SOLICITAÇÃO DE PROPOSTA

REQUEST FOR PROPOSAL — RFP

Solução de Microssegmentação

Chamamento público	Nº 2026/00X
Documento	RFP — Solicitação de Proposta
Área demandante	GPROD — Gerência de Infraestrutura e Produção
Versão	3.2
Prazo da consulta	10 (dez) dias úteis
Classificação	PÚBLICA — detalhamento do ambiente mediante termo de confidencialidade (item 13.1)
Natureza	Consulta pública ao mercado — não constitui compromisso de contratação

Sumário

1. Apresentação 4
   1.1. Natureza e efeitos desta solicitação 4
   1.2. Público-alvo 4
   1.3. Anexos que integram esta RFP 4
2. Contexto da necessidade 5
   2.1. Contexto institucional e de negócio 5
   2.2. Ambiente tecnológico de referência 5
   2.3. Problema a ser endereçado 6
   2.4. Alinhamento estratégico e regulatório 6
3. Objetivo da contratação pretendida 7
   3.1. Resultados esperados 7
   3.2. Fora do escopo 7
4. Escopo resumido da solução 8
   4.1. Composição do fornecimento 8
   4.2. Capacidades funcionais esperadas 8
   4.3. Dimensionamento de referência 9
   4.4. Serviços associados 10
5. Requisitos gerais a serem endereçados na proposta 11
   5.1. Arquitetura e integração 11
   5.2. Modos de implantação 12
   5.3. Disponibilidade, capacidade e continuidade 12
   5.4. Segurança, proteção de dados e conformidade 13
   5.5. Ciclo de vida e atualizações 13
   5.6. Portabilidade e reversibilidade 13
6. Orientações gerais aos fornecedores 14
7. Conteúdo mínimo da proposta técnica 15
8. Conteúdo mínimo da proposta comercial 17
9. Qualificação e experiência do fornecedor 17
10. Critérios de avaliação das respostas 18
11. Modelo de contratação pretendido 19
12. Cronograma indicativo do processo 21
   12.1. Forma de submissão 22
13. Disposições gerais 22
   13.1. Confidencialidade ..... **Erro! Indicador não definido.**
   13.2. Custos de participação ..... **Erro! Indicador não definido.**

13.3. Integridade e conduta ..... **Erro! Indicador não definido.**
13.4. Alterações e cancelamento..... **Erro! Indicador não definido.**
13.5. Canal de comunicação..... **Erro! Indicador não definido.**
14. Checklist de submissão 22
15. Glossário 24

1. Apresentação

O Banco da Amazônia S.A. (“Banco”), por meio da Diretoria de Tecnologia e Negócios (DITEC) e da Gerência de Infraestrutura e Produção (GPROD), torna pública a presente **Solicitação de Proposta (Request for Proposal — RFP)**, com o objetivo de consultar o mercado quanto a soluções corporativas de microssegmentação.

Este documento apresenta o contexto da necessidade, o objetivo pretendido, o escopo resumido da solução, as orientações gerais aos fornecedores e os elementos mínimos exigidos para a submissão das propostas técnica e comercial.

A RFP destina-se a subsidiar o planejamento da contratação, permitindo ao Banco: (i) confirmar a existência de soluções de mercado aderentes à necessidade institucional; (ii) avaliar modelos arquiteturais, comerciais e de licenciamento disponíveis; (iii) apurar referências de preço e de níveis de serviço praticados; e (iv) aprimorar a especificação técnica que instruirá o futuro procedimento de contratação.

1.1. Natureza e efeitos desta solicitação

Esta RFP possui caráter exclusivamente consultivo e preparatório. A apresentação de proposta não gera para o Banco qualquer obrigação de contratar, nem confere ao participante direito de preferência, expectativa de direito, exclusividade, reserva de mercado ou pretensão de ressarcimento de custos incorridos na elaboração da resposta.

A eventual contratação decorrente deste planejamento observará o regime jurídico aplicável ao Banco, notadamente a Lei nº 13.303/2016, o Regulamento de Licitações e Contratos do Banco da Amazônia e as normas internas de seleção e aquisição de soluções de Tecnologia da Informação, sendo precedida de procedimento próprio, com instrumento convocatório específico e ampla publicidade.

As informações fornecidas pelos participantes poderão ser utilizadas, de forma agregada e sem identificação comercial sensível, para instrução do Estudo Técnico Preliminar, do Termo de Referência e da estimativa de preços da futura contratação.

1.2. Público-alvo

Fabricantes, provedores de serviço, integradores, distribuidores e parceiros de canal com capacidade comprovada de fornecer, implantar, integrar e sustentar soluções de microssegmentação por software baseada em agente em ambientes corporativos híbridos de alta criticidade, com atendimento no território nacional e suporte em língua portuguesa.

1.3. Anexos que integram esta RFP

Os proponentes deverão elaborar suas propostas em estrita conformidade com este documento e com os anexos relacionados a seguir, que dele são parte integrante e indissociável para todos os fins. A numeração adotada é a do processo de contratação, preservando-se a correspondência com o Termo de Referência e seus demais anexos.

Anexo	Título	Finalidade na elaboração da proposta
ANEXO I	Especificações Técnicas — Solução de Microssegmentação	Base para a resposta técnica item a item, com indicação de atendimento e evidência documental correspondente.

Anexo	Título	Finalidade na elaboração da proposta
ANEXO II	Acordo de Níveis de Serviço	Indicadores, metas, critérios de medição, severidades, evidências e ajustes de pagamento (glosa) por nível de serviço a serem confirmados ou comentados pelo proponente.
ANEXO III	Matriz de Testes da Prova de Conceito (PoC)	Blocos de teste, casos, procedimentos, evidências esperadas, classificação de criticidade e critérios objetivos de aprovação da demonstração técnica.
ANEXO IV	Modelo de Carta-Proposta de Preços	Formato obrigatório de apresentação da proposta comercial, assinada por representante legal, contendo preços por item, composição da solução ofertada e declarações exigidas.

Em caso de divergência entre o texto desta RFP e o conteúdo dos anexos, prevalecerá: o **Anexo I**, quanto a requisitos e especificações técnicas; o **Anexo II**, quanto a indicadores, metas e critérios de medição de nível de serviço; o **Anexo III**, quanto a procedimentos e critérios de avaliação da Prova de Conceito; e o **Anexo IV**, quanto à forma de apresentação da proposta comercial.

As remissões feitas ao longo deste documento observam a numeração acima. Os demais anexos do Termo de Referência não integram esta consulta e serão disponibilizados oportunamente, por ocasião da publicação do instrumento convocatório; os fundamentos do lote único e da plataforma única de fabricante, constantes do Termo de Referência, estão reproduzidos na seção 11.1 desta RFP.

2. Contexto da necessidade

2.1. Contexto institucional e de negócio

O Banco da Amazônia é instituição financeira federal responsável pela execução da política de desenvolvimento da Amazônia Legal, operando rede de atendimento distribuída em ampla extensão territorial e conjunto crescente de canais digitais de acesso a produtos e serviços financeiros.

A continuidade dos serviços bancários exige que o comprometimento inicial de uma estação ou servidor não se propague livremente a aplicações, bancos de dados e infraestrutura de backup. A contratação busca reduzir esse alcance e produzir evidência auditável de segregação.

2.2. Ambiente tecnológico de referência

O Banco da Amazônia opera um ambiente tecnológico híbrido, distribuído entre dois data centers próprios (site principal e site de contingência) e provedores de nuvem pública. O escopo da solução de microssegmentação abrange os principais tipos de ativo desse ambiente:

- servidores virtualizados na plataforma de virtualização corporativa;
- instâncias em nuvem pública;
- servidores de banco de dados em plataforma dedicada (*engineered systems*);
- nós da plataforma de orquestração de contêineres, nos ambientes de produção, contingência, homologação e gerência;

- estações de trabalho (desktops e notebooks).

A proteção ocorre por meio do agente instalado nos ativos. Os componentes de infraestrutura que não comportam agente, como hosts físicos da plataforma hiperconvergente, equipamentos de backup, interfaces de gerenciamento e elementos de armazenamento, ficam fora da instalação direta. Eles se beneficiam de forma indireta, pelo controle das comunicações originadas ou destinadas a ativos com agente. Contêineres, bancos de dados e demais objetos lógicos executados sobre os ativos licenciados são contexto de operação e não constituem unidades adicionais de licenciamento.

A solução deverá ser compatível com as plataformas de virtualização, nuvem, contêineres e banco de dados em uso e integrar-se aos serviços corporativos de identidade, segurança, automação e operação descritos no Anexo I.

2.3. Problema a ser endereçado

O Banco da Amazônia opera um ambiente tecnológico híbrido, que reúne data centers próprios, nuvem pública, plataforma de contêineres e estações de trabalho. Nesse ambiente, a segurança de rede concentra-se no perímetro e na separação entre grandes zonas, enquanto, dentro de cada zona, os ativos se comunicam com pouca restrição. Na prática, servidores, bancos de dados e estações que não têm necessidade de interagir têm a possibilidade de se comunicar livremente, o que amplia a superfície exposta a ataques internos.

Esse modelo representa um risco relevante diante das ameaças atuais. Ataques modernos, em especial o ransomware, raramente começam pelos sistemas mais valiosos da organização. O invasor costuma entrar por um ponto frágil, como uma estação comprometida por phishing, uma credencial vazada ou um servidor desatualizado, e, a partir dele, desloca-se pela rede até alcançar os ativos críticos. Esse deslocamento interno, conhecido como movimento lateral, permite que um incidente inicialmente localizado se converta em uma paralisação ampla dos serviços, com consequências financeiras, operacionais e de imagem para o Banco.

O cenário também tem reflexos regulatórios e estratégicos. A Resolução CMN nº 4.893/2021, com a redação dada pela Resolução CMN nº 5.274/2025, reforça a exigência de controles de segmentação, rastreabilidade e isolamento dos ambientes que suportam serviços críticos, como o Pix e o STR. O Planejamento Estratégico 2026–2030 e o PDTI 2026–2027, por sua vez, estabelecem a resiliência cibernética e a continuidade dos serviços como prioridades institucionais, o que torna a questão parte da agenda estratégica do Banco, e não apenas um tema técnico.

A solução de microssegmentação enfrenta esse problema em sua origem. Ao mapear as comunicações entre os ativos, ela oferece a visibilidade hoje ausente. Ao aplicar políticas de menor privilégio ativo a ativo, permitindo apenas os fluxos efetivamente necessários, ela reduz os caminhos disponíveis ao invasor. Ao possibilitar o isolamento de um equipamento comprometido em poucos minutos, ela limita o alcance de um ataque e acelera a resposta da equipe de segurança.

Dessa forma, a contratação permitirá ao Banco evoluir de uma defesa centrada no perímetro para um modelo de confiança zero aplicado ao interior da própria rede. Esse avanço protege os ativos críticos, reduz a probabilidade de um incidente se transformar em crise e fortalece as evidências de conformidade apresentadas aos órgãos de supervisão.

2.4. Alinhamento estratégico e regulatório

A iniciativa está alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação e ao Plano Estratégico do Banco, no que se refere à infraestrutura tecnológica segura e escalável, à resiliência cibernética e à continuidade dos serviços de TIC. Relaciona-se, ainda, aos requisitos da Lei nº 13.709/2018 (LGPD), da Resolução CMN nº 4.893/2021 e alterações posteriores e, quando aplicável ao ambiente de meios de pagamento, ao padrão PCI DSS.

3. Objetivo da contratação pretendida

Obter propostas técnicas e comerciais para o fornecimento, implantação e suporte técnico especializado de solução de microssegmentação por software baseada em agente instalado no sistema operacional dos ativos protegidos, independente de hipervisor, hardware de rede e provedor de nuvem, com console única, para vigência contratual de 60 meses e ativação por ondas, compreendendo subscrições, planejamento, integração, homologação, operação assistida por 90 dias, capacitação de 12 profissionais, atualizações e transição de saída.

3.1. Resultados esperados

Reduzir comunicações indevidas e o alcance de um comprometimento; ampliar visibilidade de dependências; viabilizar aplicação por ondas e contenção com reversão; produzir evidências de políticas, registros e cobertura. Benefícios serão medidos com linha de base, sem presumir economia ou redução percentual de incidentes.

Dimensão	Resultado verificável
Segregação	Políticas de menor privilégio e registros de decisões.
Continuidade	Enforcement preservado sem console; reversão de bloqueio indevido.
Visibilidade	Mapas de dependência e inventário reconciliado.
Resposta	Contenção por API com canal de investigação preservado.
Autonomia	Capacitação da equipe do Banco, As Built, runbooks e exportação.
Sustentação	Suporte especializado 24x7, com atualização contínua de versões da plataforma, dos agentes e dos conectores ao longo de toda a vigência.

3.2. Fora do escopo

A solução de microssegmentação complementa os demais controles de segurança e continuidade do Banco e não os substitui. Proteção de estações e servidores contra códigos maliciosos, gestão de vulnerabilidades, cópias de segurança, recuperação de desastres e controle de acesso remoto continuam a cargo das ferramentas próprias. Por isso, os benefícios atribuídos à contratação ficam restritos ao que a solução comprovadamente entrega: visibilidade das comunicações internas, restrição de fluxos desnecessários e contenção de incidentes.

A proteção alcança os ativos em que a solução é instalada. Alguns componentes da infraestrutura não admitem essa instalação, como equipamentos físicos de suporte, de armazenamento e de gerenciamento. Esses componentes ficam fora da cobertura direta, mas se beneficiam de forma indireta, porque as comunicações deles com os ativos protegidos passam a ser controladas.

Aplicações, bancos de dados e demais recursos executados sobre os ativos protegidos estão cobertos pela mesma licença, sem custo adicional.

4. Escopo resumido da solução

O escopo desta seção é apresentado em nível gerencial, suficiente para orientar a elaboração das propostas. O detalhamento técnico integral, com requisitos individualizados, critérios de aceitação e procedimentos de teste, consta do **Anexo I — Especificações Técnicas**.

4.1. Composição do fornecimento

A composição abaixo corresponde à estrutura de itens adotada no **Anexo IV — Modelo de Carta-Proposta de Preços**, que deverá ser integralmente observada na proposta comercial.

Item	Descrição	Unidade (quantidade)
1	Subscrição de microssegmentação por agente — servidor (físico, virtual ou instância em nuvem), 60 meses	Servidor (863)
2	Subscrição de microssegmentação por agente — nó de cluster OpenShift (worker, master e infraestrutura), 60 meses	Nó (71)
3	Subscrição de microssegmentação por agente — estação de trabalho (desktop ou notebook), 60 meses	Estação de trabalho (4.066)
4	Planejamento, implantação, integração e homologação	Serviço (1)
5	Operação assistida (90 dias)	Serviço (1)
6	Capacitação técnica oficial e transferência de conhecimento	Vaga (12)
7	Suporte técnico especializado 24x7	Mês (60)

4.2. Capacidades funcionais esperadas

Microssegmentação por agente com enforcement local e autônomo; console única; mapeamento de dependências; rotulagem; simulação, aplicação gradual e reversão; regras por identidade e processo; proteção OpenShift; contenção via API; registros, relatórios e integração corporativa. As capacidades mínimas estão relacionadas a seguir, e seu detalhamento consta do **Anexo I**.

Capacidade	Descrição resumida
Arquitetura baseada em agente	Microssegmentação por software, com agente instalado em cada ativo protegido: servidores físicos, máquinas virtuais nos data centers do Banco, instâncias em nuvem pública, nós da plataforma de contêineres e estações de trabalho.
Visibilidade das comunicações	Mapa gráfico das dependências entre aplicações, em tempo quase real e com histórico, organizado por aplicação e ambiente.

Capacidade	Descrição resumida
Classificação dos ativos	Identificação dos ativos por rótulos como ambiente, aplicação, função, localização, criticidade e enquadramento regulatório (por exemplo, Pix).
Políticas de segurança	Regras definidas a partir dos rótulos que permitem apenas as comunicações autorizadas e bloqueiam todas as demais.
Proteção de contêineres	Cobertura da plataforma de contêineres com licenciamento por servidor do cluster, sem cobrança adicional por contêiner.
Resposta a incidentes	Isolamento rápido de um ativo ou grupo comprometido, preservando o acesso das equipes de investigação.
Integração e automação	Interface de programação (API) documentada e segura para automatizar a gestão de ativos, regras, ações de contenção e auditoria.
Registros e auditoria	Guarda dos registros de auditoria, comunicações e alertas, na solução ou no SIEM, conforme a política do Banco e a regulamentação.

4.3. Dimensionamento de referência

4.3.1 Informações complementares de dimensionamento

Para permitir a comparação das propostas e identificar limitações e custos adicionais, o proponente deverá informar, considerando os quantitativos de referência, as premissas adotadas e a fonte de cada informação sobre volumetria de fluxos e eventos, capacidade de processamento, armazenamento, retenção de dados, funcionalidades AIR, implantação, escalabilidade e licenciamento.

4.3.2 Referência de dimensionamento

Os quantitativos indicados a seguir constituem referência de dimensionamento para fins de elaboração das propostas e poderão ser revistos na etapa de especificação definitiva, inclusive em função das contribuições recebidas nesta consulta.

O dimensionamento da solução partiu do inventário mais recente da área de infraestrutura e abrange três grupos de ativos: servidores (virtualizados, em nuvem pública e de banco de dados), nós da plataforma de contêineres e estações de trabalho.

O dimensionamento não inclui reserva para crescimento sem justificativa formal aprovada. Também não considera máquinas inativas na cobertura ativa. A solução deve ter capacidade para a ativação simultânea dos ambientes de produção e de contingência; a cobrança seguirá as regras de licenciamento do Anexo I (LIC-03).

Parâmetro	Referência	Observação
Servidores protegidos	863 servidores	Servidores virtualizados, instâncias em nuvem pública e servidores de banco de dados. Quantidade provisória, que será conciliada com o inventário antes do edital. A inclusão dos

Parâmetro	Referência	Observação
		servidores de banco de dados em plataforma dedicada depende de compatibilidade e da concordância do fabricante.
Nós da plataforma de contêineres	71 nós	Inclui nós de controle (*masters*), de infraestrutura e de trabalho. A licença deverá cobrir todos os contêineres executados no nó.
Estações de trabalho	4.066	Desktops e notebooks. Inclusão condicionada à comparação com o firewall de host da solução de EDR já contratada (Anexo I, item 1.1.3).
Capacidade total de referência	5.000 ativos	Soma dos grupos acima, para planejamento. Não inclui margem implícita de crescimento.
Prazo de vigência estimado	60 meses	Inclui implantação, sustentação e transição de saída
Capacitação	12 vagas	Treinamento técnico e prático

4.4. Serviços associados

4.4.1. Implantação e integração

A contratada deverá apresentar um plano de implantação com o levantamento do ambiente, a priorização dos ativos críticos, o modelo de governança das regras, o cronograma, os riscos e o plano de reversão. A execução será gradual e feita em conjunto com a equipe do Banco: instalação dos agentes, mapeamento das comunicações validado pelos responsáveis pelas aplicações e aplicação das regras por ondas, com testes de contenção e entrega da documentação final. Nos ambientes mais sensíveis, as intervenções ocorrerão em janelas acordadas, preservando as comunicações essenciais e a continuidade dos serviços.

4.4.2. Treinamento e transferência de conhecimento

A contratada deverá oferecer capacitação técnica e prática às equipes indicadas pelo Banco. O conteúdo abrangerá a arquitetura e a administração da solução, a instalação e a gestão dos agentes, a classificação dos ativos e o mapeamento das comunicações entre aplicações. Incluirá também o ciclo de vida das regras de proteção, da criação à simulação, aprovação e aplicação, além da contenção e do isolamento de ativos em incidentes. Completam o programa as integrações com as ferramentas de segurança do Banco, os relatórios, a alta disponibilidade e os procedimentos de contingência.

