações técnicas, níveis de serviço (SLA), prazos e demais condições estabelecidas neste Termo de Referência, no Estudo Técnico Preliminar e nos seus anexos, garantindo a entrega e operação da Solução Integrada de Rede e Segurança.

16.1.1.2. Cumprir rigorosamente todos os prazos de implantação, ativação, homologação, suporte, manutenção e correções, conforme cronograma técnico e marcos contratuais aprovados pela **CONTRATANTE**.

16.1.1.3. Prestar, sempre que solicitado, esclarecimentos técnicos e administrativos sobre a execução do contrato, bem como atender tempestivamente a reclamações, notificações e recomendações emitidas pela fiscalização ou gestão contratual.

16.1.1.4. Submeter-se à fiscalização técnica e administrativa da **CONTRATANTE**, assegurando livre acesso a instalações, sistemas,

equipamentos, consoles de gerenciamento, registros, relatórios e documentos relacionados à execução do objeto.

16.1.1.5. Prover todos os meios técnicos, humanos, materiais, logísticos e operacionais necessários à plena operacionalidade da plataforma de segurança integrada, incluindo hardware, software, licenças, suporte técnico, serviços de instalação, configuração, atualização e manutenção preventiva e corretiva.

16.1.1.6. Manter sigilo e confidencialidade absolutos sobre dados, documentos, topologias, políticas de segurança, relatórios, acessos e informações técnicas ou estratégicas do Banco da Amazônia, aplicando medidas de proteção física e lógica em conformidade com a Lei nº 13.709/2018 (LGPD), as normas internas e as políticas de segurança da **CONTRATANTE**.

16.1.1.7. Executar todas as atividades em conformidade com a legislação brasileira vigente, especialmente a Lei nº 13.303/2016, a Resolução nº 4.893/2021 do Banco Central do Brasil, a Lei Geral de Proteção de Dados (LGPD), bem como as normas de segurança da informação, trabalhistas, fiscais e ambientais aplicáveis.

16.1.1.8. Não empregar, direta ou indiretamente, trabalho ilegal, infantil ou análogo à escravidão, devendo garantir que todos os seus fornecedores, subcontratados e prestadores de serviço observem integralmente a legislação trabalhista e de direitos humanos.

16.1.1.9. Adotar políticas de equidade e não discriminação no ambiente de trabalho, assegurando respeito à diversidade e à inclusão social, conforme boas práticas corporativas e princípios de responsabilidade social do Banco da Amazônia.

16.1.1.10. Executar os serviços com responsabilidade socioambiental, observando a legislação ambiental vigente e as boas práticas de sustentabilidade, incluindo descarte correto de resíduos eletrônicos, redução de impactos ambientais e uso racional de recursos.

16.1.1.11. Corrigir imediatamente, sem ônus para a **CONTRATANTE**, quaisquer falhas, deficiências, inconsistências ou desvios técnicos identificados pela fiscalização, dentro dos prazos estabelecidos nas notificações formais.

16.1.1.12. Responder civil e administrativamente por eventuais danos causados à **CONTRATANTE** ou a terceiros, decorrentes de ações ou omissões de seus empregados, subcontratados ou prepostos, desde que comprovada culpa ou dolo, inclusive por comprometimento de dados, indisponibilidade de serviços ou falhas de segurança.

Obrigações Específicas Relacionadas à Solução Integrada de Rede e Segurança

16.1.1.13. Garantir a alta disponibilidade da infraestrutura **CONTRATADA**, conforme SLA definido em anexo, assegurando monitoramento contínuo 24x7x365, suporte técnico proativo e tempos de resposta e resolução compatíveis com a criticidade dos serviços.

16.1.1.14. Monitorar continuamente o desempenho, a integridade e os indicadores da solução por meio da plataforma central de gerenciamento, utilizando

inteligência artificial e machine learning para detecção de anomalias, priorização de alertas e geração de relatórios técnicos e executivos periódicos.

16.1.1.15. Assegurar a redundância e a resiliência operacional de todos os componentes, incluindo módulos de NDR, NGIPS, blindagem de vulnerabilidades e MDR, mantendo mecanismos automáticos de failover e replicação segura entre datacenters.

16.1.1.16. Disponibilizar profissionais qualificados e certificados pelo fabricante para todas as atividades de implantação, configuração, suporte técnico e manutenção da solução, conforme perfis mínimos estabelecidos no Termo de Referência e no Anexo VI-F.

16.1.1.17. Garantir compatibilidade plena entre os módulos e equipamentos fornecidos, com atualizações automáticas de firmware, assinaturas, patches de segurança e versões, sem interrupções na operação e sem impacto sobre a disponibilidade dos serviços críticos do Banco.

16.1.1.18. Manter infraestrutura técnica, logística e de suporte suficiente para atuação local e remota, conforme os níveis de atendimento definidos em contrato, assegurando resposta imediata a incidentes, inclusive em regiões remotas da Amazônia Legal.

16.2. DAS OBRIGAÇÕES DO CONTRATANTE

16.2.1. O Banco da Amazônia, na qualidade de **CONTRATANTE**, compromete-se a cumprir as obrigações a seguir, sem prejuízo de outras previstas em lei, no contrato ou em seus anexos, com vistas a assegurar a boa execução do objeto contratado:

16.2.2. Exigir o cumprimento integral de todas as obrigações assumidas pela **CONTRATADA**, em conformidade com as cláusulas contratuais, o Termo de Referência, os Anexos Técnicos e a proposta comercial vencedora.

16.2.3. Designar formalmente os fiscais técnico e administrativo do contrato, os quais exercerão as atividades de acompanhamento e fiscalização da execução dos serviços, conforme previsto no Art. 117 da Lei nº 13.303/2016 e no Art. 99 do Regulamento de Licitações e Contratos do Banco da Amazônia.

16.2.4. Atuar no controle e validação das entregas contratuais, por meio do atesto técnico das Notas Fiscais/Faturas correspondentes às etapas executadas, condicionando o pagamento à comprovação da conformidade dos serviços e ao cumprimento dos SLA acordados.

16.2.5. Rejeitar, total ou parcialmente, os serviços prestados em desacordo com as especificações técnicas, padrões de qualidade, cronograma, prazos ou qualquer outra obrigação prevista contratualmente, comunicando formalmente à **CONTRATADA** as não conformidades apuradas.

16.2.6. Efetuar o pagamento das Notas Fiscais/Faturas apresentadas pela **CONTRATADA**, desde que protocoladas com antecedência mínima de 30

(trinta) dias do vencimento, e que os serviços prestados estejam integralmente atestados pelo setor técnico competente.

16.2.7. Disponibilizar os meios e recursos mínimos necessários à prestação dos serviços contratados, quando aplicável, incluindo:

I. Acesso remoto (VPN) para diagnóstico e suporte;

II. Apoio logístico local, mediante solicitação prévia, nas unidades operacionais do Banco;

III. Autorização para entrada em ambientes de missão crítica, mediante credenciamento prévio do(s)técnico(s) da **CONTRATADA**.

16.2.8. Receber e identificar os prepostos da **CONTRATADA**, adotando as providências administrativas necessárias para garantir o acesso autorizado às dependências do Banco, conforme normas de segurança institucional.

16.2.9. Assegurar que ordens e solicitações relativas à execução dos serviços sejam formalmente encaminhadas ao preposto da **CONTRATADA**, evitando interferência direta nos seus empregados, exceto em situações de emergência ou risco iminente.

16.2.10. Notificar a **CONTRATADA**, por escrito, sempre que houver constatação de falhas, irregularidades ou infrações contratuais, estabelecendo prazo razoável para a sua correção, bem como aplicar penalidades administrativas, quando cabíveis, observando o contraditório e a ampla defesa.

Obrigações Complementares Específicas ao Objeto

16.2.11. Disponibilizar, quando necessário, as informações técnicas e operacionais essenciais para viabilizar a correta configuração dos equipamentos e enlaces contratados, sem que isso implique compartilhamento de informações sigilosas ou estratégicas.

16.2.12. Garantir a interlocução institucional com os demais setores do Banco (como infraestrutura predial, segurança da informação, TI, logística e agências), para assegurar ambiente técnico e organizacional adequado à implantação e operação da solução de Rede.

16.2.13. Planejar, com a devida antecedência, os procedimentos necessários à renovação, substituição ou nova contratação dos serviços, de forma a evitar descontinuidade na prestação dos serviços de conectividade ao término da vigência contratual.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. As partes **CONTRATANTE**s elegem o foro da Comarca de ....., Estado do ....., para a solução de qualquer questão oriunda do presente Contrato, com exclusão de qualquer outro.

17.2. 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.