4.4.3. Suporte e sustentação

Suporte técnico em regime 24x7 por telefone, correio eletrônico e portal de chamados, compreendendo registro e classificação de chamados, diagnóstico e correção de falhas, apoio ao tratamento de incidentes, escalonamento ao fabricante, manutenção das integrações, atualizações de versão da plataforma, dos agentes e dos conectores, e atualização da documentação técnica. As severidades, os tempos de resposta inicial, de contorno e de solução

definitiva (TRI, TCR e TSD), os critérios de medição e os ajustes de pagamento por nível de serviço constam do **Anexo II**.

4.4.4. Transição de saída

Até 90 dias antes do término do contrato, a contratada deverá apresentar um plano de transição de saída que assegure a continuidade da proteção do ambiente e a preservação das informações do Banco. O plano deverá prever a entrega, em formato aberto e reutilizável, de todas as informações produzidas durante a vigência: classificação dos ativos, regras de proteção e respectivas exceções, inventário, mapas de comunicação e registros.

A contratada deverá admitir a convivência temporária com a solução sucessora e conduzir a remoção dos agentes de forma coordenada, sem indisponibilidade dos serviços. Também deverá revogar todos os acessos concedidos e eliminar com segurança os dados do Banco sob sua guarda, com apresentação de evidências. Por fim, os scripts e as integrações desenvolvidos e remunerados no âmbito do contrato passarão a pertencer ao Banco.

5. Requisitos gerais a serem endereçados na proposta

Os requisitos desta seção são apresentados em nível gerencial e não substituem as especificações do **Anexo I**, às quais o proponente deverá responder item a item.

5.1. Arquitetura e integração

O Banco busca uma solução de microssegmentação por software baseada em agente, em que as regras de proteção sejam aplicadas no próprio sistema operacional de cada ativo protegido. A solução deve funcionar de forma independente do hipervisor, do hardware de rede e do provedor de nuvem. Ela deverá cobrir de modo uniforme os servidores físicos e virtuais dos data centers do Banco, as instâncias em nuvem pública, os nós da plataforma de contêineres e as estações de trabalho. Soluções cujo mecanismo principal dependa de firewall distribuído do hipervisor, de recursos da infraestrutura de rede ou de orquestração remota sem agente não atendem ao objeto.

A consistência da proteção entre os diferentes ambientes é requisito de resultado. O fornecedor deverá descrever objetivamente, na proposta técnica, como sua arquitetura assegura:

- a aplicação uniforme das regras de proteção em todos os tipos de ativo, independentemente do ambiente em que estejam hospedados;
- o uso de uma única classificação dos ativos (rótulos) e de uma única base de regras para todos os ambientes;
- a coleta e a correlação centralizadas das comunicações e dos eventos de segurança, com visão integrada de todo o ambiente;
- a propagação das alterações de regras e das ações de contenção a todos os ativos afetados, sem janelas de inconsistência entre ambientes;
- a continuidade da proteção nos ativos em caso de perda de comunicação com a console de gestão.

Para esse resultado, o Banco considera preferível uma plataforma única, de um único fabricante, com console única de gestão para todos os tipos de ativo. Essa preferência será confirmada como requisito somente se a consulta ao mercado demonstrar que ela é atendida por mais de um fabricante. Os respondentes deverão informar se a solução proposta atende a essa condição e, caso não atenda, quais componentes são de terceiros e como se dá a integração entre eles.

Deverão ser indicados os sistemas operacionais e as plataformas suportados, com as respectivas versões, incluindo, conforme aplicável:

- sistemas Windows Server e distribuições Linux corporativas, inclusive Oracle Linux e Red Hat Enterprise Linux;
- sistemas operacionais de estações de trabalho;
- VMware vSphere;
- Oracle Cloud Infrastructure (OCI) e Microsoft Azure;
- Red Hat OpenShift e Kubernetes;
- servidores de banco de dados em plataforma Oracle Exadata, com indicação expressa da posição do fabricante Oracle quanto à instalação do agente.

Deverão ser descritos os mecanismos de integração com os componentes corporativos do Banco, por meio de APIs documentadas, conectores, webhooks, Syslog, CEF, LEEF, JSON ou outros padrões abertos e interoperáveis. A descrição deverá contemplar, no mínimo:

- VMware vCenter, OCI e Azure;
- serviços de diretório (Active Directory e Microsoft Entra ID);
- SIEM;
- ServiceNow Security Incident Response (SIR) e ferramentas de gestão de serviços de TI;
- demais ferramentas de segurança do Banco, como proteção de endpoint e gestão de acessos privilegiados.

Para cada integração, o fornecedor deverá informar se ela é nativa ou depende de desenvolvimento, e se a considera obrigatória ou desejável no contexto do Banco.

5.2. Modos de implantação

O fornecedor deverá indicar se a console de gestão é oferecida em nuvem (SaaS), instalada nos data centers do Banco (*on-premises*) ou nos dois modelos; o Banco aceita qualquer um deles. No modelo SaaS, só serão admitidos localmente os agentes e eventuais conectores leves. No modelo *on-premises*, a proposta deverá listar os recursos de infraestrutura necessários, que serão providos pelo Banco. Em ambos, as regras serão aplicadas no próprio ativo protegido, sem alterar a rede nem criar ponto único de falha.

O modelo exclusivamente SaaS constitui a arquitetura inicialmente pretendida para fins desta consulta ao mercado, cuja adoção definitiva será confirmada após a avaliação das respostas dos participantes, nos termos do item 1.3.2-A do Anexo I.

Os agentes deverão operar em modo somente visibilidade, que será o padrão inicial, e em modo de aplicação das regras, selecionáveis por ativo ou grupo para uma transição gradual. O fornecedor também deverá descrever como o agente se comporta se perder a comunicação com a console ou falhar.

5.3. Disponibilidade, capacidade e continuidade

O fornecedor deverá descrever os mecanismos de alta disponibilidade, redundância e contingência da solução e o comportamento dela em falhas. Os agentes devem continuar aplicando a última regra válida mesmo sem comunicação com a console. Constituem mínimos de referência a disponibilidade mensal de 99,9% no modelo SaaS e, no modelo *on-premises*, a operação em cluster com replicação entre os sites do Banco, sem ponto único de falha em nenhum dos dois.

A proposta deverá demonstrar capacidade para os 5.000 ativos de referência, sem reserva adicional presumida. Também deverá explicar o tratamento das licenças de ativos inativos e de contingência e informar os alertas de consumo. Atingir o limite contratado não poderá suspender a proteção, causar perda de registros ou degradar os serviços.

5.4. Segurança, proteção de dados e conformidade

O fornecedor deverá demonstrar os controles de gestão, registro e segurança da própria solução previstos no Anexo I, contemplando no mínimo:

- controles de acesso administrativo à console com autenticação multifator (MFA), integração com o serviço de diretório do Banco, controle baseado em funções (RBAC), menor privilégio, segregação de funções e trilhas de auditoria individualizadas e protegidas contra alteração;
- criptografia dos dados em trânsito e em repouso, inclusive na comunicação entre agentes e console, com autenticação mútua e proteção de credenciais, chaves e segredos;
- proteção dos agentes contra desativação, desinstalação ou adulteração não autorizadas, com alerta à console em caso de tentativa;
- distribuição de atualizações dos agentes e da plataforma por canal seguro, com verificação de integridade e assinatura digital;
- retenção configurável dos registros por tipo (auditoria administrativa, comunicações e alertas), na própria solução ou no SIEM do Banco, conforme política interna, com exportação em formato aberto;
- indicação dos locais de processamento, armazenamento, retenção e cópia de segurança dos dados e registros, bem como dos suboperadores e terceiros envolvidos, especialmente no modelo SaaS;
- aderência à Lei nº 13.709/2018 (LGPD) e à Resolução CMN nº 4.893/2021, com a redação dada pela Resolução CMN nº 5.274/2025, inclusive quanto aos requisitos de contratação de serviços de processamento e armazenamento de dados em nuvem;
- certificações de segurança e conformidade do fabricante e do provedor do serviço em nuvem, quando aplicável, com indicação de escopo e vigência.

A solução contribui de forma parcial ou complementar para o cumprimento das exigências regulatórias, conforme a matriz informativa do Anexo I. O atendimento integral dessas exigências depende do conjunto de controles do Banco, e não exclusivamente desta contratação.

5.5. Ciclo de vida e atualizações

Todos os componentes ofertados deverão ser originais, regularmente licenciados e estar em versões estáveis e suportadas pelo fabricante. O ciclo de vida deverá ser compatível com o período estimado de contratação. O fornecedor deverá confirmar o fornecimento, sem ônus adicional e durante toda a vigência, de atualizações de versão da plataforma e dos agentes, correções de segurança, atualização de conectores e integrações e suporte a novas versões dos sistemas operacionais e das plataformas em uso pelo Banco. Também deverá confirmar a substituição, sem custo, de componentes que percam suporte durante a vigência.

A atualização da console de gestão não poderá interromper a aplicação das regras de proteção nos ativos. A atualização dos agentes deverá ser feita a partir da console, em lotes e por grupo de ativos, com agendamento de janelas e possibilidade de reversão, sem necessidade de acesso manual a cada equipamento.

5.6. Portabilidade e reversibilidade

A solução deverá permitir exportar rótulos, regras, exceções, inventário, mapas de comunicação, configurações e registros em formatos abertos e documentados. Isso evita a dependência tecnológica e viabiliza a substituição futura. A retirada dos agentes deverá remover todas as regras aplicadas, sem deixar ativos isolados e sem interromper as aplicações.

Até 90 dias antes do fim do contrato, o fornecedor apresentará um plano de saída. O plano deverá prever a entrega dos dados exportados, a convivência com a solução sucessora, a remoção coordenada dos agentes, a revogação de acessos, a eliminação segura dos dados e a cessão ao Banco dos scripts e integrações desenvolvidos.

6. Orientações gerais aos fornecedores

1. As propostas deverão ser elaboradas em estrita conformidade com este documento e com os Anexos I, II, III e IV, observando-se obrigatoriamente o modelo de carta-proposta do Anexo IV.
2. A proposta deverá identificar o fabricante, a edição, a versão, os módulos e os componentes ofertados, bem como a infraestrutura exigida para seu funcionamento. A proposta deve refletir solução efetivamente disponível no mercado na data da submissão. Funcionalidades em *roadmap*, em desenvolvimento ou anunciadas para versões futuras devem ser expressamente identificadas como tal e não serão consideradas como atendimento.
3. Todos os módulos, licenças, subscrições, componentes e serviços indispensáveis ao funcionamento da solução devem estar identificados e precificados. Itens essenciais apresentados como opcionais, condicionados ou omitidos não serão considerados.
4. O fornecedor deve explicitar as premissas adotadas, as dependências técnicas e as responsabilidades atribuídas ao Banco que sustentam sua proposta, incluindo recursos de infraestrutura, acessos, janelas de mudança e participação de equipes internas.
5. O fornecedor deverá informar se a solução é composta por produtos de um único fabricante, com console única de gestão para todos os tipos de ativo, conforme o item de arquitetura e integração. Os serviços de implantação, suporte e capacitação poderão ser prestados pela proponente, pelo fabricante ou por parceiros sob responsabilidade integral da proponente. Deverão ser descritos o modelo de integração com os componentes corporativos do Banco e a responsabilidade pela operação de ponta a ponta.
6. As respostas devem ser objetivas e verificáveis. Cada requisito deverá ter remissão à documentação técnica oficial do fabricante, com indicação do documento, da seção ou página, do trecho pertinente e do endereço eletrônico em que a informação possa ser confirmada.
7. Materiais publicitários, apresentações institucionais e declarações genéricas de atendimento não substituem evidência técnica. Declarações também não substituem a demonstração de eficácia, desempenho ou comportamento em falha, que poderá ser verificada em prova de conceito.
8. O fornecedor deve indicar, de forma transparente, os requisitos desta RFP ou do Anexo I que sua solução não atende ou atende parcialmente, com a respectiva justificativa técnica. Quando cabível, poderá propor alternativa equivalente, que será recebida como contribuição à consulta e não implica dispensa do requisito. Nesta etapa, o não atendimento a requisitos desejáveis não exclui o participante.
9. O fornecedor deverá manifestar-se expressamente sobre:
    - a viabilidade de execução dos casos de teste do Anexo III, indicando recursos necessários, prazo de preparação, eventuais restrições operacionais e infraestrutura exigida para o laboratório isolado;
    - a viabilidade de instalação do agente nos servidores de banco de dados da plataforma Oracle Exadata, com indicação da posição do fabricante Oracle;
    - a convivência do agente com a solução de proteção de endpoint em uso no Banco;
    - a cobertura dos nós de controle e de gerência da plataforma de contêineres, bem como a métrica de licenciamento por nó;

- o tratamento das licenças nos cenários de replicação e de contingência.

10. Contribuições quanto a parâmetros de dimensionamento, métricas de licenciamento, modelos de precificação, indicadores de nível de serviço e boas práticas de mercado são bem-vindas e serão consideradas no aprimoramento da especificação. Os parâmetros pendentes de definição deverão receber contribuição fundamentada, pois serão fixados pelo Banco antes do edital, de forma uniforme e auditável para todos os participantes.
11. Os participantes deverão identificar eventuais requisitos técnicos ou condições de fornecimento que possam restringir a oferta de soluções disponíveis no mercado, apresentando justificativa técnica e, quando aplicável, propostas de atendimento funcionalmente equivalente. As contribuições deverão demonstrar como a alternativa sugerida preserva os objetivos de segurança, desempenho, integração, disponibilidade e continuidade pretendidos pelo Banco. Essas manifestações serão consideradas na consolidação da especificação definitiva, sem implicar aceitação automática das alternativas propostas.

O Banco poderá solicitar esclarecimentos complementares, agendar sessões técnicas de aprofundamento e requerer demonstração funcional da solução, observado tratamento isonômico entre os participantes e o prazo de 10 (dez) dias úteis fixado para a consulta.

7. Conteúdo mínimo da proposta técnica

A proposta técnica deverá ser apresentada em documento estruturado, preferencialmente seguindo a ordem abaixo, com identificação clara das seções e remissão aos itens correspondentes do **Anexo I**.

Nº	Seção	Conteúdo mínimo
A	Sumário executivo	Visão geral da solução proposta, diferenciais e aderência à necessidade descrita nesta RFP (até 2 páginas).
B	Arquitetura proposta	Desenho lógico da solução: agentes, console de gestão (SaaS ou *on-premises*), conectores e coletores, infraestrutura exigida, fluxos de comunicação entre os componentes e modelo de gestão e correlação de eventos.
C	Composição da solução	Fabricante, produto, edição, versão, módulo, SKU ou *part number*, métrica de licenciamento, quantidade, período de cobertura e função na arquitetura, conforme quadro do Anexo IV.
D	Cobertura e compatibilidade	Tipos de ativo cobertos por unidade de licença e versões suportadas de sistemas operacionais e plataformas. Inclui a manifestação sobre convivência com a solução de proteção de endpoint, instalação nos servidores Oracle Exadata, cobertura dos nós de controle e de gerência do OpenShift e tratamento dos ativos que não comportam agente.
E	Matriz de aderência	Resposta item a item aos 104 requisitos do Anexo I, separando obrigatórios e desejáveis e indicando atendimento pleno, parcial ou não atendimento, com

Nº	Seção	Conteúdo mínimo
		evidência documental (documento, endereço eletrônico, página ou seção).
F	Políticas e contenção	Modelo de rótulos, uso de identidade e processo nas regras, simulação de impacto, aprovação, aplicação gradual, reversão e isolamento de ativos comprometidos.
G	Integrações	Modelo de integração por API com SIEM, Active Directory e Entra ID, vCenter, OCI, Azure, ServiceNow SIR e demais ferramentas de segurança, com indicação de mecanismos e formatos suportados.
H	Disponibilidade e continuidade	Alta disponibilidade da console, contingência, *failover* e *failback*; comportamento dos agentes sem comunicação com a console; limites técnicos e escalabilidade.
I	Níveis de serviço	Manifestação quanto aos indicadores, metas, severidades e critérios de medição do Anexo II, com indicação dos SLA efetivamente praticados e contribuição para os parâmetros pendentes de definição.
J	Segurança e privacidade	Controles de acesso, criptografia, proteção dos agentes contra adulteração, retenção e localização de dados, suboperadores, certificações e conformidade
K	Licenciamento	Métrica de licenciamento, realocação de licenças entre ativos, tratamento de ambientes de contingência e de ativos inativos, itens incluídos na subscrição e condições de expansão.
L	Implantação	Metodologia, ondas, cronograma referencial, marcos, matriz de responsabilidades (RACI), critérios de aceite, plano de reversão, equipe alocada e premissas de execução.
M	Capacitação	Programa de treinamento para 12 participantes, com carga horária, formato, conteúdo e materiais.
N	Sustentação	Operação assistida por 90 dias, estrutura de suporte 24x7, canais, escalonamento ao fabricante, idioma de atendimento e atualizações.
O	Prova de conceito	Manifestação quanto aos casos de teste do Anexo III, recursos necessários, amostra de ativos, evidências a serem produzidas, prazo de preparação e eventuais restrições.

Nº	Seção	Conteúdo mínimo
P	Transição de saída	Estratégia de reversibilidade, artefatos exportáveis e formatos, remoção dos agentes sem regras residuais e eliminação segura de dados.
Q	Referências	Experiências anteriores em ambientes de porte e complexidade comparáveis, com escopo, período e quantidade de ativos protegidos.
R	Premissas e exceções	Dependências, condicionantes, limitações conhecidas e eventuais desvios em relação a esta RFP e aos seus anexos.

8. Conteúdo mínimo da proposta comercial

A proposta comercial deverá ser apresentada em documento separado da proposta técnica, obrigatoriamente conforme o modelo do Anexo IV (Modelo de Carta-Proposta de Preços), em moeda nacional, com valores expressos com até duas casas decimais. Deverá conter, no mínimo:

- preços unitários e totais de cada um dos itens 1 a 7, conforme o quadro do Anexo IV;
- valor global da proposta e sua distribuição ao longo do período estimado de 60 (sessenta) meses, com memória de cálculo anual e mensal;
- identificação clara da parcela não recorrente (implantação, operação assistida e capacitação) e da parcela recorrente (subscrições e suporte);
- quadro de composição da solução ofertada, com fabricante, produto, edição, módulo, SKU ou *part number*, métrica de licenciamento, quantidade e prazo de cobertura;
- indicação expressa dos custos já incluídos na subscrição, especialmente o suporte do fabricante, para evitar cobrança em duplicidade entre itens;
- regras de licenciamento aplicáveis à realocação de licenças entre ativos, aos ambientes de contingência, aos ativos inativos e a eventuais excedentes;
- condições para ativação das licenças por ondas de implantação, dentro de marcos únicos de início e de término do contrato;
- custos de infraestrutura, quando a console for *on-premises*, e de integrações, se houver;
- tributos, encargos, deslocamentos e demais custos diretos e indiretos considerados;
- condições comerciais e de reajuste propostas, com indicação de sua validade ao longo do período considerado;
- prazo de validade da proposta de 90 (noventa) dias, conforme o modelo do Anexo IV.

Caso o modelo comercial do fornecedor não permita a precificação isolada de determinado item, deverá ser demonstrado objetivamente que os respectivos custos estão integralmente contemplados no preço do item principal, sem redução de capacidade, dupla contagem ou transferência de custos entre itens.

Eventuais modelos alternativos de licenciamento ou de precificação poderão ser apresentados como proposta complementar, desde que a proposta principal observe o modelo do Anexo IV.