Belém-PA..... de .....de 202.....

Pelo Banco da Amazônia:

....

Pela **CONTRATADA**:

.....

Testemunhas:

1ª.....
Nome:
CPF:

2ª.....
Nome:
CPF:

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. 11.129/2022.

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)

ANEXO IX

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 90008/2026

ANEXO X

MATRIZ DE RISCO

Categoria	Descrição	Consequência.	Medidas Mitigadoras	Alocação do Risco
Risco de Tempo e Qualidade	Atraso na entrega de equipamentos.	Descumprimento de prazos acordados em cronograma de projeto.	Estabelecer novos prazos de entrega.	**CONTRATADA**.
	Equipamentos em desconformidade com as especificações.	Instalação dos Equipamentos	Reunião c/o preposto para exigência troca dos equipamentos.	Banco
	Fatores de força maior ou modificação do escopo pelo Banco	Aumento do custo	Revisão do preço c/aprovação da Diretoria	Banco
Risco da Atividade Empresarial	Alteração de enquadramento tributário ou mudança de atividade empresarial	Aumento ou redução do lucro da empresa	Planejamento tributário	**CONTRATADA**
	Elevação dos preços de mercado de equipamentos e serviços.	Não entrega de equipamentos	Negociação com o fabricante para solicitação de descontos adicionais.	**CONTRATADA**.
	Aumento dos custos da mão de obra por dissídio da categoria	Aumento do preço do ponto de função	Negociação com a mão de obra para adequação do projeto	**CONTRATADA**.
	Aumento dos custos operacionais	Aumento dos preços do contrato	Planejamento e Negociação	Banco e **CONTRATADA**
Riscos Trabalhistas e Previdenciários	Falta de pagamento de salários, falta de recolhimento de contribuições ao INSS, FGTS, etc.	**CONTRATANTE** considerado como co-responsável.	Fiscalização junto à **CONTRATADA**	Banco
Risco Tributário e Fiscal (não tributário)	Recolhimento indevido ou falta de recolhimento	Débito ou crédito tributário	Ressarcimento pela empresa ou retenção de pagamentos até o limite pago pelo Banco.	**CONTRATADA**.

Risco Operacional	Substituição de empregados da equipe sem anuência do Banco	Retardamento nos prazos de entrega e baixa qualidade dos entregáveis	Fiscalização	Banco.
	Ausência de preposto	Dificuldades no tratamento sobre a execução do contrato.	Fiscalização	Banco
	Não realização de reunião formal de iniciação contratual.	Não entrega de documentos exigidos no contrato, tais como cronogramas, apresentação da equipe, etc.	Fiscalização	Banco
	Rotatividade de mão de obra.	Descumprimento de prazos, atrasos na execução do contrato.	Fiscalização e reunião c/preposto.	Banco
	Desatenção ao Termo de responsabilidade/segurança da informação	Descumprimento de normativos	Fiscalização e Reunião c/preposto	Banco e **CONTRATADA**
	Pagamentos indevidos (a maior)	Influência no resultado operacional do Banco	Ressarcimento do Banco.	Banco e **CONTRATADA**
Riscos Internos	Não aplicação de multas e glosas	Perdas financeiras	Ressarcimento do Banco.	Banco
	Ausência de notificações ao fornecedor	Impedimento para abertura de processo administrativo tempestivo	Gestão e Fiscalização	Banco
	Ausência de livro de ocorrências	Falta de evidências de acompanhamento contratual	Gestão e Fiscalização	Banco
	Ausência de nomeação de fiscal	Descumprimento de normativos internos	Gestão e Fiscalização	Banco
	Não realização de repasse de conhecimento e treinamentos	Falta de acompanhamento contratual	Gestão e Fiscalização	Banco
Riscos de Infraestrutura	Falta de equipamentos por não especificação do cliente	Falha na ativação dos serviços	Verificar especificações	Banco
	Falta de equipamentos por não entrega do fornecedor	Falha na ativação dos serviços.	Analisar detalhadamente proposta e part number de equipamentos	Banco
	Necessidades posteriores a assinatura do contrato	Sem possibilidade de expansão do projeto.	Revisão do preço c/aprovação da Diretoria	Banco

	Incompatibilidade dos equipamentos contratados com a infraestrutura do Banco.	Atraso na implantação por adequação aos equipamentos	Fiscalização/ levantamento da infraestrutura	**CONTRATADA**