9. Qualificação e experiência do fornecedor

Para fins de avaliação da capacidade de execução, o participante deverá informar:

- a identificação completa da pessoa jurídica, o papel no fornecimento (fabricante, integrador, distribuidor ou parceiro) e o tempo de atuação no segmento;
- as experiências anteriores em implantação, integração, operação ou sustentação de soluções de microssegmentação baseadas em agente, com escopo executado, período, ambiente e porte, incluindo:
    - número de ativos protegidos, por tipo (servidores, nós de contêineres e estações de trabalho);
    - atuação em ambientes híbridos, com data center próprio e nuvem pública;
    - integrações realizadas;
    - serviços prestados;
- a estrutura de suporte técnico 24x7, os canais de atendimento, o processo formal de escalonamento ao fabricante e a capacidade de atendimento remoto e presencial;
- os perfis profissionais disponíveis para o projeto, incluindo:
    - preposto;
    - gerente de projeto;
    - arquiteto da solução;
    - especialistas em microssegmentação e em segurança de redes;
    - profissional de integração e automação;
    - profissional de infraestrutura, nuvem e plataformas de contêineres;
- quando o participante não for o fabricante, a forma de comprovação de acesso regular a licenças, atualizações, suporte oficial e mecanismos de escalonamento durante todo o período considerado.

As informações prestadas nesta seção destinam-se exclusivamente à compreensão da capacidade de mercado; não constituem habilitação nem exigem comprovação documental nesta fase, cujos requisitos serão estabelecidos no futuro instrumento convocatório.

10. Critérios de avaliação das respostas

As respostas recebidas serão analisadas por equipe técnica designada pelo Banco, com base nos critérios abaixo, de forma qualitativa e comparativa, exclusivamente para fins de planejamento da contratação.

Critério	Elementos considerados
Aderência funcional	Atendimento dos requisitos obrigatórios e identificação dos desejáveis do Anexo I, com evidência documental verificável.
Cobertura do ambiente	Compatibilidade com os tipos de ativo, sistemas operacionais e plataformas do inventário de referência, inclusive Oracle Exadata, OpenShift e estações de trabalho.
Consistência arquitetural	Coerência entre a arquitetura proposta, o ambiente tecnológico do Banco e o modelo de gestão, visibilidade e contenção.
Viabilidade de implantação	Aplicação efetiva das regras nos ativos, metodologia por ondas, convivência com a solução de proteção de endpoint, plano de reversão, dependências declaradas e realismo do cronograma.

Critério	Elementos considerados
Capacidade e resiliência	Limites técnicos documentados, escalabilidade e comportamento da solução em falhas.
Maturidade operacional	Estrutura de suporte, aderência aos indicadores e metas do Anexo II, processos de escalonamento e atendimento em português.
Segurança e conformidade	Proteção da própria solução, tratamento e localização de dados, certificações e aderência regulatória.
Sustentabilidade econômica	Custo total em 60 meses, incluídos serviços e ativação por ondas; transparência da composição de preços; clareza da métrica de licenciamento; ausência de custos condicionados ou duplicados.
Reversibilidade	Exportação de artefatos em formatos abertos, remoção dos agentes sem regras residuais e redução de dependência tecnológica.
Competitividade	Quantidade de fabricantes e integradores aptos a atender ao modelo de contratação proposto.
Clareza de resposta	Objetividade, completude e organização das informações, inclusive quanto à observância do modelo do Anexo IV.

O Banco poderá, a seu exclusivo critério, solicitar demonstração funcional da solução em ambiente controlado, observados os casos de teste do Anexo III e assegurado tratamento isonômico aos participantes.

O futuro procedimento de contratação prevê a prova de conceito como etapa formal de validação técnica. A prova será realizada com o primeiro colocado, em laboratório isolado, com resultado de atende ou não atende para cada requisito obrigatório aplicável. A aprovação exigirá o atendimento integral desses requisitos.

11. Modelo de contratação pretendido

As informações desta seção são indicativas e destinam-se a permitir que o participante dimensione adequadamente sua proposta. As definições finais constarão do instrumento convocatório.

Aspecto	Orientação indicativa
Regime jurídico	Lei nº 13.303/2016, Regulamento de Licitações e Contratos do Banco da Amazônia e normas internas aplicáveis.
Vigência estimada	60 (sessenta) meses, contados da assinatura do contrato.
Estrutura do objeto	Lote único, com adjudicação global e componentes individualizados; console única de gestão para todos os tipos de

Aspecto	Orientação indicativa
	ativo, com fabricante único como preferência sujeita à verificação nesta consulta (item 11.1); compreendendo fornecimento, implantação, sustentação e transição, com responsabilidade fim a fim da contratada.
Dedicação de mão de obra	Sem dedicação exclusiva de mão de obra, com execução orientada a resultados, entregas e níveis de serviço.
Local de prestação	Execução preponderantemente remota, com atendimento presencial eventual nas unidades do Banco quando necessário.
Reajuste	Periodicidade mínima de 12 meses; índice a definir no instrumento convocatório, admitida sugestão do proponente (seção 8).
Níveis de serviço	Apuração mensal, com relatório de SLA e ajustes de pagamento (glosa) por descumprimento, conforme o **Anexo II**.
Validação técnica	Prova de Conceito com o licitante provisoriamente classificada em primeiro lugar, conforme o **Anexo III**.
Fiscalização	Acompanhamento por gestor e fiscais designados, com verificação de entregas, disponibilidade, desempenho e níveis de serviço.

11.1. Lote único e plataforma única — fundamentos

O objeto será licitado em lote único, com adjudicação pelo menor preço global. A proposta deverá individualizar componentes, quantitativos, métricas de licenciamento e preços unitários. A contratada terá responsabilidade integral pela implantação, operação assistida, suporte, continuidade e transição da solução. A decisão decorre do Estudo Técnico Preliminar (seção "Justificativas para o não parcelamento da solução") e do Termo de Referência, e se fundamenta no art. 32, inciso III, da Lei nº 13.303/2016, na Súmula TCU nº 247 e no Regulamento de Licitações e Contratos do Banco.

Natureza do objeto e prática de mercado. As soluções de microssegmentação são comercializadas como subscrição de uma única plataforma, licenciada por ativo protegido (servidor, nó de contêineres ou estação de trabalho) e gerenciada a partir de uma console central. Os serviços de implantação, operação assistida, capacitação e suporte dependem do conhecimento do produto ofertado. As regras de proteção são construídas sobre os mapas de comunicação gerados pelos próprios agentes. O parcelamento entre fornecedores distintos criaria lotes artificiais sobre a mesma plataforma e diluiria a responsabilidade por bloqueios indevidos e falhas de proteção.

Interdependência e economicidade. Licenças, implantação, operação assistida e suporte são tecnicamente interdependentes. Em contratos separados, cada fornecedor poderia cumprir isoladamente seu nível de serviço mesmo com falha do resultado, e caberia ao Banco a integração e a arbitragem entre as partes. Sob a ótica do custo total em 60 meses, o lote único evita duplicidade de implantação, integração, suporte, capacitação, prova de conceito e transição. Também assegura continuidade entre as fases do contrato e uma gestão contratual mais eficiente.

Segregação de itens dentro do lote. O parcelamento foi atendido pela divisão do lote em itens com preço próprio:

- subscrição por tipo de ativo;
- implantação;
- operação assistida;
- capacitação;
- suporte.

Essa divisão preserva a transparência de preços e a fiscalização item a item sem fragmentar a responsabilidade técnica.

Plataforma única de fabricante. Trata-se de requisito técnico distinto do lote único. O Banco considera preferível que todos os componentes pertençam a uma única plataforma, de um único fabricante, com console única de gestão para todos os tipos de ativo. Com isso, rótulos, regras e telemetria permanecem consistentes entre os ambientes do data center, da nuvem, da plataforma de contêineres e das estações de trabalho. A exigência será mantida somente se esta consulta confirmar que múltiplos fabricantes a atendem. Os serviços de implantação, suporte e capacitação poderão ser prestados pela proponente, pelo fabricante ou por parceiros sob responsabilidade integral da proponente.

A presente consulta ao mercado destina-se também a verificar a existência de fabricantes e integradores aptos a atender à modelagem proposta, considerando os requisitos técnicos, as condições de fornecimento e a estrutura integrada da contratação. As respostas recebidas subsidiarão a avaliação da competitividade, da viabilidade do lote único e da conveniência técnica de adoção de plataforma de fabricante único. Caso sejam identificadas restrições relevantes à participação de fornecedores ou alternativas tecnicamente equivalentes, a modelagem será reavaliada antes da consolidação do Termo de Referência e da publicação do instrumento convocatório

12. Cronograma indicativo do processo

O cronograma abaixo observa o prazo de 10 (dez) dias úteis de disponibilidade da consulta pública, contados da publicação no Diário Oficial e no sítio eletrônico do Banco. O cronograma poderá ser ajustado mediante comunicação aos participantes.

Etapa	Atividade	Prazo de referência
1	Publicação do chamamento no Diário Oficial e no sítio eletrônico do Banco	D (início da contagem)
2	Envio de dúvidas e sugestões pelos participantes	Até D+7 dias úteis
3	Submissão das propostas técnicas e comercial, conforme Anexos I, II, III e IV	Até D+10 dias úteis
4	Encerramento da consulta pública	D+10 dias úteis
5	Análise técnica e comercial das respostas recebidas	Após o encerramento da consulta
6	Sessões de esclarecimento e demonstrações, se aplicável	Conforme convocação do Banco
7	Adequação do Termo de Referência e prosseguimento do rito de contratação	Etapa subsequente

Não serão consideradas propostas recebidas após o encerramento do prazo de 10 (dez) dias úteis.

12.1. Forma de submissão

As propostas e demais informações deverão ser encaminhadas para o endereço eletrônico licitacoes@basa.com.br, devidamente assinadas pelos representantes legais da empresa, dentro do prazo fixado no cronograma desta consulta. O assunto da mensagem deverá indicar a referência do chamamento e o objeto desta RFP.

As propostas técnicas e comerciais deverão ser apresentadas em arquivos separados, com a identificação da empresa e do representante responsável pelas informações. Os arquivos deverão ser apresentados preferencialmente em PDF pesquisável e acompanhados de:

- carta de apresentação assinada por representante legal, com dados de contato dos responsáveis técnico e comercial;
- carta-proposta no modelo do Anexo IV;
- planilhas de composição e memória de cálculo dos preços, em formato editável;
- evidências técnicas verificáveis referenciadas na matriz de aderência.

Os arquivos deverão ser nomeados de forma a identificar o participante, o tipo de documento e a versão.

Documentos que contenham informações comerciais protegidas deverão ser identificados pelo participante. Essa identificação não impede o acesso pelas áreas responsáveis pela análise, fiscalização, auditoria e controle, observadas as regras aplicáveis ao tratamento de informações sigilosas.

13. Disposições gerais

13.1. Confidencialidade

As informações disponibilizadas pelo Banco no âmbito desta RFP são de uso restrito, especialmente as relativas a inventário, topologia e configuração do ambiente tecnológico. Elas destinam-se exclusivamente à elaboração das propostas e não poderão ser divulgadas, reproduzidas ou utilizadas para outra finalidade sem autorização prévia e expressa. Informações mais detalhadas sobre o ambiente somente serão fornecidas conforme a classificação definida pelo Banco e, quando for o caso, mediante termo de confidencialidade. O participante deverá adotar medidas técnicas e administrativas adequadas à proteção dessas informações.

13.2. Custos de participação

Todos os custos incorridos pelo participante na elaboração e apresentação da proposta, bem como em eventuais sessões técnicas ou demonstrações, correrão por sua exclusiva conta, sem direito a ressarcimento. A proposta deverá indicar todos os componentes necessários à avaliação da solução.

13.3. Integridade e conduta

Os participantes declaram conhecer e observar a legislação brasileira de prevenção à corrupção, notadamente a Lei nº 8.429/1992 e a Lei nº 12.846/2013, bem como os princípios éticos e compromissos de conduta do Código de Conduta Ética do Banco da Amazônia. Esta consulta não cria requisitos de habilitação, que serão estabelecidos no futuro instrumento convocatório.

13.4. Alterações e cancelamento

O Banco poderá, mediante decisão motivada e comunicação pública, alterar, suspender, prorrogar ou cancelar esta RFP, no todo ou em parte, observados os princípios da transparência, isonomia e publicidade. Eventuais alterações que afetem a elaboração das propostas deverão ser comunicadas aos interessados, com avaliação da necessidade de adequação dos prazos inicialmente estabelecidos.

13.5. Canal de comunicação

Todas as comunicações relativas a esta RFP, inclusive dúvidas e sugestões, deverão ser dirigidas por escrito, em língua portuguesa, ao endereço eletrônico licitacoes@basa.com.br, com indicação da referência do chamamento e do objeto desta RFP. Não serão consideradas manifestações prestadas por canais diversos.

14. Checklist de submissão

Recomenda-se ao participante verificar, antes do envio, a presença dos itens relacionados a seguir, observado o prazo de 10 (dez) dias úteis.

Nº	Item	Referência
1	Carta de apresentação assinada por representante legal, com dados de contato do responsável técnico e do responsável comercial	Seção 12.1
2	Carta-proposta de preços elaborada conforme o modelo obrigatório	**Anexo IV**
3	Quadro de composição da solução ofertada, com fabricante, edição, *part numbers* e métricas de licenciamento	Anexo IV e proposta técnica, seção C
4	Proposta técnica estruturada conforme as seções A a R	Proposta técnica
5	Desenho da arquitetura proposta	Proposta técnica, seção B
6	Manifestação sobre cobertura e compatibilidade com o inventário: convivência com a solução de endpoint, Oracle Exadata, OpenShift e estações de trabalho	Seção 4.3 e proposta técnica, seção D
7	Matriz de aderência item a item às especificações técnicas, com evidências documentais	Anexo I e proposta técnica, seção E
8	Manifestação quanto aos indicadores, metas e critérios de medição de nível de serviço, com sugestões para os parâmetros pendentes de definição	Anexo II e proposta técnica, seção I
9	Informações de segurança, privacidade, localização de dados e certificações	Proposta técnica, seção J
10	Regras de licenciamento, realocação, contingência e ativação por ondas	Proposta técnica, seção K
11	Plano e cronograma referencial de implantação	Anexo I, item 2.9, e proposta técnica, seção L

Nº	Item	Referência
12	Manifestação quanto aos casos de teste, recursos e evidências da prova de conceito	Anexo III e proposta técnica, seção O
13	Planilha de composição e memória de cálculo dos preços, em formato editável, considerando a vigência de 60 meses com término único	Seção 8 e Anexo IV
14	Informações de qualificação e experiência	Seção 9 e proposta técnica, seção Q
15	Relação de premissas, dependências e exceções	Proposta técnica, seção R
16	Declaração de validade da proposta de 90 (noventa) dias	Anexo IV e seção 8

15. Glossário

Termo	Significado
Agente	Software instalado no sistema operacional do ativo, responsável por coletar as comunicações e aplicar as regras de proteção.
Ativo protegido	Servidor, nó da plataforma de contêineres ou estação de trabalho com agente instalado.
Servidor	Servidor físico, máquina virtual ou instância em nuvem protegida por agente.
Nó	Servidor que compõe o cluster OpenShift (de trabalho, de controle ou de infraestrutura). Não equivale ao cluster.
Rótulo	Atributo usado para classificar os ativos (ambiente, aplicação, função, localização, criticidade) e definir as regras de proteção.
Modo de visibilidade	Operação em que o agente registra as comunicações sem bloqueá-las.
Aplicação das regras (*enforcement*)	Operação em que o agente aplica efetivamente as regras de proteção no ativo.
Proteção indireta (*ring-fencing*)	Controle exercido pelos ativos com agente sobre as comunicações com ativos que não comportam agente.
Contenção	Isolamento de um ativo ou grupo comprometido, preservando o acesso das equipes de investigação.
Requisito obrigatório (O)	Requisito cujo atendimento é indispensável.
Requisito desejável (D)	Requisito que agrega valor à solução, mas não elimina o participante.

Termo	Significado
DOC, PoC, ACE, DEC	Formas de comprovação dos requisitos: documentação, prova de conceito, aceite na implantação e declaração.
TCO	Custo total de propriedade, calculado para a mesma cobertura e vigência.
SIR	Módulo ServiceNow Security Incident Response.

Belém/PA, _____ de _____ de 2026.

Gerência de Infraestrutura e Produção — GPROD
Diretoria de Tecnologia e Negócios — DITEC
Banco da Amazônia S.A.

ANEXO I — ESPECIFICAÇÕES TÉCNICAS

Solução de Microssegmentação por Agente

1. ITENS 1 A 3 — SUBSCRIÇÃO DE SOLUÇÃO DE MICROSSEGMENTAÇÃO POR AGENTE (SERVIDORES, NÓS DE CONTÊINERES E ESTAÇÕES DE TRABALHO)

Cada requisito traz, ao final, entre parênteses, o identificador, a classificação (O ou D) e a forma de comprovação, para rastreabilidade com a matriz de aderência normativa e com o Matriz de Testes da Prova de Conceito (Anexo III).

1.1. OBJETO E ESCOPO TÉCNICO

1.1.1. A solução deverá prover, pelo período de 60 (sessenta) meses, microssegmentação por software baseada em agente instalado no sistema operacional de cada ativo protegido, para os seguintes ativos do Banco da Amazônia:

a) 863 (oitocentos e sessenta e três) servidores (item 1), assim distribuídos:
- máquinas virtuais em VMware vSphere;
- instâncias na Oracle Cloud Infrastructure (OCI);
- instância no Microsoft Azure;
- *database servers bare metal* do Oracle Exadata;

b) 71 (setenta e um) nós da plataforma Red Hat OpenShift (item 2), nos clusters de produção, contingência, qualidade/homologação e gerenciamento (ACM), incluídos os nós de controle (*masters*) e de infraestrutura;

c) 4.066 (quatro mil e sessenta e seis) estações de trabalho, desktops e notebooks (item 3).

Os três itens totalizam a capacidade de referência de 5.000 (cinco mil) ativos.

1.1.2. Os quantitativos têm como base o inventário da área de infraestrutura de 30/09/2026 e constituem base provisória de planejamento. Eles serão reconciliados com a exportação formal do inventário antes da publicação do edital. O detalhamento por plataforma, versão e ambiente será fornecido aos participantes mediante termo de confidencialidade (item 13.1 da RFP). A composição de cada item é a seguinte:

a) **Item 1:** máquinas virtuais vSphere, instâncias em nuvem pública em execução e database servers do Exadata, descontadas as máquinas virtuais que são nós OpenShift, já contados no item 2.

b) **Item 2:** nós dos clusters de produção, contingência, qualidade/homologação e gerenciamento.

c) **Item 3:** calculado por diferença em relação à capacidade de referência. Depende da confirmação do parque de desktops e notebooks, das versões em uso e da localização dos equipamentos.

1.1.3. A inclusão definitiva das estações de trabalho e dos requisitos EST depende do inventário das estações e da comparação econômica e funcional com o firewall de host da solução de EDR já contratada, conforme as condicionantes do Estudo Técnico Preliminar. Essa decisão deverá anteceder a publicação do edital e fixará a aplicabilidade dos testes MC28 a MC30 do Anexo III.

1.1.4. Não recebem agente os seguintes ativos:

- os 4 servidores físicos da solução de backup contratada como serviço, de propriedade do fornecedor;
- as interfaces de gerenciamento da plataforma hiperconvergente;
- os *storage cells* do Exadata.

Esses ativos serão protegidos indiretamente, por regras aplicadas pelos agentes instalados nos ativos que se comunicam com eles (*ring-fencing*). A proteção indireta controla apenas as comunicações originadas ou destinadas a ativos com agente. Ela não protege diretamente o equipamento sem agente nem controla fluxos entre dois ativos sem agente.

1.1.5. Contêineres, bancos de dados conteinerizados (CDBs), instâncias de banco e demais objetos lógicos executados sobre os ativos licenciados constituem contexto de operação e não geram unidades adicionais de licença.

1.1.6. Não integram o núcleo deste objeto soluções autônomas de EDR, gestão de vulnerabilidades, backup, recuperação de desastres ou ZTNA. Quando existentes no ambiente, esses controles deverão interoperar com a solução por mecanismos documentados. Não serão atribuídos à solução benefícios fora desse perímetro sem demonstração da relação técnica.

1.2. CONVENÇÕES

1.2.1. **Classificação:** O = obrigatório; D = desejável, não eliminatório.

1.2.2. **Comprovação:**

- DOC: documentação técnica pública do fabricante, indicada na tabela ponto a ponto;

- PoC: demonstração na Prova de Conceito;
- ACE: teste de aceite na implantação;
- DEC: declaração do fabricante endereçada ao processo, admitida apenas para requisitos que não dependam de eficácia, desempenho ou comportamento em falha.

1.2.3. Marcas citadas nos requisitos identificam componentes do ambiente do Banco com os quais a solução deve interoperar, como EDR, vCenter, ServiceNow, OCI, Azure e Oracle Exadata. Elas não indicam preferência quanto ao fabricante da solução.

1.2.4. Os identificadores SAG-03 e NUV-03 foram suprimidos com a definição do escopo por agente. Os demais identificadores foram mantidos para preservar a rastreabilidade.

1.2.5. Os valores de referência deste Anexo poderão ser ajustados com base nas contribuições desta consulta, antes da publicação do edital, e não poderão permanecer como critérios eliminatórios indeterminados.

1.2.6. Não serão exigidos como obrigatórios:

- monitoramento de integridade de arquivos;
- consultas no estilo OSQUERY;
- *deception* ou *honeypots*;
- gravação de sessão de atacante;
- independência do firewall do sistema operacional.

1.3. ARQUITETURA E MODELOS DE IMPLANTAÇÃO

1.3.1. A solução deverá ser de microssegmentação por software baseada em agente. As regras de proteção deverão ser aplicadas pelo agente no sistema operacional de cada ativo, independentemente do hardware de rede, do hipervisor e do provedor de nuvem. A cobertura deverá abranger:

- servidores físicos;
- máquinas virtuais *on-premises*;
- instâncias em nuvem pública: obrigatoriamente OCI e Azure, e demais provedores como desejável para expansão futura;
- nós de contêiner (OpenShift/Kubernetes).

Não serão aceitas soluções cuja aplicação de regras dependa do hipervisor, de equipamentos de rede ou de orquestração remota sem agente. (ARQ-01 | O | DOC/PoC)

1.3.2. A adoção preferencial do modelo SaaS decorre das premissas do Estudo Técnico Preliminar, considerando a possibilidade de reduzir a infraestrutura local de gerenciamento, transferir ao fabricante as responsabilidades de operação, atualização e continuidade da plataforma e otimizar os custos totais da solução durante a vigência contratual.

A manutenção desse modelo como requisito obrigatório dependerá da análise das respostas desta consulta, inclusive da confirmação de alternativas tecnicamente aptas, da avaliação econômica e dos impactos sobre a competitividade.

Caso essas condições não sejam demonstradas, o Banco reavaliará a exigência antes da elaboração do instrumento convocatório definitivo

(ARQ-02 | O | DOC)

1.3.3. A aplicação das regras deverá ser local e autônoma. Quando houver perda de comunicação com a console, o agente deverá manter ativa a última regra válida, com comportamento seguro em falha configurável por grupo, sem bloquear o tráfego legítimo nem liberar indevidamente o tráfego. (ARQ-03 | O | PoC)

1.3.4. O plano de gerenciamento deverá ter alta disponibilidade, sem ponto único de falha:

- no modelo SaaS, com disponibilidade mensal mínima de 99,9%;
- no modelo *on-premises*, em cluster com *failover* automático e replicação entre os sites principal e de contingência do Banco.

(ARQ-04 | O | DOC/ACE)

1.3.5. A atualização da plataforma de gerenciamento não poderá interromper a aplicação das regras nos ativos. (ARQ-05 | O | DOC/ACE)

1.3.6. A comunicação entre agente e console deverá ser criptografada, com TLS 1.2 ou superior, e usar autenticação mútua ou mecanismo equivalente de identidade do agente. (ARQ-06 | O | DOC)

1.3.7. A solução deverá operar com múltiplos sites, ambientes e escopos administrativos em console única, com delegação por escopo, por exemplo por ambiente, aplicação ou diretoria. (ARQ-07 | O | DOC/PoC)

1.3.8. A solução deverá suportar ambientes segregados, com regra que impeça a comunicação entre produção e não produção, salvo exceção aprovada. (ARQ-08 | O | PoC)

1.3.9. O produto ofertado deverá ser final e estável, sem versões alfa, beta ou *release candidate*. O fabricante deverá declarar que não há fim de vida, de venda ou de suporte anunciado até o aceite da implantação. Em caso de descontinuidade, o componente deverá ser substituído por equivalente ou superior, sem ônus. (ARQ-09 | O | DEC)

1.3.10. A solução deverá operar de forma compatível com o proxy corporativo e com a arquitetura de firewalls do Banco, com lista documentada de portas, protocolos e FQDNs necessários. (ARQ-10 | O | DOC)

1.3.11. As regras deverão acompanhar o ativo quando ele mudar de endereço IP ou migrar entre o ambiente *on-premises* e a nuvem, sem reescrita manual (regra por rótulo). (ARQ-11 | O | PoC)

1.4. DIMENSIONAMENTO E CAPACIDADE CONTRATADA

1.4.1. A solução deverá ter capacidade para 863 servidores, 71 nós OpenShift e 4.066 estações, na base provisória de 5.000 ativos, com arquitetura e limites técnicos documentados. Reserva adicional de crescimento somente será considerada com memória de cálculo aprovada, sem presumir margem já contratada para os 60 meses. (DES-01 | O | DOC/DEC)

1.4.2. A solução deverá processar fluxos na taxa derivada da volumetria do ambiente, conforme memória de cálculo apresentada pelo proponente. (DES-02 | O | DOC)

1.4.3. A propagação de alteração de regra aos agentes afetados deverá ocorrer em até 5 (cinco) minutos. (DES-03 | O | PoC)

1.4.4. A degradação da latência p95 das transações de teste deverá ser de, no máximo, 5% em relação à linha de base, sob carga equivalente e com a regra aplicada, conforme o caso MC06 do Anexo III. (DES-04 | O | PoC)

1.5. GERENCIAMENTO, GOVERNANÇA E CONTROLE ADMINISTRATIVO

1.5.1. A console deverá ser acessada via web por HTTPS e ser compatível com as versões correntes dos navegadores Chrome, Edge e Firefox. (GER-01 | O | DOC)

1.5.2. A autenticação deverá ser feita por SSO (SAML 2.0 ou OpenID Connect) com o provedor de identidade corporativo (Microsoft Entra ID e/ou AD FS) e MFA. Contas locais serão admitidas apenas para contingência (*break glass*), com registro de uso. (GER-02 | O | PoC)

1.5.3. A solução deverá oferecer controle de acesso granular por papel e escopo (RBAC), com, no mínimo, os seguintes perfis:

- administrador global;
- administrador de regras por escopo;
- operador;
- responsável pela aplicação, para propor e aprovar regras no seu escopo;
- auditor somente leitura;
- analista do SOC, para visualização e contenção.

(GER-03 | O | PoC)

1.5.4. A solução deverá admitir número ilimitado de usuários administrativos, sem custo adicional. (GER-04 | O | DEC)

1.5.5. O acesso administrativo deverá ser compatível com a intermediação pela solução de gestão de acessos privilegiados (PAM), com sessões gravadas. (GER-05 | O | ACE)

1.5.6. A solução deverá manter trilha de auditoria de toda ação administrativa, exportável para o SIEM:

- ações abrangidas: autenticação, alteração de regras, rótulos e exceções, contenções, consultas e exportações;
- dados registrados: data e hora, usuário, IP de origem, objeto, valor anterior e valor posterior.

(GER-06 | O | PoC)

1.5.7. A solução deverá oferecer painéis configuráveis de cobertura, saúde dos agentes, estado das regras (simulação ou aplicação), fluxos bloqueados e exceções. (GER-07 | O | DOC/PoC)

1.5.8. A solução deverá monitorar a saúde de todos os componentes (agentes, conectores e coletores), com emissão de alertas. (GER-08 | O | PoC)

1.5.9. A atualização dos agentes deverá ser feita a partir da console, em lotes e por grupo, com janela agendada e possibilidade de reversão, sem acesso manual ao equipamento. (GER-09 | O | PoC)

1.6. AGENTES

1.6.1. Deverá haver agentes para as versões de Windows Server (de 2003 até a versão atual) e Linux a partir da versão 6 (RHEL, Oracle Linux e demais distribuições) constantes do inventário do Banco, e para as versões de Windows das estações de trabalho de Windows 7 até a versão atual. (AGT-01 | O | DOC)

1.6.2. A instalação deverá ser silenciosa e em massa (MSI, RPM/DEB, scripts, SCCM, Ansible ou equivalente), com parâmetros de rótulo e de ativação. (AGT-02 | O | DOC/ACE)

1.6.3. A instalação e a atualização do agente não deverão exigir reinicialização do sistema operacional, ressalvadas as exceções documentadas por sistema operacional. (AGT-03 | O | PoC)

1.6.4. O consumo médio do agente deverá ser inferior a 5% de CPU e a 10% de memória, em carga representativa e medido com metodologia definida pelo Banco. O consumo deverá respeitar limites configuráveis pelo Banco. (AGT-04 | O | PoC/ACE)

1.6.5. O agente deverá conviver comprovadamente, sem conflito de filtros de rede (WFP, iptables/nftables, eBPF), com:

- o agente da solução de EDR corporativa, inclusive o módulo de firewall de host, se ativo;
- DLP e CASB;
- o scanner de vulnerabilidades;
- o SCCM;
- o cliente de VPN/ZTNA.

(AGT-05 | O | PoC)

1.6.6. O agente deverá iniciar em modo somente visibilidade, sem bloqueio, como padrão, com transição controlada para o modo de aplicação das regras por ativo ou por grupo. (AGT-06 | O | PoC)

1.6.7. O agente deverá ser protegido contra adulteração. Desativação, desinstalação ou alteração local das regras deverão ser impedidas sem credencial autorizada, com alerta à console. (AGT-07 | O | PoC)

1.6.8. O agente deverá identificar o processo, o serviço e, quando aplicável, o usuário associado a cada fluxo. (AGT-08 | O | PoC)

1.6.9. A retirada do agente deverá remover integralmente as regras aplicadas, inclusive após o término do contrato, sem:

- deixar o ativo isolado;
- deixar regras residuais;
- interromper as aplicações.

(AGT-09 | O | PoC)

1.6.10. O agente deverá operar em máquinas virtuais clonadas ou geradas a partir de *templates* (VDI, autoescalonamento) sem duplicidade de identidade. (AGT-10 | O | DOC)

1.6.11. Desejável: disponibilidade de agentes para sistemas UNIX legados. (AGT-11 | D | DOC)

1.6.12. O agente deverá ser compatível com os 11 *database servers* do Oracle Exadata, que usam Oracle Linux com kernel UEK, na versão do Exadata System Software em uso.

a) **Comprovação e limites:** a compatibilidade deverá ser comprovada por documentação pública do fabricante da solução, sem instalação nos *storage cells* e sem prejuízo ao suporte da Oracle. A ausência de compatibilidade documentada implica o não atendimento.

b) **Redes do cluster:** o agente não poderá filtrar nem degradar o *interconnect* privado do RAC nem a rede de armazenamento (RoCE/InfiniBand). Deverá permitir excluir essas interfaces da aplicação de regras.

c) **Rótulos e regras:** o agente deverá suportar rótulos por cluster RAC (produção, qualidade e contingência) e regras por serviço ou *listener* dos CDBs, preservando a replicação entre produção e contingência.

d) **Recusa da Oracle:** somente se a Oracle não admitir a instalação, os *database servers* serão tratados como ativos sem agente (subseção 1.7). Nessa hipótese, o item 1 será reduzido em 11 unidades.

(AGT-12 | O | DOC/PoC)

1.7. ATIVOS SEM AGENTE

1.7.1. A solução deverá permitir cadastrar, rotular e controlar, por meio das regras aplicadas nos ativos protegidos que se comunicam com eles, os ativos que não suportam ou não admitem agente. Incluem-se:

- *appliances*, bancos de dados gerenciados, dispositivos IoT, impressoras e sistemas legados;
- servidores de terceiros, como os 4 servidores da solução de backup contratada como serviço;
- *database servers* e *storage cells* do Oracle Exadata, quando o agente não for admitido pela Oracle;
- interfaces de gerenciamento da plataforma hiperconvergente.

(SAG-01 | O | PoC)

1.7.2. A solução deverá descobrir ativos sem agente a partir dos fluxos observados pelos agentes. (SAG-02 | O | PoC)

1.8. CONTÊINERES

1.8.1. A solução deverá oferecer visibilidade e aplicação de regras em OpenShift 4x e em Kubernetes *upstream*, com rótulos derivados de *namespace*, *deployment*, *label* e *service*. (CNT-01 | O | PoC)

1.8.2. O licenciamento deverá ser por nó do cluster (de trabalho, de controle e de infraestrutura), cobrindo todos os *pods* e contêineres do nó, sem cobrança por contêiner ou por *namespace*.

a) A densidade de contêineres por nó não poderá alterar o preço. Para referência, o Banco possui 71 nós e cerca de 9.990 contêineres.

b) Estão incluídas a proteção dos nós de controle (API e etcd) e a do cluster de gerenciamento (ACM).

(CNT-02 | O | DEC)

1.8.3. A solução deverá ser compatível com a interface de rede de contêineres (CNI) em uso e com as *NetworkPolicies* existentes, sem conflito. (CNT-03 | O | PoC)

1.8.4. A solução deverá permitir regras entre cargas de trabalho em contêiner e cargas de trabalho tradicionais (máquina virtual ou *bare metal*) na mesma console. (CNT-04 | O | PoC)

1.9. ESTAÇÕES DE TRABALHO — DESKTOPS E NOTEBOOKS

1.9.1. Deverá haver agente para as versões de sistema operacional das estações constantes do inventário do Banco. O agente deverá ser gerenciado na mesma console e com a mesma taxonomia de rótulos dos servidores. (EST-01 | O | DOC/PoC)

1.9.2. A solução deverá bloquear, por padrão, as comunicações entre estações por protocolos de compartilhamento e de administração remota (SMB, RDP, WinRM e equivalentes), com exceções aprovadas e registradas. (EST-02 | O | PoC)

1.9.3. As regras deverão ser aplicadas também quando a estação estiver fora da rede corporativa, com perfis por localização e sincronização automática ao retornar. (EST-03 | O | PoC)

1.9.4. A instalação e a atualização deverão ser silenciosas, pela ferramenta corporativa de distribuição de software, sem interação do usuário e sem mensagens indevidas na tela. (EST-04 | O | PoC)

1.9.5. O consumo médio de CPU e memória do agente nas estações deverá respeitar limites definidos pelo Banco. (EST-05 | O | PoC)

1.9.6. O agente das estações deverá conviver comprovadamente com EDR, DLP, cliente de acesso remoto/ZTNA e VPN. (EST-06 | O | PoC)

1.9.7. A solução deverá permitir o isolamento de estação pela console e por API integrada ao ServiceNow SIR, preservando o canal de investigação. (EST-07 | O | PoC)

1.9.8. A solução deverá permitir regras de acesso das estações aos servidores por grupo do AD e por usuário. (EST-08 | O | PoC)

1.9.9. Desejável: suporte a ambientes de desktop virtual (VDI), se existentes no Banco. (EST-09 | D | DOC)

1.10. NUVEM

1.10.1. A solução deverá dispor de conectores para OCI e Azure que importem o inventário e as *tags* das instâncias para rotulagem automática. (NUV-01 | O | DOC/PoC)

1.10.2. A solução deverá proteger instâncias IaaS por agente, independentemente do provedor. (NUV-02 | O | DOC)

1.10.3. Desejável: conectores para outros provedores (AWS, GCP), para expansão futura sem troca de solução. (NUV-04 | D | DOC)

1.11. VISIBILIDADE E MAPA DE DEPENDÊNCIAS

1.11.1. A solução deverá apresentar mapa gráfico de dependências de aplicações, em tempo quase real e com histórico, com agregação por rótulo, aplicação e ambiente. (VIS-01 | O | PoC)

1.11.2. A solução deverá oferecer visibilidade leste-oeste e norte-sul dos ativos protegidos, com origem, destino, porta, protocolo, processo e contagem de conexões. (VIS-02 | O | PoC)

1.11.3. Os dados de fluxo deverão ficar disponíveis para consulta na console por, no mínimo, 90 dias, com exportação para o SIEM ou repositório corporativo, conforme a política de retenção do Banco. (VIS-03 | O | DOC)

1.11.4. A solução deverá permitir filtros e buscas por rótulo, aplicação, processo, porta, IP ou FQDN, período e decisão da regra (permitido, bloqueado ou potencialmente bloqueado). (VIS-04 | O | PoC)

1.11.5. A solução deverá apresentar a visão de tráfego potencialmente bloqueado em modo de simulação. (VIS-05 | O | PoC)

1.11.6. A solução deverá exportar mapas e fluxos em formatos abertos (CSV, JSON). (VIS-06 | O | DOC)

1.11.7. A solução deverá exibir comunicações estabelecidas, bloqueadas e com falha (*timeout*), com origem, usuário e processo, e com destino e processo. (VIS-07 | O | PoC)

1.12. ROTULAGEM E INVENTÁRIO

1.12.1. A solução deverá suportar rótulos multidimensionais, no mínimo:

- ambiente;
- aplicação;
- função ou camada;
- localização ou site;
- criticidade;
- marcador regulatório (ex.: Pix, RSFN, PCI).

(ROT-01 | O | PoC)

1.12.2. A solução deverá permitir rotulagem automática por regras (nome, sistema operacional, sub-rede, grupo do AD, *tag* de nuvem, atributo da CMDB) e importação e exportação em massa (CSV/XLS/API). (ROT-02 | O | PoC)

1.12.3. Desejável: sincronização com a CMDB do ServiceNow, com leitura de itens de configuração e relacionamentos e, se aplicável, gravação de rótulos. (ROT-03 | D | DOC)

1.13. REGRAS DE PROTEÇÃO E APLICAÇÃO

1.13.1. As regras deverão ser baseadas em rótulos, com modelo de lista de permissão (bloqueio por padrão em cada escopo). (POL-01 | O | PoC)

1.13.2. A solução deverá permitir regras por IP, sub-rede, faixa, FQDN, porta ou intervalo de portas, protocolo e processo, inclusive portas dinâmicas associadas a processo. (POL-02 | O | PoC)

1.13.3. A solução deverá permitir regras baseadas na identidade do usuário ou do grupo do AD para sessões interativas, inclusive em servidores multiusuário (VDI, Terminal Services, Citrix). Exemplo: RDP ou SSH somente a partir de grupos administrativos e de servidores de salto ou PAM. (POL-03 | O | PoC)

1.13.4. A solução deverá recomendar regras automaticamente a partir dos fluxos observados, com revisão humana. (POL-04 | O | PoC)

1.13.5. A solução deverá permitir simulação e análise de impacto antes da aplicação, com identificação dos fluxos que seriam bloqueados. (POL-05 | O | PoC)

1.13.6. A solução deverá permitir aplicação gradual por ativo, grupo ou aplicação e reversão imediata para o modo de visibilidade. (POL-06 | O | PoC)

1.13.7. A solução deverá oferecer versionamento, histórico, comparação entre versões e reversão de regras sem restauração de backup. (POL-07 | O | PoC)

1.13.8. A solução deverá oferecer fluxo de aprovação de mudanças de regras, nativo ou por integração com a ferramenta de gestão de serviços de TI. No fluxo, o responsável pela aplicação propõe a mudança e a área de segurança a aprova. (POL-08 | O | PoC)

1.13.9. A solução deverá permitir exceções temporárias com expiração automática, justificativa e responsável (acesso *just-in-time*). (POL-09 | O | PoC)

1.13.10. A solução deverá oferecer modelos de regra para serviços de infraestrutura: AD, DNS, DHCP, NTP, bancos de dados, backup, monitoramento e atualização. (POL-10 | O | DOC)

1.13.11. A solução deverá permitir regras de entrada e de saída, inclusive saída para a internet por FQDN. Exemplo: restringir a máquina virtual do projeto de IA aos serviços de IA autorizados. (POL-11 | O | PoC)

1.13.12. Desejável: detecção de conflitos, redundâncias e regras não utilizadas. (POL-12 | D | DOC)

1.13.13. A solução deverá conviver com os firewalls de rede do Banco, sem exigir sua substituição. (POL-13 | O | DOC)

1.13.14. A solução deverá permitir regras que combinem origem (ativo, usuário ou grupo do AD e processo) e destino (serviço ou FQDN). Exemplo: somente o processo X, executado por usuários do grupo Y, acessa o serviço Z. (POL-14 | O | PoC)

1.14. RESPOSTA A INCIDENTES E CONTENÇÃO

1.14.1. A solução deverá permitir o isolamento (quarentena) de ativo ou grupo pela console e por API, com propagação em até 60 segundos. O isolamento deverá preservar o canal de investigação: console do EDR, coleta forense e PAM. (RES-01 | O | PoC)

1.14.2. A contenção deverá poder ser acionada pela ferramenta de orquestração de resposta (SOAR) ou pelo ServiceNow SIR, via API documentada. (RES-02 | O | PoC)

1.14.3. A solução deverá emitir alertas de violação de regra, tentativas de conexão bloqueadas e desvios de comportamento, com severidade configurável. (RES-03 | O | PoC)

1.14.4. Desejável: ingestão de contexto de risco (vulnerabilidades da ferramenta corporativa de gestão de vulnerabilidades, detecções do EDR) para priorização ou aplicação automática de regra restritiva. (RES-04 | D | DOC)

1.15. INTEGRAÇÕES E API

1.15.1. A solução deverá dispor de API REST documentada publicamente, com:

- autenticação por *token* ou chave com escopo;
- cobertura de inventário, rótulos, regras, fluxos, contenção e auditoria;

- operações em lote.

(INT-01 | O | DOC/PoC)

1.15.2. A solução deverá enviar eventos, fluxos e registros de auditoria ao SIEM do Banco por Syslog (CEF/LEEF/JSON) e/ou API, com fila e reenvio em caso de falha. (INT-02 | O | PoC)

1.15.3. A solução deverá se integrar com AD/LDAPS e Entra ID para obtenção de grupos e usuários. (INT-03 | O | PoC)

1.15.4. Desejável: integração com ferramentas de automação e infraestrutura como código (Ansible, Terraform ou equivalente) e com *pipelines* de CI/CD, para rotular e aplicar regras a novos ativos. (INT-04 | D | DOC)

1.15.5. Desejável: integração com a ferramenta de gestão de serviços de TI (ServiceNow) para abertura, aprovação e rastreamento de mudanças e incidentes. (INT-05 | D | DOC)

1.15.6. A solução deverá se integrar com o VMware vCenter (na versão em uso no Banco) para inventário e rotulagem por *tags* e atributos de máquina virtual. Deverá também conviver, sem conflito de filtragem, com o firewall distribuído da plataforma de virtualização, caso venha a ser ativado. (INT-06 | O | DOC/PoC)

1.16. LOGS, AUDITORIA E GOVERNANÇA DE DADOS

1.16.1. Todos os componentes deverão sincronizar o tempo com a fonte corporativa (NTP). (LOG-01 | O | ACE)

1.16.2. Os registros deverão ser protegidos contra alteração e exclusão indevidas. (LOG-02 | O | DOC)

1.16.3. A retenção deverá ser definida por classe de registro (auditoria administrativa, fluxos e alertas), na própria solução ou no SIEM, conforme a política do Banco e a Resolução CMN nº 4.893/2021, sem retenção indiscriminada. (LOG-03 | O | DOC)

1.16.4. No modelo SaaS, a contratada deverá:

- informar a localização de processamento e armazenamento, os suboperadores e eventual transferência internacional de dados;
- garantir criptografia em trânsito e em repouso;
- firmar acordo de tratamento de dados nos termos da LGPD;
- assegurar o direito de auditoria do Banco e o acesso do Banco Central, nos termos da Resolução CMN nº 4.893/2021.

(LOG-04 | O | DOC/DEC)

1.16.5. Ao término do contrato, a solução deverá permitir a exportação integral de dados, rótulos, regras e registros em formato documentado, seguida da eliminação segura, com evidência. (LOG-05 | O | DEC)

1.17. SEGURANÇA DA PRÓPRIA SOLUÇÃO, PRIVACIDADE E CONFORMIDADE

1.17.1. O fabricante deverá adotar processo de desenvolvimento seguro e manter canal público de divulgação de vulnerabilidades, com boletins e prazos de correção. (SEG-01 | O | DOC)

1.17.2. No modelo SaaS, deverá haver evidência de controles independentes: certificação ISO/IEC 27001 e/ou relatório SOC 2 Tipo II vigentes. (SEG-02 | O | DOC)

1.17.3. Os componentes *on-premises* e os agentes deverão ter *hardening* documentado. (SEG-03 | O | DOC)

1.17.4. Desejável: suporte a IPv6. (SEG-04 | D | DOC)

1.17.5. A solução deverá contribuir para o atendimento à LGPD, às normas regulatórias aplicáveis e às políticas internas do Banco. Ela não será considerada suficiente, isoladamente, para assegurar a conformidade institucional.

1.18. RELATÓRIOS

1.18.1. A solução deverá gerar relatórios de cobertura, estado de aplicação das regras, exceções, violações e mudanças, agendáveis e exportáveis em PDF e CSV. (REL-01 | O | PoC)

1.18.2. A solução deverá gerar relatório de evidência de segregação entre ambientes e zonas, utilizável em auditorias. Exemplo: validação de segmentação exigida pelo PCI DSS, quando aplicável. (REL-02 | O | DOC/PoC)

1.18.3. Desejável: métricas de uso e de operação, como regras por estado, tempo entre simulação e aplicação e exceções vencidas. (REL-03 | D | DOC)

1.19. LICENCIAMENTO, CICLO DE VIDA E ATUALIZAÇÕES

1.19.1. O licenciamento deverá ser segregado em 863 servidores, 71 nós OpenShift (incluídos os nós de controle e de infraestrutura) e 4.066 estações.

a) **Contagem:** os nós não poderão ser contados novamente como máquinas virtuais. Contêineres, CDBs e instâncias de banco não poderão gerar licenças adicionais.

b) **Composição do preço:** todas as funções obrigatórias e os componentes necessários deverão constar do preço, com equivalência por item e *part numbers*.

(LIC-01 | O | DEC)

1.19.2. As licenças deverão poder ser realocadas entre ativos sem custo, em casos de desativação, substituição ou migração para a nuvem. (LIC-02 | O | DEC)

1.19.3. A proposta deverá tratar explicitamente as máquinas virtuais OCI paradas e as réplicas de contingência desligadas:

a) **Ativos inativos:** não deverão ser cobrados como ativos protegidos simultâneos enquanto estiverem inativos, conforme o modelo validado na consulta ao mercado.

b) **Ativação e excedente:** a proposta deverá registrar a capacidade para ativação simultânea dos ambientes de produção e de contingência, a realocação e eventual excedente.

c) **Limite de licenças:** não se presume disponibilidade ilimitada de licenças.

(LIC-03 | O | DEC)

1.19.4. As atualizações de versão deverão ser garantidas durante toda a vigência. (LIC-04 | O | DEC)

1.19.5. Todos os componentes deverão estar em versões suportadas, com ciclo de vida compatível com a vigência contratual. Atualizações relevantes deverão ser planejadas, testadas, registradas e passíveis de reversão. Caso componente essencial seja descontinuado durante a vigência, deverá ser substituído por equivalente ou superior, sem redução funcional nem custo adicional.

1.20. PORTABILIDADE, TRANSIÇÃO E SAÍDA

1.20.1. A solução deverá permitir a exportação de rótulos, regras, exceções, configurações, inventário, mapas de comunicação, registros, relatórios e evidências, em formatos documentados e reutilizáveis (VIS-06, LOG-05).

1.20.2. A contratada deverá fornecer a documentação dos esquemas e formatos necessários à interpretação dos dados exportados.

1.20.3. A retirada dos agentes deverá observar o requisito AGT-09, sem deixar ativos isolados ou com regras residuais.

1.21. TESTES, PROVA DE CONCEITO E CRITÉRIOS DE ACEITE

1.21.1. Os requisitos com comprovação PoC serão verificados conforme o Matriz de Testes da Prova de Conceito (Anexo III). Os requisitos com comprovação ACE serão verificados nos testes de aceite da implantação.

1.21.2. Na Prova de Conceito, a documentação técnica e a licença de avaliação deverão demonstrar a mesma edição e os mesmos módulos ofertados.

1.21.3. A amostra funcional da Prova de Conceito não comprova a escala de 5.000 ativos. O licitante deverá apresentar memória de capacidade considerando 863 servidores, 71 nós, as estações confirmadas e a volumetria de fluxos.

1.21.4. Os limites da proteção indireta dos ativos sem agente deverão ser registrados no plano de cobertura e verificados no teste MC12 do Anexo III (e no MC24, na hipótese do item 2.6 daquele Anexo): servidores de backup de terceiro, *storage cells* e interfaces de gerenciamento.

1.21.5. O aceite não se limitará à entrega de licenças ou componentes. Ele estará condicionado à comprovação, no ambiente do Banco, de:

- proteção;
- desempenho;
- interoperabilidade;
- rastreabilidade;
- resiliência;
- operacionalidade da solução.

Na implantação, o inventário, os agentes ativos e as licenças faturadas serão reconciliados por identificador único.

2. ITENS 4 E 5 — SERVIÇOS DE PLANEJAMENTO, IMPLANTAÇÃO, INTEGRAÇÃO, OPERAÇÃO ASSISTIDA E TRANSIÇÃO DE SAÍDA

2.1. Características Gerais

2.1.1. A contratada deverá executar todos os serviços necessários à entrada em produção da solução de microssegmentação: planejamento, projeto executivo, instalação, configuração, integração, testes, homologação, ajuste fino e ativação. Os serviços abrangem os agentes, a console e os conectores que componham a arquitetura ofertada.

2.1.2. Os serviços deverão contemplar os ambientes VMware vSphere, OCI, Azure, OpenShift, Oracle Exadata e as estações de trabalho. Deverão incluir a integração com:

- serviços de diretório;
- SIEM;
- ServiceNow SIR e ferramenta de gestão de serviços de TI;
- vCenter;
- ferramentas de distribuição de software;
- demais componentes definidos no Projeto Executivo.

2.1.3. A implantação será integral, executada por ondas, com documentação e aceites.

- O item 4 será pago por marcos aceitos.
- O item 5 corresponde a 90 (noventa) dias de operação assistida após o último marco de implantação, com relatório final aceito.

2.1.4. A execução deverá preservar a disponibilidade, a integridade e o desempenho das aplicações. Todas as mudanças com potencial impacto ao ambiente de produção deverão prever procedimentos de contingência e reversão para o modo de visibilidade.

2.2. Planejamento e Projeto Executivo

2.2.1. Antes da implantação, a contratada deverá realizar levantamento técnico detalhado do ambiente, contemplando:

a) ativos, sistemas operacionais e versões;

b) redes, nuvens e clusters;

c) aplicações e respectivos responsáveis;

d) ferramentas de distribuição de software e automação;

e) integrações com serviços de diretório, SIEM, ServiceNow SIR e vCenter;

f) requisitos de alta disponibilidade e contingência;

g) dependências e restrições técnicas, inclusive do Oracle Exadata e do OpenShift;

h) requisitos de segurança e controle de acesso; e

i) critérios de aceite e homologação.

2.2.2. A contratada deverá elaborar Projeto Executivo (Plano de Implantação) contendo, no mínimo:

a) mapeamento do ambiente: ativos, sistemas operacionais, redes, nuvens e clusters;

b) estratégia de instalação por tipo de ativo (SCCM, Ansible, imagem base, *DaemonSet*);

c) taxonomia de rótulos e regras de rotulagem automática;

d) ondas e critérios de priorização, começando pelos ativos críticos;

e) integrações necessárias;

f) modelo de governança das regras, com:

- matriz de responsabilidades (RACI) entre segurança, infraestrutura e responsáveis pelas aplicações;
- fluxo de aprovação e de exceções;

g) critérios objetivos para a passagem do modo de visibilidade para o de aplicação em cada aplicação. Exemplo: 30 dias de observação sem fluxo não explicado;

h) cronograma de execução;

i) plano de comunicação;

j) riscos;

k) plano de reversão;

l) plano de testes por onda; e

m) recursos exigidos do Banco.

2.3. Instalação e Configuração

2.3.1. A contratada deverá instalar, provisionar, ativar e configurar todos os componentes necessários à operação integral da solução.

2.3.2. Deverão ser executados, no mínimo:

a) instalação e configuração da console e dos conectores;

b) implantação dos agentes, em conjunto com a equipe do Banco;

c) rotulagem dos ativos;

d) mapeamento de dependências, com validação pelos responsáveis pelas aplicações;

e) construção, simulação, aprovação e aplicação de regras, por ondas;

f) integrações com os componentes corporativos;

g) configuração de alertas, painéis e relatórios;

h) configuração de controles administrativos, RBAC, SSO e MFA; e

i) elaboração de documentação final do ambiente (*As Built*) editável e de procedimentos de operação, contenção e reversão.

2.4. Migração e Integração

2.4.1. A implantação deverá ser gradual e controlada, reduzindo riscos de indisponibilidade e permitindo reversão quando necessário.

2.4.2. Deverão ser observados os seguintes cuidados específicos:

a) **Oracle Exadata:** instalação em janela acordada com a área de banco de dados, com exclusão das interfaces de *interconnect* do RAC e de armazenamento e com liberação explícita da replicação entre produção e contingência;

b) **OpenShift:** proteção prioritária dos nós de controle e do cluster de gerenciamento (ACM);

c) **servidores de backup do fornecedor:** isolamento por proteção indireta a partir dos ativos com agente, liberando apenas os fluxos de backup autorizados.

2.4.3. A contratada deverá assegurar que eventos, alertas e registros relevantes sejam encaminhados ao SIEM com informações suficientes para correlação e rastreabilidade.

2.5. Testes e Homologação

2.5.1. A homologação seguirá roteiro por onda, com casos de teste, critérios objetivos, evidências, responsáveis e procedimento de reversão.

2.5.2. Os testes deverão contemplar, no mínimo:

a) funcionamento das aplicações sem regressão;

b) consumo de recursos do agente (AGT-04);

c) comportamento dos agentes sem comunicação com a console (ARQ-03);

d) contenção e liberação de ativos (RES-01);

e) integridade dos registros no SIEM (INT-02);

f) *failover* da console *on-premises*, se aplicável (ARQ-04); e

g) remoção limpa do agente (AGT-09).

2.5.3. A homologação não se confunde com a Prova de Conceito nem substitui testes de intrusão independentes.

2.6. Ajuste Fino e Entrada em Produção

2.6.1. Antes da aplicação de bloqueios, a contratada deverá:

a) mapear as dependências e simular as regras;

b) validar os fluxos com os responsáveis pelas aplicações;

c) obter a aprovação da mudança;

d) prever a reversão para o modo de visibilidade; e

e) executar os testes previstos para a onda.

2.6.2. Mudanças em produção ocorrerão apenas em janelas aprovadas pelo Comitê de Mudanças, com plano de reversão.

2.7. Operação Assistida e Estabilização

2.7.1. Por 90 (noventa) dias após o último marco de implantação, a contratada deverá prestar operação assistida, com especialista que tenha participado da implantação, compreendendo:

a) acompanhamento de alertas e fluxos bloqueados;

b) ajuste fino das regras;

c) tratamento de exceções;

d) atualização de agentes;

e) simulação de incidentes, com contenção via ServiceNow SIR; e

f) transferência de conhecimento na prática (*on the job*).

2.7.2. O término da operação assistida será formalizado com relatório final e procedimentos de operação customizados, mediante aceite do Banco.

2.8. Transição de Saída

2.8.1. Até 90 (noventa) dias antes do término do contrato, a contratada deverá apresentar plano de saída, contemplando:

a) exportação de rótulos, regras, exceções, inventário, mapas e registros;

b) convivência temporária com a solução sucessora;

c) remoção coordenada dos agentes, sem indisponibilidade;

d) revogação de contas, credenciais e acessos concedidos à contratada;

e) eliminação segura dos dados mantidos pela contratada, com evidência; e

f) cessão ao Banco dos scripts e integrações desenvolvidos e remunerados.

2.9. Marcos e Prazos de Referência

Marco	Entregável	Prazo de referência
M0 — Início	Reunião inicial; designação de preposto, gerente de projeto, especialistas certificados e ponto focal técnico do fabricante	Até 10 dias da assinatura
M1 — Plano de Implantação	Plano versão 1 e plano definitivo aceito (mapeamento, taxonomia de rótulos, ondas, integrações, RACI, riscos e reversão)	Versão 1 em 30 dias; definitivo em 45 dias
M2 — Ativação	Licenças ativadas e console provisionada, com relatório de ativação	Até 15 dias após M1
M3 — Onda 0	Agentes e integrações no ambiente de homologação e em grupo piloto de estações; testes de convivência (EDR, Exadata, OpenShift, estações)	Até 30 dias após M2

Marco	Entregável	Prazo de referência
M4 — Visibilidade total	Agentes em, no mínimo, 98% dos servidores e nós, em modo de visibilidade; estações conforme o piloto e as ondas; mapas por aplicação	Até 90 dias após M2
M5 — Ativos críticos	Regras simuladas, aprovadas e aplicadas nos ativos críticos	Até 180 dias após M2
M6 — Aplicação ampliada	Separação entre produção e não produção em todo o escopo; regras por aplicação nas ondas seguintes; bloqueio das comunicações entre estações por ondas de unidades; *As Built* final	Até 270 dias após M2
M7 — Operação assistida	90 dias de acompanhamento; procedimentos de operação e relatório final	Após M6

2.9.1. Cada marco será aceito mediante termo, com o seguinte rito:

- a primeira versão do entregável será apresentada 15 dias antes do prazo;
- o Banco fará a análise em 5 dias úteis;
- a contratada fará as correções em 5 dias úteis.

3. ITEM 6 — TREINAMENTO OPERACIONAL E TRANSFERÊNCIA DE CONHECIMENTO

3.1. Características Gerais

3.1.1. A contratada deverá prestar treinamento oficial do fabricante ou de parceiro autorizado, na trilha técnica de administração, a 12 (doze) participantes indicados pelo Banco. O treinamento deverá proporcionar autonomia para administração, operação, monitoramento e fiscalização da solução.

3.1.2. O treinamento será realizado em uma ou duas turmas, antes da Onda 0. Terá caráter predominantemente técnico e prático e abrangerá a arquitetura e os componentes efetivamente fornecidos.

3.1.3. Está incluído, sem custo adicional, *workshop* de 4 (quatro) horas para os responsáveis pelas aplicações.

3.2. Conteúdo Mínimo

3.2.1. O treinamento deverá contemplar, no mínimo, conforme a trilha oficial da solução e os procedimentos customizados:

a) arquitetura da solução;

b) administração da plataforma, usuários, RBAC e MFA;

c) instalação e gestão dos agentes;

d) rotulagem e inventário;

e) mapeamento de dependências;

f) criação, simulação, aplicação e reversão de regras;

g) tratamento de exceções;

h) contenção e isolamento de ativos;

i) análise de eventos, alertas e registros;

j) integrações com SIEM, ServiceNow SIR e serviços de diretório;

k) relatórios;

l) alta disponibilidade e procedimentos de contingência; e

m) atualização da solução e diagnóstico de problemas.

3.3. Metodologia

3.3.1. O treinamento será presencial em Belém/PA ou remoto ao vivo, em português ou com tradução, com laboratórios práticos.

3.3.2. A carga horária mínima será definida a partir da consulta ao mercado e fixada antes do edital.

3.3.3. Os participantes deverão executar atividades práticas de administração, criação e ajuste de regras, análise de eventos e diagnóstico de falhas.

3.4. Instrutores

3.4.1. Os instrutores deverão ser do fabricante ou de parceiro autorizado, com conhecimento comprovado nos produtos efetivamente implantados. A trilha e a carga horária deverão ser identificadas na proposta.

3.5. Entregáveis

3.5.1. Ao término do treinamento, a contratada deverá fornecer:

a) material didático oficial;

b) conteúdo programático;

c) lista de participantes e registro das atividades; e

d) certificados com carga horária para as 12 vagas.

3.5.2. A conclusão do treinamento deverá ser formalmente aceita pelo Banco.

3.6. Transferência Contínua de Conhecimento

3.6.1. A transferência de conhecimento não se limitará ao treinamento formal. Ela deverá ocorrer também durante a implantação, a operação assistida, o suporte, o tratamento de incidentes, as atualizações relevantes e a transição de saída.

3.6.2. Durante os 90 dias de operação assistida, a transferência ocorrerá na prática (*on the job*), com procedimentos de operação customizados e procedimentos de contenção e reversão.

4. ITEM 7 — SUPORTE TÉCNICO ESPECIALIZADO 24X7 E SUSTENTAÇÃO

4.1. Características Gerais

4.1.1. A contratada deverá prestar, durante os 60 (sessenta) meses da contratação, serviço continuado de suporte técnico, sustentação, manutenção, atualização e apoio ao tratamento de incidentes. O serviço abrange todos os componentes da solução: agentes, console, conectores e integrações.

4.1.2. O suporte será prestado sob responsabilidade de ponta a ponta da contratada, inclusive quanto aos serviços prestados pelo fabricante ou por parceiros.

4.1.3. O suporte de nível 3 do fabricante está incluído na subscrição, sem limite de acionamentos. Esse suporte não poderá ser cobrado novamente como serviço do integrador.

4.2. Cobertura do Suporte

4.2.1. O serviço deverá contemplar, no mínimo:

a) diagnóstico e solução de falhas da plataforma, dos agentes e das integrações;

b) análise de registros e eventos;

c) correção de erros e defeitos;

d) tratamento de incidentes, inclusive bloqueios indevidos;

e) apoio à revisão e ao ajuste de regras e exceções;

f) correções de segurança;

g) suporte às integrações;

h) suporte à alta disponibilidade e aos procedimentos de contingência;

i) apoio à reversão de regras;

j) análise de desempenho e capacidade;

k) identificação de causa raiz; e

l) recomendações técnicas relacionadas à estabilidade e à segurança da solução.

4.2.2. A operação continuada integral pela contratada permanece sujeita à decisão da área demandante e, se adotada, será consolidada antes do edital.

4.3. Atendimento 24x7

4.3.1. As severidades 1 e 2 terão atendimento 24x7x365, em português. As severidades 3 e 4 terão atendimento em horário comercial, nos tempos do Anexo II.

4.3.2. O atendimento será prestado por portal, e-mail e telefone acessível no Brasil, com número único de chamado e histórico consultável.

4.3.3. Deverá ser permitida a abertura de número ilimitado de chamados relacionados ao escopo contratado.

4.3.4. Em incidente de severidade 1 com bloqueio indevido, a contratada deverá reverter imediatamente as regras afetadas para o modo de visibilidade.

4.4. Escalonamento

4.4.1. A contratada conduzirá o escalonamento ao fabricante sempre que necessário, cabendo-lhe:

a) abrir o chamado junto ao fabricante;

b) fornecer as evidências técnicas;

c) acompanhar o atendimento e realizar os escalonamentos necessários;

d) manter o Banco informado sobre a evolução; e

e) acompanhar o chamado até a efetiva resolução.

4.4.2. O acionamento do fabricante ou de terceiros não suspenderá os níveis de serviço atribuídos à contratada.

4.5. Manutenção e Atualização

4.5.1. Durante toda a vigência, estão incluídas as atualizações de versão, as correções de segurança e de defeitos e a atualização de conectores e integrações.

4.5.2. As atualizações deverão ser geridas por lotes e janelas, com reversão e continuidade da aplicação das regras nos ativos.

4.5.3. Nenhum componente essencial poderá permanecer em versão sem suporte durante a vigência.

4.6. Sustentação e Ajuste de Regras

4.6.1. A contratada deverá realizar revisão trimestral da plataforma, das regras não utilizadas e das exceções.

4.6.2. A sustentação deverá incluir apoio ao ajuste das regras em decorrência de:

- novas aplicações;
- alterações de infraestrutura;
- novas ameaças;
- incidentes de segurança;
- recomendações do fabricante.

4.7. Gestão de Capacidade

4.7.1. A contratada deverá acompanhar o inventário, os agentes, as licenças, os fluxos e os recursos da solução.

4.7.2. Deverão ser emitidos alertas preventivos de aproximação do limite de licenças contratadas, acompanhados de tendência e recomendação técnica.

4.7.3. Reserva de crescimento somente será considerada com memória de cálculo aprovada e sem duplicidade de contagem.

4.8. Continuidade Operacional

4.8.1. A aplicação das regras deverá ser local e autônoma. Quando houver perda de comunicação com a console, o agente deverá manter ativa a última regra válida, com comportamento seguro em falha configurável por grupo, sem bloquear o tráfego legítimo nem liberar indevidamente o tráfego (ARQ-03).

4.8.2. A contratada deverá apoiar e participar dos procedimentos e testes de contingência, *failover* e *failback* da solução.

4.9. Relatório Mensal

4.9.1. A contratada deverá apresentar relatório gerencial até o 10º dia do mês seguinte, contendo, no mínimo:

a) chamados e incidentes por severidade;

b) tempos de atendimento e solução;

c) cumprimento dos níveis de serviço do Anexo II;

d) cobertura e saúde dos agentes;

e) licenças em uso;

f) atualizações realizadas;

g) alterações de regras e exceções;

h) situação das integrações;

i) análises de causa raiz; e

j) planos de ação pendentes.

4.9.2. O relatório constituirá evidência para fiscalização e medição dos serviços.

4.10. Condições Gerais

4.10.1. O serviço será prestado sem dedicação exclusiva de mão de obra. Cabe à contratada dimensionar e gerir sua equipe de forma suficiente para cumprir os resultados e os níveis de serviço contratados.

4.10.2. Todos os acessos dos profissionais da contratada deverão ser individualizados, autorizados e rastreáveis, observando:

- o menor privilégio;
- a segregação de funções;
- as políticas de segurança da informação do Banco.

4.10.3. O escopo, as responsabilidades e eventual operação continuada serão consolidados antes do edital.

5. MATRIZ DE ADERÊNCIA NORMATIVA E AOS REFERENCIAIS TÉCNICOS

5.1. A matriz abaixo relaciona os requisitos deste Anexo aos seguintes referenciais:

- dispositivos da Resolução CMN nº 4.893/2021, com a redação da Resolução CMN nº 5.274/2025;
- subcategorias do NIST Cybersecurity Framework 2.0;
- salvaguardas dos CIS Critical Security Controls v8.

A matriz é informativa: demonstra a finalidade dos requisitos e não cria requisito adicional nem critério de aceitação. Ela também não implica que a solução assegure, isoladamente, a conformidade com a norma ou com os referenciais.

5.2. No art. 3º-A, I, “b” e “c” (isolamento dos ambientes Pix e STR), a solução contribui para a parcela lógica do isolamento e para sua evidência. A parcela física e a instância dedicada em nuvem dependem da arquitetura do ambiente. Requisitos sem correspondência na matriz atendem a necessidades operacionais, de desempenho ou de licenciamento.

5.3. Requisitos marcados (D) são desejáveis e não eliminatórios. O grau de contribuição de cada dispositivo e controle (principal, parcial ou complementar) consta da subseção 3.3 do Estudo Técnico Preliminar.

ID	Res. CMN nº 4.893/2021 (redação da Res. 5.274/2025)	NIST CSF 2.0	CIS v8
ARQ-01	art. 3º, § 11, II	PR.IR-01	4.4
ARQ-03	—	PR.IR-03	—
ARQ-04	—	PR.IR-03	—
ARQ-08	art. 3º, § 2º, XI, e § 11, I; art. 3º-A, I, “b” e “c”	PR.IR-01	3.12; 12.2
GER-02	art. 3º-A, I, “a”	—	—
GER-03	—	PR.AA-05	6.8
GER-05	art. 3º-A, I, “a”	—	—
GER-06	art. 3º, § 2º, VI, e § 7º, I a III	PR.PS-04	8.2 / 8.9 / 8.10
GER-08	—	DE.CM-09	—
AGT-08	—	DE.CM-09	—
SAG-02	art. 3º, § 8º, II	—	1.5
EST-01	—	—	4.5
EST-02	art. 3º, § 11, VI, e § 9º, I	PR.IR-01	4.5; 13.4
EST-03	—	PR.IR-01	4.5
EST-08	art. 3º, § 11, VI, e § 9º, I	—	—
NUV-01	—	ID.AM-01 / ID.AM-02	1.1
VIS-01	—	ID.AM-03	12.4
VIS-02	art. 3º, § 11, II	DE.CM-01; ID.AM-03	13.6
VIS-03	art. 3º, § 2º, VI, e § 7º, I a III	ID.AM-03; RS.AN-03	13.6
VIS-04	art. 3º, § 11, III e IV	ID.AM-03; RS.AN-03	—
VIS-05	—	ID.AM-03	—
VIS-06	—	ID.AM-03	12.4
VIS-07	art. 3º, § 11, II	ID.AM-03	—

ID	Res. CMN nº 4.893/2021 (redação da Res. 5.274/2025)	NIST CSF 2.0	CIS v8
ROT-01	—	ID.AM-01 / ID.AM-02; ID.AM-05	1.1; 3.12
ROT-02	art. 3º, § 8º, II	ID.AM-01 / ID.AM-02	—
ROT-03 (D)	—	ID.AM-01 / ID.AM-02	—
POL-01	art. 3º, § 11, II; art. 3º, § 11, VI, e § 9º, I; art. 3º, § 2º, XI, e § 11, I; art. 3º-A, I, “b” e “c”	PR.AA-05; PR.IR-01	3.12; 4.4; 12.2; 13.4
POL-02	art. 3º, § 11, II	PR.IR-01	13.4
POL-03	art. 3º, § 11, V; art. 3º, § 11, VI, e § 9º, I; art. 3º-A, I, “a”	PR.AA-05; PR.IR-01	—
POL-04	—	PR.IR-01	—
POL-05	art. 3º, § 2º, XI, e § 11, I	PR.IR-01	—
POL-06	art. 3º, § 2º, XI, e § 11, I	PR.IR-01; PR.IR-03	—
POL-07	—	PR.IR-01	—
POL-08	—	PR.IR-01	—
POL-09	—	PR.IR-01	—
POL-10	—	PR.IR-01	—
POL-11	art. 3º, § 11, III e IV	PR.IR-01	—
POL-14	art. 3º, § 11, V; art. 3º, § 11, VI, e § 9º, I	PR.AA-05	—
RES-01	art. 3º, § 2º, III; art. 3º, § 2º, VIII, e § 8º, V	RS.MI-01	17.4
RES-02	—	RS.MI-01	17.4
RES-03	art. 3º, § 11, III e IV; art. 3º, § 11, V; art. 3º, § 2º, III	DE.CM-01	13.1
RES-04 (D)	art. 3º, § 2º, VIII, e § 8º, V	DE.AE-02 / DE.AE-03	—
INT-02	art. 3º, § 11, V; art. 3º, § 2º, VI, e § 7º, I a III	DE.AE-02 / DE.AE-03; PR.PS-04	8.2 / 8.9 / 8.10; 13.1
INT-06	—	ID.AM-01 / ID.AM-02	1.1
LOG-01	art. 3º, § 2º, VI, e § 7º, I a III	PR.PS-04	—
LOG-02	art. 3º, § 2º, VI, e § 7º, I a III	PR.PS-04	—
LOG-03	art. 3º, § 2º, VI, e § 7º, I a III	PR.PS-04	8.2 / 8.9 / 8.10
LOG-04	—	GV.SC-05	—
LOG-05	—	GV.SC-05	—
SEG-01	—	GV.SC-05	—
SEG-02	—	GV.SC-05	—
REL-02	art. 22-A; art. 3º, § 2º, XI, e § 11, I; art. 3º-A, I, “b” e “c”	—	—

6. COMPROVAÇÃO DO ATENDIMENTO

6.1. O licitante provisoriamente classificado em primeiro lugar apresentará tabela ponto a ponto contendo, para cada requisito:

- número do requisito;
- descrição;
- documento comprobatório;
- endereço eletrônico (URL);

- página ou seção;
- trecho transcrito.

6.2. Documentos internos ou inacessíveis ao Banco não serão aceitos como comprovação.

6.3. Os requisitos marcados PoC serão verificados conforme o Matriz de Testes da Prova de Conceito (Anexo III).

7. REGRAS DE FORNECIMENTO, PREÇOS E VERIFICAÇÃO

7.1. A proposta deverá ser apresentada por itens, compatível com o Estudo Técnico Preliminar:

Item	Descrição	Quantidade
1	Servidores	863
2	Nós OpenShift	71
3	Estações de trabalho	4.066
4	Implantação	1 serviço
5	Operação assistida	90 dias
6	Treinamento	12 vagas
7	Suporte especializado	60 meses

7.2. Para cada item, a proposta deverá informar:

- preço unitário e preço total;
- prazo de cobertura;
- fabricante, edição, sku, *part number* e módulos;
- console e infraestrutura exigida;
- atualizações incluídas;
- suporte do fabricante e sustentação do integrador.

7.3. O início e o fim da vigência contratual serão únicos e definidos no Termo de Referência. Ativações posteriores não prorrogam automaticamente o término nem geram 60 meses adicionais por licença.

7.4. O preço deverá permitir o pagamento pelas unidades ativadas, a medição mensal e a ativação por ondas.

7.5. Se a solução exigir licenciamento diferente do previsto, o licitante deverá apresentar a conversão e o custo da cobertura equivalente antes da aceitação.

7.6. Antes do edital, serão fixados:

- as versões de sistema operacional, de UEK e do OpenShift;
- os limites de CPU e memória;
- a taxa de fluxos e a retenção;
- o limiar de latência p95;
- os tempos de propagação e de contenção;
- os critérios de glosa;
- a aplicação dos testes de Exadata e de estações;

- a duração dos períodos de medição.

Parâmetros pendentes de definição não poderão permanecer como critérios eliminatórios indeterminados.

ANEXO II — ACORDO DE NÍVEIS DE SERVIÇO

Solução de Microssegmentação por Agente

1. OBJETO E ESCOPO DO ACORDO

1.1. Este Acordo de Níveis de Serviço estabelece, para a sustentação da solução de microssegmentação por agente pelo período contratual de 60 (sessenta) meses:

- os indicadores e as metas;
- os critérios de medição e as evidências;
- as responsabilidades;
- os ajustes de pagamento por nível de serviço;
- os procedimentos aplicáveis.

1.2. Os níveis de serviço abrangem, conforme a arquitetura aprovada:

- os agentes instalados nos ativos protegidos;
- a console de gerenciamento, em modelo SaaS ou *on-premises*;
- os conectores e coletores;
- as integrações com SIEM, ServiceNow SIR, serviços de diretório e vCenter;
- o suporte técnico especializado;
- os procedimentos de contingência e de reversão.

1.3. A medição será orientada aos resultados efetivamente percebidos pelo Banco e utilizará evidências auditáveis, não se limitando a declarações da contratada ou do fabricante.

2. DEFINIÇÕES E REGRAS GERAIS DE MEDIÇÃO

2.1. **Aplicação das regras (*enforcement*):** capacidade dos agentes de manter ativas, nos ativos protegidos, as regras de proteção aprovadas, inclusive quando houver perda de comunicação com a console (requisito ARQ-03 do Anexo I).

2.2. **Disponibilidade do plano de gerenciamento:** percentual de tempo em que a console, as APIs administrativas, a gestão de regras, as funções de contenção e os relatórios permanecem acessíveis e operacionais.

2.3. **Integridade da aplicação das regras:** percentual de agentes saudáveis e aplicando a regra vigente em relação aos agentes implantados. A falha silenciosa de agentes é o principal risco operacional desse tipo de solução.

2.4. **Tempo de Resposta Inicial (TRI):** intervalo entre a abertura do chamado ou a detecção formal do incidente e o início efetivo do atendimento por profissional habilitado, com avaliação preliminar e comunicação ao Banco. A confirmação automática de abertura de chamado não constitui resposta inicial.

2.5. **Tempo de Contorno ou Restabelecimento (TCR):** intervalo entre o início da contagem e a execução de medida que reduza o impacto, recupere a proteção ou restabeleça o serviço afetado, ainda que mediante solução temporária aprovada. Inclui a reversão das regras afetadas para o modo de visibilidade.

2.6. **Tempo de Solução Definitiva (TSD):** intervalo necessário para a correção da causa do incidente e a validação da estabilidade do ambiente. A solução temporária não encerra a obrigação de correção definitiva.

2.7. **Bloqueio indevido:** bloqueio, pela solução, de comunicação legítima necessária ao funcionamento de aplicação ou serviço do Banco.

2.8. **Janela de manutenção:** período previamente autorizado pelo Comitê de Mudanças para intervenção planejada, observado o disposto neste Anexo.

2.9. **Minutos indisponíveis:** minutos em que o componente ou a função sujeita ao indicador permanece incapaz de cumprir sua finalidade contratada, conforme evidências do Banco e/ou da contratada.

2.10. Cada indicador possuirá definição, fórmula de cálculo, fonte de dados, periodicidade, responsável pela apuração e critérios de aceitação. Os registros utilizarão referência de horário consistente (requisito LOG-01) e deverão permitir a reconstrução dos eventos.

2.11. Para incidentes de severidade 1 e 2, a contagem dos prazos será contínua, em regime 24x7, inclusive sábados, domingos e feriados. Para as severidades 3 e 4, os prazos de resposta serão medidos em horas úteis, conforme indicado no item 4.

2.12. A contagem do prazo poderá ser suspensa quando o prosseguimento do atendimento depender de ação de responsabilidade exclusiva do Banco. A suspensão exige registro no chamado da dependência, com data, hora, justificativa, providência requerida e evidência objetiva. A suspensão limita-se à atividade impedida, mantendo-se a execução das demais ações possíveis.

3. CLASSIFICAÇÃO DE SEVERIDADE DOS INCIDENTES

3.1. A severidade será definida pelo impacto sobre a proteção e a continuidade dos serviços. A quantidade de ativos afetados será avaliada em conjunto com sua criticidade, pois o comprometimento de um único ativo pode afetar um serviço essencial.

Severidade	Classificação	Critério principal	Exemplos aplicáveis à microssegmentação
1	CRÍTICA	Interrupção de serviço essencial, perda de proteção de ambiente crítico ou impossibilidade de executar contenção necessária diante de incidente em curso.	Bloqueio indevido de tráfego em produção que interrompa operação bancária crítica; falha massiva de agentes; falha de aplicação das regras em ambiente crítico; indisponibilidade da console que impeça a contenção de ameaça ativa.
2	ALTA	Degradação relevante da proteção ou da operação, com	Falha de agentes em grupo restrito ou relevante de ativos; indisponibilidade do

Severidade	Classificação	Critério principal	Exemplos aplicáveis à microssegmentação
		impacto significativo e continuidade parcial dos serviços.	gerenciamento que impeça alterações urgentes; falha de integração com o SIEM ou o ServiceNow SIR.
3	MÉDIA	Falha localizada, com impacto limitado e alternativa operacional aceitável.	Funcionalidade não crítica indisponível, com contorno; inconsistência de relatório ou painel; falha de integração sem comprometimento imediato da proteção.
4	BAIXA	Ocorrência sem impacto relevante sobre a proteção ou a continuidade dos serviços.	Dúvida técnica, solicitação de informação, configuração ou melhoria sem urgência operacional.

3.2. O enquadramento e a reclassificação deverão ser registrados e justificados. A redução da severidade dependerá de evidência de redução do impacto e de validação pelo Banco.

4. NÍVEIS DE SERVIÇO PARA SUPORTE E INCIDENTES

4.1. O suporte técnico estará disponível para abertura de chamados em regime 24x7. Os prazos máximos abaixo serão contados a partir do primeiro destes eventos que tiver evidência auditável:

- registro do incidente pelo Banco;
- alerta gerado pela própria solução;
- detecção formal pela contratada.

Sev.	Cobertura	TRI máximo	TCR máximo	Solução definitiva
1	24x7	1 h	4 h	3 dias corridos, com plano de ação
2	24x7	2 h	8 h	10 dias corridos
3	Abertura 24x7; tratamento em horário útil	4 h úteis	72 h	30 dias corridos
4	Abertura 24x7; tratamento em horário útil	4 h úteis	—	Resposta em até 15 dias corridos

4.2. Os prazos acima reproduzem os parâmetros efetivamente contratados em processo público de microssegmentação utilizado como referência no Estudo Técnico Preliminar.

4.3. A periodicidade das atualizações de andamento de cada severidade será fixada antes do edital. Cada atualização informará diagnóstico, providências, impedimentos e previsão de restabelecimento.

4.4. Para as severidades 1 e 2, a contratada deverá mobilizar os níveis de escalonamento necessários, inclusive o fabricante, sem aguardar o esgotamento do prazo máximo de contorno.

4.5. Na severidade 1 com bloqueio indevido, a contratada deverá reverter imediatamente as regras afetadas para o modo de visibilidade, preservando a continuidade do negócio, e só depois investigar a causa.

4.6. O TCR será considerado cumprido quando houver restabelecimento comprovado da proteção e do serviço em condição operacional aceitável, ainda que a correção definitiva da causa permaneça em andamento.

4.7. Incidentes de severidade 1 deverão ter relatório de análise de causa, com causa, impacto, linha do tempo e medidas preventivas. O mesmo se aplica a incidentes de severidade 2 cuja recorrência justifique investigação. Os prazos de entrega dos relatórios serão fixados antes do edital [DEFINIR].

5. DISPONIBILIDADE DOS COMPONENTES E SERVIÇOS

5.1. A disponibilidade será apurada mensalmente, por componente ou função, pela fórmula D (%) = [(TM − TI) / TM] × 100, em que:

- TM corresponde ao total de minutos do período de medição;
- TI corresponde aos minutos de indisponibilidade atribuíveis à contratada.

Componente ou função	Meta mínima	Critério de indisponibilidade	Periodicidade
Console de gerenciamento SaaS	99,9% ao mês	Console ou API administrativa indisponível de forma que impeça a gestão, a consulta, a alteração de regras ou a contenção	Mensal
Console de gerenciamento *on-premises*, em cluster com alta disponibilidade, sob responsabilidade da contratada	99,9% ao mês	Indisponibilidade do conjunto de componentes que impeça as funções de gerenciamento, excluídas as falhas de infraestrutura do Banco	Mensal
Integridade da aplicação das regras	Percentual mínimo de agentes saudáveis e aplicando a regra vigente [DEFINIR]	Agentes implantados sem aplicar a regra vigente ou sem comunicação não detectada e não tratada	Mensal
Canais de suporte para severidades 1 e 2	24x7	Indisponibilidade simultânea dos canais definidos para abertura e escalonamento de incidentes críticos	Mensal

5.2. A disponibilidade da console será apurada separadamente da continuidade da aplicação das regras nos ativos. A indisponibilidade da console pode afetar a administração sem interromper a aplicação das regras existentes. As regras de cálculo deverão impedir que a disponibilidade de componentes não afetados oculte a indisponibilidade de uma função crítica.

5.3. Não serão consideradas indisponibilidade atribuível à contratada as ocorrências decorrentes exclusivamente de:

- ato ou omissão comprovada do Banco;
- indisponibilidade de infraestrutura, aplicação, rede ou serviço externo que não esteja sob responsabilidade contratual da contratada;
- caso fortuito ou força maior devidamente comprovados;
- mudanças solicitadas pelo Banco que impliquem indisponibilidade expressamente aceita.

5.4. Será contabilizada normalmente a indisponibilidade causada por qualquer destes fatores sob responsabilidade da contratada:

- erro de configuração;
- atualização;

- integração;
- mudança;
- operação;
- componente;
- terceiro.

6. MANUTENÇÃO PROGRAMADA E EMERGENCIAL

6.1. As manutenções programadas com potencial de impacto deverão ser comunicadas com antecedência mínima a ser fixada antes do edital [DEFINIR]. A comunicação deverá conter:

- escopo e risco;
- duração estimada;
- serviços e ativos afetados;
- plano de reversão;
- responsável técnico.

6.2. As intervenções em produção ocorrerão apenas em janelas aprovadas pelo Comitê de Mudanças do Banco, com avaliação de impacto e plano de reversão.

6.3. A atualização da console não poderá interromper a aplicação das regras nos ativos (requisito ARQ-05). A atualização dos agentes será feita em lotes e por grupo, com janela agendada e reversão (requisito GER-09).

6.4. A exclusão dos efeitos de manutenção programada no cálculo dos indicadores dependerá de autorização prévia e expressa do Banco. Ela não abrange falhas ou interrupções que excedam o período autorizado.

6.5. A manutenção emergencial destinada a tratar risco crítico de segurança ou de continuidade deverá ser comunicada imediatamente. Quando não for possível aviso prévio, a contratada registrará a justificativa e comunicará o Banco tão logo a intervenção seja iniciada.

6.6. A ausência de comunicação, a inexistência de justificativa técnica ou a falha de procedimento que resulte em indisponibilidade fará com que o período seja computado normalmente.

7. INDICADORES OPERACIONAIS DE SEGURANÇA E PROTEÇÃO

7.1. Os indicadores abaixo serão acompanhados e reportados mensalmente. As metas numéricas que dependam de linha de base serão homologadas nos testes de aceite e mantidas documentadas durante a vigência.

Indicador	Medição	Meta / tratamento
Cobertura dos ativos elegíveis	Proporção de ativos do escopo com agente implantado e operacional	Conforme os marcos de implantação; após M4, mínimo de 98% dos servidores e nós
Integridade da aplicação das regras	Agentes saudáveis e aplicando a regra vigente	Meta conforme o item 5; falhas tratadas por severidade
Conformidade das regras aplicadas	Divergências entre as regras aprovadas e as efetivamente aplicadas	Divergências tratadas como incidente, conforme o impacto

Indicador	Medição	Meta / tratamento
Bloqueios indevidos com impacto operacional	Quantidade, aplicações afetadas e tempo até a reversão	Tratamento como severidade 1 ou 2, conforme o impacto; redução contínua
Propagação de regras	Tempo entre a publicação aprovada e a efetivação nos agentes afetados	Até 5 minutos (requisito DES-03)
Tempo de contenção	Tempo entre o comando de isolamento e sua efetivação no ativo	Até 60 segundos (requisito RES-01)
Desempenho dos agentes	Consumo de CPU e memória e impacto na latência p95 das transações	Limites dos requisitos AGT-04, EST-05 e DES-04
Entrega de registros ao SIEM	Continuidade e tempestividade da entrega de eventos, fluxos e auditoria	Interrupções relevantes classificadas por severidade
Atualização dos componentes	Cumprimento dos prazos aprovados para correções e atualizações	Falhas críticas tratadas como incidente

8. CAPACIDADE, CONSUMO E ALERTAS PREVENTIVOS

8.1. A contratada deverá disponibilizar indicadores que permitam acompanhar, no mínimo:

- os ativos inventariados e os agentes implantados e ativos;
- as licenças contratadas, ativadas e disponíveis, por item;
- o volume de fluxos e de registros;
- o consumo de recursos da console *on-premises*, quando aplicável.

8.2. A linha de base contratada corresponde aos quantitativos e às especificações do Anexo I.

8.3. A contratada deverá emitir alertas preventivos quando a utilização das licenças contratadas se aproximar dos limites, em percentuais a serem fixados antes do edital [DEFINIR]. Os alertas serão acompanhados de tendência e recomendação técnica.

8.4. O atingimento do limite contratado não poderá resultar em:

- suspensão automática da proteção;
- remoção de regras;
- perda de registros;
- degradação dos serviços.

8.5. As licenças serão reconciliadas com o inventário e os agentes ativos por identificador único.

9. CONTINUIDADE, FAILOVER, FAILBACK E RECUPERAÇÃO

9.1. A arquitetura deverá evitar ponto único de falha capaz de interromper o gerenciamento ou a capacidade de contenção (requisito ARQ-04).

9.2. Na perda de comunicação com a console, os agentes deverão manter ativa a última regra válida, com comportamento seguro em falha configurável por grupo, sem bloquear o tráfego legítimo nem liberar indevidamente o tráfego (requisito ARQ-03).

9.3. A contratada deverá participar dos testes de *failover* e *failback* da console *on-premises*, quando aplicável, e dos testes de perda de comunicação entre agente e console. Os testes seguirão o plano aprovado pelo Banco e serão repetidos após alterações arquiteturais relevantes.

9.4. Os testes deverão registrar:

- o tempo de detecção, comutação e retorno;
- a preservação das regras;
- a integridade dos registros;
- os impactos observados.

9.5. Falhas de *failover* ou perda de redundância serão classificadas conforme a severidade e tratadas nos prazos do item 4.

10. APURAÇÃO, EVIDÊNCIAS E RELATÓRIO MENSAL

10.1. A apuração será mensal e consolidará os indicadores do período, inclusive em meses sem incidentes. Incidentes de severidade 1 terão acompanhamento imediato, independentemente do ciclo mensal.

10.2. A contratada deverá apresentar, até o 10º (décimo) dia do mês subsequente, relatório gerencial contendo, no mínimo:

- disponibilidade por componente ou função;
- cobertura e integridade da aplicação das regras;
- relação de incidentes e chamados, com severidade, horários, TRI, TCR, TSD e situação final;
- bloqueios indevidos e reversões executadas;
- manutenções realizadas;
- eventos de *failover* e *failback*;
- licenças em uso e indicadores de capacidade;
- alterações de regras e exceções;
- situação das integrações e da entrega de registros;
- atualizações de versão dos agentes e da plataforma;
- relatórios de análise de causa e planos de ação pendentes;
- cálculo dos ajustes de pagamento, quando aplicáveis.

10.3. A revisão da plataforma, das regras não utilizadas e das exceções será trimestral.

10.4. As principais fontes de evidência serão:

- o monitoramento do Banco;
- o SIEM;
- os registros e a trilha de auditoria da solução;
- os registros do ServiceNow;
- a telemetria do fabricante;
- os relatórios de disponibilidade;
- os testes controlados.

10.5. Em caso de divergência entre fontes, prevalecerá a análise técnica baseada em evidências reproduzíveis e na visão de ponta a ponta do serviço percebido pelas aplicações.

11. AJUSTES DE PAGAMENTO POR DESCUMPRIMENTO DOS NÍVEIS DE SERVIÇO

11.1. Os ajustes previstos neste item adequam a remuneração ao nível de serviço efetivamente entregue. Eles não se confundem com sanções administrativas por inexecução contratual.

11.2. O descumprimento dos prazos do item 4 gerará glosa sobre a fatura mensal do suporte técnico (item 7), por indicador. A soma das glosas no mês ficará limitada a 20% (vinte por cento) do valor dessa fatura.

11.3. A escala de glosa por indicador e por severidade será fixada antes do edital [DEFINIR].

11.4. A indisponibilidade da console SaaS abaixo da meta gerará crédito ou glosa proporcional sobre a subscrição, conforme regra a ser definida com a área jurídica [DEFINIR].

Elemento	Situação
Teto da glosa sobre o suporte	20% da fatura mensal [DEFINIR escala].
Disponibilidade e atendimento	Escala de glosa a ser divulgada no instrumento convocatório [DEFINIR].

11.5. O mesmo fato gerador não será utilizado para duplicar ajustes dentro do mesmo indicador.

11.6. A contratada terá direito ao contraditório quanto à apuração, devendo apresentar evidências técnicas no prazo definido no contrato ou na notificação de glosa.

12. REINCIDÊNCIA E ESCALONAMENTO CONTRATUAL

12.1. Os desvios dos níveis de serviço serão apurados e acompanhados de medidas corretivas. A contratada conduzirá o escalonamento ao fabricante, e o Banco fará o acompanhamento.

12.2. Desvios recorrentes deverão gerar Plano de Ação Corretiva formal, com causa raiz, responsáveis, prazos e medidas preventivas.

12.3. Os gatilhos quantitativos de reincidência e as medidas administrativas correspondentes serão definidos no instrumento contratual definitivo [DEFINIR].

13. INDICADORES SUJEITOS À HOMOLOGAÇÃO DE LINHA DE BASE

13.1. Antes do edital, deverão ser fixados:

- as versões de sistema operacional, de UEK e do OpenShift;
- os limites de CPU e memória dos agentes;
- a taxa de fluxos e a retenção;
- o limiar de latência p95;
- os tempos de propagação e de contenção;
- os critérios de glosa;
- a aplicação dos testes de Exadata e de estações;

- a duração dos períodos de medição.

13.2. Para cada indicador, o método de medição, o ambiente, a duração, os limites e as exclusões serão definidos de modo uniforme antes do edital e confirmados no aceite.

13.3. Não serão aplicadas metas numéricas sem memória de cálculo, método de medição, fonte de evidência e responsabilidade claramente definidos. Nenhuma meta pendente de definição poderá tornar-se obrigatória ou permanecer como critério eliminatório indeterminado.

13.4. Uma vez homologadas, as metas passarão a integrar a linha de base operacional e constarão do relatório mensal.

14. DISPOSIÇÕES FINAIS

14.1. A aprovação da solução na Prova de Conceito ou no aceite não afasta a obrigação de cumprimento contínuo dos níveis de serviço durante toda a vigência. A Prova de Conceito também não substitui a homologação por ondas nem a fiscalização contínua.

14.2. Os ajustes de pagamento previstos neste Anexo não eximem a contratada das seguintes obrigações:

- corrigir a causa;
- restabelecer a solução;
- manter a continuidade;
- apresentar a análise de causa;
- cumprir as demais obrigações contratuais.

14.3. O Banco poderá auditar os indicadores e solicitar os dados brutos necessários à comprovação dos resultados, observadas as regras de segurança e confidencialidade.

14.4. A apuração observará evidências auditáveis, responsabilidades claras e o direito de contestação, conforme o Estudo Técnico Preliminar. Situações não previstas serão tratadas com base no impacto efetivo ao serviço, na matriz de responsabilidades, nas evidências técnicas e nas disposições do Termo de Referência e do contrato.

ANEXO III — MATRIZ DE TESTES DA PROVA DE CONCEITO (PoC)

Solução de Microssegmentação por Agente

1. OBJETO

1.1. Este Anexo estabelece, para a Prova de Conceito (PoC) da solução de microssegmentação por agente:

- os critérios e procedimentos;
- os casos de teste;

- as evidências exigidas;
- as responsabilidades;
- as condições de aprovação ou reprovação.

1.2. A PoC será realizada com o licitante provisoriamente classificado em primeiro lugar, após a fase de julgamento e antes da adjudicação do objeto.

1.3. A finalidade da PoC é comprovar, de forma prática, objetiva, verificável e mensurável, que a solução ofertada atende aos requisitos obrigatórios aplicáveis do Edital, do Termo de Referência e do Anexo I. A verificação será feita por meio de 30 (trinta) casos de teste, executados em laboratório do Banco isolado do ambiente de produção.

1.4. A PoC não constitui apresentação comercial. Não serão admitidos como comprovação suficiente:

a) declaração unilateral do licitante;

b) material de marketing;

c) *roadmap*;

d) funcionalidade futura;

e) promessa de desenvolvimento;

f) customização ainda não disponível; ou

g) demonstração de edição, módulo ou solução distinta daquela efetivamente ofertada.

2. PRINCÍPIOS DA AVALIAÇÃO

2.1. Os testes serão orientados ao resultado funcional da solução, e não à reprodução de nomes comerciais, consoles ou arquiteturas de determinado fabricante. Não serão exigidas como teste funcionalidades fora do objeto.

2.2. A PoC deverá ser executada com a mesma edição e os mesmos módulos ofertados. A documentação técnica e a licença de avaliação deverão comprovar essa identidade.

2.3. Os métodos de comprovação (DOC, PoC, ACE e DEC) são os definidos no Anexo I. Requisitos com comprovação por teste de aceite (ACE) não são convertidos automaticamente em exigência da PoC. Documentação e declaração observam os limites de comprovação do Anexo I.

2.4. Os casos de teste estão agrupados nos seguintes blocos:

I. arquitetura e governança;

II. agentes e compatibilidade;

III. inventário, visibilidade e rotulagem;

IV. regras de proteção, identidade e contenção;

V. nuvem, OpenShift e Oracle Exadata;

VI. integrações, registros e relatórios;

VII. estações de trabalho (condicionado).

2.5. Os casos do bloco VII somente serão aplicados se o escopo de estações de trabalho for mantido antes do edital. Essa decisão depende da validação do inventário e da comparação do custo total em 60 meses com o controle já disponível na solução de EDR.

2.6. O caso MC24 depende da compatibilidade com o Oracle Exadata, conforme as versões de Oracle Linux, UEK e Exadata System Software e a admissibilidade pela Oracle. Se a Oracle não admitir a instalação do agente nos *database servers*, o caso será substituído pela verificação da proteção indireta desses ativos (SAG-01).

2.7. Os valores de referência e os campos pendentes serão fixados antes do edital e não poderão permanecer como critérios eliminatórios indeterminados.

3. CONVOCAÇÃO E PREPARAÇÃO DA PoC

3.1. O licitante será convocado para reunião preparatória da PoC.

3.2. Na reunião, deverão ser definidos:

a) o laboratório de execução, isolado da produção, com VMware vSphere, OpenShift, OCI, Azure e ambiente equivalente ao Exadata;

b) a amostra de ativos e as respectivas versões de sistema operacional;

c) a versão do OpenShift e o CNI em uso;

d) as aplicações de teste e os fluxos legítimos e indevidos;

e) as contas de usuário e os grupos do AD;

f) as integrações (SIEM, ServiceNow SIR, AD/Entra ID, vCenter) ou seus simuladores;

g) a linha de base de desempenho e a metodologia de medição;

h) os procedimentos de reversão;

i) as ferramentas de geração de tráfego e de medição;

j) as responsabilidades do Banco e do licitante; e

k) o cronograma.

3.3. O licitante deverá informar previamente todos os recursos necessários à realização da PoC. Os recursos, as responsabilidades e o cronograma serão consolidados antes do edital [CONSOLIDAR].

3.4. A modalidade de execução não poderá prejudicar:

- a auditabilidade;
- a rastreabilidade;
- a isonomia;
- a segurança;

- o acompanhamento pela comissão;
- a reprodução dos resultados.

3.5. Todos os custos do licitante associados à PoC serão de sua responsabilidade.

4. COMISSÃO TÉCNICA

4.1. A PoC será avaliada por comissão técnica formalmente designada pelo Banco [DESIGNAR].

4.2. Poderão compor a comissão representantes das áreas de:

a) segurança;

b) infraestrutura;

c) redes;

d) aplicações;

e) SOC; e

f) fiscalização técnica.

A composição observará a governança das regras e a matriz de responsabilidades (RACI).

4.3. Compete à comissão:

a) conduzir os testes;

b) verificar os requisitos;

c) solicitar a repetição de testes, quando tecnicamente necessária;

d) registrar as evidências;

e) registrar as ocorrências e limitações;

f) classificar cada teste; e

g) produzir o relatório final.

5. CRITÉRIOS DE AVALIAÇÃO

5.1. Cada caso de teste receberá um dos seguintes resultados, com a respectiva evidência:

- ATENDE
- NÃO ATENDE

5.2. Os testes serão classificados como:

- **CRÍTICO:** verifica requisito obrigatório aplicável; atendimento obrigatório.
- **COMPLEMENTAR:** verifica requisito desejável; registrado sem reprovação.

5.3. A solução será aprovada quando atender integralmente aos casos CRÍTICOS aplicáveis.

5.4. A falta de recurso do laboratório deverá ser registrada e resolvida, sem equiparar automaticamente a impossibilidade de execução a falha da solução. O teste poderá ser repetido quando a limitação for comprovadamente atribuível ao laboratório do Banco.

5.5. Quando uma capacidade não puder ser razoavelmente reproduzida em escala na PoC, a via de comprovação alternativa deverá estar definida antes do certame. A via alternativa deverá ser compatível com o método do requisito e poderá combinar:

a) teste representativo;

b) documentação oficial;

c) evidência de licenciamento;

d) arquitetura ofertada;

e) memória de dimensionamento; e

f) evidência técnica verificável.

6. MATRIZ CONSOLIDADA DE TESTES

6.1. BLOCO I — ARQUITETURA E GOVERNANÇA

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC01	Agente e console única (ARQ-01, ARQ-02)	Demonstrar a console e a regra aplicada localmente pelo agente em máquina virtual e em instância de nuvem	Arquitetura e edição ofertadas; decisão de fluxo tomada no próprio ativo	CRÍTICO
MC02	Autonomia sem console (ARQ-03)	Interromper a comunicação entre agente e console; testar fluxo autorizado e vedado; restabelecer a comunicação	Última regra válida mantida; tráfego legítimo e bloqueios preservados	CRÍTICO
MC03	Administração segura (GER-01 a GER-06)	Demonstrar SSO com MFA, perfis RBAC permitidos e vedados e trilha de auditoria	Registros de acesso, permissões segregadas e auditoria com usuário, data, hora, objeto e valores anterior e posterior	CRÍTICO
MC04	Integridade e remoção do agente (AGT-07, AGT-09)	Tentar adulterar o agente sem autorização; retirar o agente de forma autorizada	Alerta na console; ausência de regra residual e de interrupção da aplicação	CRÍTICO

6.2. BLOCO II — AGENTES E COMPATIBILIDADE

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC05	Instalação e atualização (AGT-02, AGT-03, GER-09)	Instalar e atualizar agentes em grupo, com procedimento de reversão, observando reinicializações	Registros de versão e de reinicialização; instalação em massa comprovada no aceite (ACE)	CRÍTICO
MC06	Consumo de recursos e latência (AGT-04, DES-04)	Medir CPU, memória e latência p95 antes e depois da aplicação das regras, sob carga equivalente	Linha de base e séries de medição; CPU < 5%, memória < 10% e p95 ≤ 5%	CRÍTICO

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC07	Convivência com EDR e agentes corporativos (AGT-05)	Executar fluxos e regras com a solução de EDR e os demais agentes corporativos presentes na amostra	Ausência de conflito de filtros de rede, de falhas e de regressão	CRÍTICO
MC08	Identificação de processo e serviço (AGT-08, VIS-02, POL-02)	Distinguir processos distintos em fluxos para o mesmo destino e porta	Fluxos com o processo identificado e aplicação da regra correspondente	CRÍTICO

6.3. BLOCO III — INVENTÁRIO, VISIBILIDADE E ROTULAGEM

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC09	Mapa de dependências e consultas (VIS-01, VIS-04, VIS-07)	Gerar conexões permitidas, bloqueadas e com falha; pesquisar o histórico e o mapa	Origem, destino, processo e decisão exibidos; filtros funcionais	CRÍTICO
MC10	Modo de visibilidade e simulação (AGT-06, VIS-05, POL-05)	Observar a aplicação sem bloqueio e simular regra restritiva	Fluxo real preservado e impacto previsto exibido	CRÍTICO
MC11	Rótulos multidimensionais (ROT-01, ROT-02)	Rotular por ambiente, aplicação, camada e localização; alterar atributo e validar a atualização automática	Regras de rotulagem automática, rótulos e agrupamento atualizados	CRÍTICO
MC12	Ativos sem agente (SAG-01, SAG-02)	Cadastrar e descobrir ativo sem agente; testar comunicações a partir de ativo protegido	Proteção indireta (*ring-fencing*) efetiva; registro explícito dos fluxos não cobertos	CRÍTICO

6.4. BLOCO IV — REGRAS DE PROTEÇÃO, IDENTIDADE E CONTENÇÃO

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC13	Menor privilégio (POL-01, POL-02)	Aplicar lista de permissão por rótulo, IP, porta e processo; testar exceções	Fluxos previstos permitidos e demais bloqueados	CRÍTICO
MC14	Identidade e processo (POL-03, POL-14, INT-03)	Comparar usuários autorizados e vedados e processos distintos no mesmo serviço	Decisão correlacionada a usuário, grupo do AD e processo	CRÍTICO
MC15	Recomendação e aplicação por ondas (POL-04, POL-06)	Gerar recomendação a partir dos fluxos e aprovar aplicação em grupo piloto	Revisão humana, simulação e ativação por grupo	CRÍTICO
MC16	Versionamento e aprovação (POL-07, POL-08)	Alterar regra, registrar aprovação e retornar à versão anterior	Histórico, aprovador e reversão sem restauração de backup	CRÍTICO
MC17	Exceção temporária (POL-09)	Criar exceção justificada e observar a expiração automática	Prazo, responsável e regra expirada	CRÍTICO
MC18	Saída por FQDN (POL-11)	Permitir destino externo autorizado e vedar outro, na amostra definida	Decisão de saída por FQDN e processo	CRÍTICO

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC19	Contenção pela console (RES-01, RES-03)	Isolar ativo; medir a propagação; manter o canal de investigação (EDR, coleta forense ou PAM) conforme o plano	Isolamento em até 60 segundos; alertas emitidos; canal de investigação preservado; liberação executada	CRÍTICO
MC20	Contenção via ServiceNow SIR (RES-02, INT-01)	Acionar a contenção e a reversão pela API integrada ao ServiceNow SIR	Chamada autenticada, ação executada no agente e registro em auditoria	CRÍTICO

6.5. BLOCO V — NUVEM, OPENSHIFT E ORACLE EXADATA

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC21	Conectores de nuvem (NUV-01, NUV-02)	Importar inventário e *tags* da OCI e do Azure e comprovar a aplicação das regras pelo agente	Instâncias e rótulos importados; aplicação sem dependência do provedor	CRÍTICO
MC22	OpenShift e CNI (CNT-01, CNT-03)	Aplicar regras em *namespaces* e *deployments*; verificar a convivência com o CNI e as *NetworkPolicies*	Recriação de cargas de trabalho sem perda de regra e sem falha do cluster	CRÍTICO
MC23	Contêiner e máquina virtual (CNT-04)	Testar fluxos entre carga de trabalho em contêiner e máquina virtual protegida, na mesma console	Regra e mapa unificados	CRÍTICO
MC24	Oracle Exadata e RAC (AGT-12)	Validar a documentação de versões e a admissibilidade; testar o agente em ambiente admitido, com exclusão das interfaces de *interconnect* e de armazenamento, e verificar os fluxos de replicação	Compatibilidade documentada publicamente; ausência de degradação; rede privada e replicação preservadas; via equivalente [DEFINIR]	CRÍTICO, condicionado (item 2.6)

6.6. BLOCO VI — INTEGRAÇÕES, REGISTROS E RELATÓRIOS

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC25	API e SIEM (INT-01, INT-02)	Testar a API com escopo; enviar eventos ao SIEM; interromper e restabelecer a integração	Eventos íntegros; fila e reenvio funcionais	CRÍTICO
MC26	vCenter e inventário (INT-06)	Importar *tags* de máquinas virtuais e verificar a convivência com o vSphere e o firewall distribuído da plataforma de virtualização	Inventário e regras sem conflito	CRÍTICO
MC27	Relatórios e evidências (REL-01, REL-02)	Gerar e exportar relatórios de cobertura, exceções, violações e segregação entre ambientes	Relatórios auditáveis exportados	CRÍTICO

6.7. BLOCO VII — ESTAÇÕES DE TRABALHO (CONDICIONADO)

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC28	Bloqueio entre estações (EST-01, EST-02, EST-04, EST-06)	Em piloto confirmado, instalar o agente silenciosamente e bloquear SMB, RDP e WinRM indevidos, mantendo as exceções	Fluxos autorizados preservados; convivência com os demais agentes	CRÍTICO, condicionado (item 2.5)
MC29	Notebook fora da rede (EST-03, EST-05)	Testar o perfil externo, a perda de comunicação com a console e o retorno à rede, com linha de base de recursos	Regra local mantida; sincronização no retorno; limites de consumo	CRÍTICO, condicionado (item 2.5)

ID	Requisito	Procedimento resumido	Evidência esperada	Classificação
MC30	Identidade e isolamento de estação (EST-07, EST-08)	Testar o acesso por grupo do AD e isolar a estação via ServiceNow SIR, preservando a investigação	Acesso por identidade, contenção e reversão auditáveis	CRÍTICO, condicionado (item 2.5)

7. COMPROVAÇÃO DE CAPACIDADE E LICENCIAMENTO

7.1. A amostra funcional da PoC não demonstra a escala de 5.000 ativos. O licitante deverá apresentar, conforme os requisitos DES-01 e DES-02:

- arquitetura da solução;
- memória de capacidade;
- volumetria de fluxos;
- cobertura;
- licença da edição ofertada.

7.2. Serão validadas a documentação de escala, as unidades de licenciamento, os módulos e os *part numbers*. Também serão verificadas as seguintes regras de licenciamento:

- os nós de controle e de infraestrutura do OpenShift estão incluídos;
- *pods*, CDBs e instâncias de banco não geram licenças adicionais;
- os nós não são contados novamente como máquinas virtuais;
- ativos inativos e ativação simultânea do ambiente de contingência têm tratamento explícito.

8. EVIDÊNCIAS

8.1. Para cada caso de teste, deverão ser registrados:

- configuração;
- versão da solução e do agente;
- dados de entrada;
- resultado esperado;
- resultado obtido;
- registros (*logs*);
- duração;
- responsáveis.

8.2. Os dados e os horários dos testes deverão ser preservados, de modo a permitir a reprodução dos resultados.

9. APROVAÇÃO

9.1. A solução será aprovada quando atender integralmente aos requisitos obrigatórios aplicáveis, com comprovação nos métodos estabelecidos no Anexo I.

9.2. Os requisitos desejáveis não são eliminatórios. Os parâmetros e a aplicabilidade dos casos condicionados deverão estar fixados antes do edital.

10. REPROVAÇÃO

10.1. A solução será reprovada no caso de não atendimento comprovado de requisito obrigatório aplicável e previamente determinado.

10.2. Impedimento atribuível ao laboratório do Banco será registrado para providência técnica, sem presunção automática de reprovação.

11. RELATÓRIO FINAL

11.1. A comissão técnica produzirá relatório final contendo:

a) a solução e a edição avaliadas;

b) os requisitos e casos de teste executados;

c) as evidências;

d) a aplicabilidade dos casos condicionados;

e) as limitações e ocorrências;

f) os resultados por caso; e

g) a conclusão de aprovação ou reprovação, motivada.

12. DISPOSIÇÕES FINAIS

12.1. A PoC não substitui:

- o aceite por onda de implantação;
- os testes de intrusão independentes;
- o acompanhamento dos níveis de serviço do Anexo II.

12.2. Os casos de estações de trabalho (bloco VII) somente se aplicam se esse escopo for mantido antes do edital.

12.3. O roteiro executivo, as versões, a duração e as ferramentas da PoC serão consolidados antes do edital.

ANEXO IV — MODELO DE CARTA-PROPOSTA DE PREÇOS

Solução de Microssegmentação por Agente

CARTA-PROPOSTA DE PREÇOS

REF.: RFP — Chamamento Público nº 2026/[PREENCHER]

Data: [PREENCHER]

1. PROPONENTE

Razão Social:

Sede:

CNPJ/MF:

Telefone:

Endereço completo:

E-mail:

Prezados Senhores,

Pela presente, submetemos à apreciação de V. Sªs. nossa proposta de preços relativa ao chamamento público 2026/[PREENCHER], para a solução de microssegmentação por agente. Assumimos inteira responsabilidade por quaisquer erros ou omissões que venham a ser verificados na sua preparação.

Declaramos ter pleno conhecimento das condições de fornecimento e de prestação de serviços previstas na RFP e em seus Anexos, que conhecemos em todos os seus termos e a respeito dos quais não temos quaisquer dúvidas.

Identificamos, na matriz de aderência da proposta técnica, o atendimento integral, parcial ou o não atendimento de cada requisito, bem como as premissas e as condições de fornecimento. Esta proposta considera a base provisória e as condicionantes do dimensionamento de referência e não constitui contrato ou adjudicação.

2. PROPOSTA DE PREÇOS

Item	Descrição	Quant.	Unidade	Valor Unitário (R$)	Valor Total (R$)
1	Subscrição de solução de microssegmentação por agente para servidores (físicos, virtuais ou instâncias em nuvem), incluindo console de gerenciamento, agentes, conectores, atualizações e suporte de nível 3 do fabricante.	863	Servidor/mês, por 60 meses		
2	Subscrição de solução de microssegmentação por agente para nós de cluster OpenShift (de	71	Nó/mês, por 60 meses		

Item	Descrição	Quant.	Unidade	Valor Unitário (R$)	Valor Total (R$)
	trabalho, de controle e de infraestrutura), cobrindo todos os contêineres do nó.				
3	Subscrição de solução de microssegmentação por agente para estações de trabalho (desktops e notebooks).	4.066	Estação/mês, por 60 meses		
4	Serviços de planejamento, projeto executivo, instalação, configuração, integração, testes, homologação e entrada em produção da solução, por ondas, incluindo integração com SIEM, ServiceNow SIR, serviços de diretório e vCenter.	1	Serviço		
5	Operação assistida e estabilização por 90 (noventa) dias após o último marco de implantação.	1	Serviço		
6	Capacitação técnica oficial do fabricante e transferência de conhecimento para as equipes indicadas pelo Banco.	12	Vaga		
7	Serviço mensal de suporte técnico especializado 24x7, sustentação, manutenção, escalonamento ao fabricante e apoio a incidentes relacionados à solução, excluídos o suporte de nível 3 do fabricante e as atualizações já incluídos na subscrição (itens 1 a 3).	60	Mês		
	VALOR GLOBAL DA PROPOSTA				R$

VALOR TOTAL: R$ _____ (_____)

VALIDADE DA PROPOSTA: 90 (noventa) dias.

2.1. Para os itens 1 a 3, deverão ser informados o valor por unidade e mês, o equivalente anual e o custo da cobertura durante a vigência contratual única de 60 meses.

2.2. Os itens serão calculados da seguinte forma:

Item	Forma de cálculo
1 a 3	Teto com ativação integral = quantidade × preço unitário mensal × 60. O desembolso efetivo seguirá as unidades ativadas e os meses restantes até o término do contrato. A ativação por ondas não renova o prazo de 60 meses.
4 e 5	Valor do serviço integral.
6	Preço por vaga × 12.
7	Valor mensal × 60.

2.3. Se a métrica comercial do fabricante divergir da prevista, a proponente deverá anexar a conversão para a cobertura equivalente.

2.4. A proponente deverá distinguir o suporte de nível 3 do fabricante, incluído na subscrição, do suporte especializado prestado pelo integrador (item 7). Componente necessário embutido em outro item deverá ser identificado como incluído, com indicação do item em que é cobrado. Componente sem cotação permanecerá pendente e nunca será presumido gratuito.

3. COMPOSIÇÃO DA SOLUÇÃO OFERTADA

A PROPONENTE deverá informar os componentes que integram a solução ofertada, permitindo a rastreabilidade técnica e comercial da proposta.

Item	Fabricante	Produto/Solução	Módulo, Edição e Versão	SKU/Part Number, quando aplicável	Métrica de Licenciamento	Quantidade	Vigência
1							60 meses
2							60 meses
3							60 meses
4							
5							90 dias
6							
7							60 meses

Deverão ser relacionados a console, os módulos, os agentes, os conectores e a infraestrutura necessária. Os componentes necessários já incluídos deverão ser descritos com a indicação do item em que são cobrados, sem duplicidade de custos.

Quando determinado componente não possuir SKU ou *Part Number*, a PROPONENTE deverá informar a denominação comercial e a respectiva métrica utilizada pelo fabricante.

4. DECLARAÇÕES DA PROPONENTE

A proponente declara que:

a) esta proposta corresponde exatamente às exigências contidas na RFP e em seus Anexos, às quais adere formalmente;

b) as métricas, a cobertura, os preços, os tributos e as dependências foram explicitados, e a solução demonstrada na Prova de Conceito corresponderá à edição e aos módulos ofertados;

c) as licenças terão término compatível com a vigência contratual única, sem novo prazo de 60 meses a cada ativação;

d) as ressalvas e os requisitos não atendidos foram identificados na matriz de aderência;

e) para a sua participação neste processo, não incorreu na prática de atos lesivos à Administração Pública elencados no art. 5º da Lei nº 12.846/2013, estando ciente das penalidades a que ficará sujeita no caso de cometimento de tais atos;

f) não possui sócio, dirigente ou administrador que seja empregado do BANCO DA AMAZÔNIA ou que possua vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau) com:

- empregados detentores de cargo comissionado que atuem em área do BANCO DA AMAZÔNIA com gerenciamento sobre o contrato ou sobre o objeto da presente contratação;
- empregados detentores de cargo comissionado que atuem na área demandante;
- empregados detentores de cargo comissionado que atuem na área que realiza a contratação;
- autoridade do BANCO DA AMAZÔNIA hierarquicamente superior às áreas mencionadas.

TIPO DE GARANTIA CONTRATUAL: [DEFINIR no instrumento definitivo, se aplicável].

FORMA DE HABILITAÇÃO: [DEFINIR no instrumento definitivo]. Esta RFP não constitui habilitação.

5. DETALHAMENTO DE PREÇOS E TRIBUTOS

A proponente deverá apresentar, em anexo a esta carta, planilha de formação de preços em formato editável, contendo:

a) a memória de cálculo por item;

b) os tributos incidentes (ISS, PIS, COFINS e demais aplicáveis) e as respectivas alíquotas;

c) os custos de infraestrutura, de deslocamento e de integrações, se houver;

d) a discriminação entre parcela recorrente (subscrições e suporte) e não recorrente (implantação, operação assistida e capacitação); e

e) o desembolso previsto por ondas de ativação.

Preços não informados ficarão pendentes.

6. DADOS DA EMPRESA E DO REPRESENTANTE LEGAL

Dados da empresa:

Razão Social:

CNPJ/MF:

Endereço Sede:

Cidade/UF:

CEP:

Telefone:

E-mail:

Banco/Agência:

Conta Corrente:

Dados do representante legal da empresa para assinatura do contrato:

Nome:

Cargo:

Endereço:

CEP:

Cidade/UF:

CPF/MF:

RG/Órgão Expedidor:

Telefone/E-mail:

Caso nos seja adjudicado o objeto da futura licitação, comprometemo-nos a assinar o Contrato no prazo determinado no documento de convocação.

……..(……), ….. de ……. de 2026.

Nome e assinatura do representante legal da proponente