NOTA TÉCNICA / SUSTENTAÇÃO TÉCNICA

Fundamentação para Contratação de Solução de Microssegmentação por Software Baseada em Agente, com Console Única, para Ambiente Híbrido, em Lote Único

Documento de referência técnico-jurídica para instrução da RFP, do Estudo Técnico Preliminar (ETP) e do Termo de Referência (TR)

BANCO DA AMAZÔNIA S.A.

[Nº DO PROCESSO ADMINISTRATIVO — A PREENCHER] | Minuta v1.0

Outubro de 2026

SUMÁRIO

1. Apresentação e Premissas 3

2. Objeto 3

3. Fundamentação Legal e Normativa 4

3.1. Lei nº 13.303/2016 (Lei das Estatais) e Regulamento de Licitações e Contratos do Banco 4

3.2. Referenciais metodológicos de planejamento e pesquisa de preços 5

3.3. Lei Geral de Proteção de Dados Pessoais — LGPD (Lei nº 13.709/2018) 5

3.4. Regulação de segurança cibernética e referenciais técnicos 5

3.5. Controle da competitividade e fundamentação da modelagem 5

4. Contextualização Técnica da Necessidade 6

4.1. Da movimentação lateral e da aplicação do menor privilégio 6

4.2. Da cobertura híbrida e da autonomia da aplicação das regras 6

4.3. Do risco de operação fragmentada 7

4.4. Da console única, do fabricante único e do lote único 8

5. Justificativa Técnica para Contratação em Plataforma Única 8

5.1. Sistema integrado e interdependência técnica 8

5.2. Transparência de preços e eficiência de gestão contratual 9

5.3. Preservação da competitividade — requisito funcional, não marca 9

5.4. Consulta ao mercado e validação das alternativas 9

6. Requisito Central: Consistência de Regras e Aplicação Local 10

6.1. Objetos de gestão sujeitos a consistência 11

6.2. Requisitos funcionais mínimos, objetivos e mensuráveis 11

6.3. Tratamento de dados pessoais (LGPD) 11

7. Especificação Funcional da Solução 12

7.1. Métricas objetivas e evidências de conformidade 13

8. Modelo de Julgamento e Critérios de Aceitação 14

9. Gestão de Riscos da Contratação 14

10. Matriz de Mitigação de Riscos de Impugnação 17

11. Estimativa de Custos e Pesquisa de Preços 18

12. Conclusão e Recomendação 19

Referências 20

Anexo I — Pesquisa de Preços Públicos Consolidada no ETP 21

Numeração de páginas referente a esta versão do documento; poderá deslocar-se levemente após o preenchimento dos campos assinalados entre colchetes.

1. APRESENTAÇÃO E PREMISSAS

Este documento constitui a sustentação técnica destinada a fundamentar, perante a área técnica, a área jurídica e os órgãos de controle, a contratação de solução de microssegmentação por software baseada em agente instalado no sistema operacional dos ativos protegidos, independente de hipervisor, de hardware de rede e de provedor de nuvem, gerenciada por console única, para o ambiente híbrido do Banco da Amazônia — data centers próprios, nuvem pública, plataforma de contêineres, servidores de banco de dados dedicados e estações de trabalho.

O texto reorganiza, na estrutura de nota técnica adotada como modelo, o conteúdo do Estudo Técnico Preliminar (ETP) e do Anexo de Especificações Técnicas da contratação. Os campos entre colchetes (ex.: "[PREENCHER]", "[CALIBRAR]", "[DEFINIR]") devem ser completados pela equipe de planejamento com os dados concretos do processo. Os quantitativos técnicos têm como base provisória o inventário da área de infraestrutura de 30/09/2026 e a capacidade de referência de 5.000 ativos, e deverão ser reconciliados com a exportação formal do inventário antes do edital.

Duas condicionantes permanecem abertas e afetam o dimensionamento: (i) a inclusão definitiva das estações de trabalho depende da validação do inventário e da comparação do custo total de propriedade (TCO) de 60 meses com o firewall de host da solução de EDR já contratada; e (ii) a compatibilidade com o Oracle Exadata depende das versões de Oracle Linux, UEK e Exadata System Software e da admissibilidade da instalação pela Oracle. Se a Oracle não admitir o agente nos 11 *database servers*, o item 1 será reduzido em 11 unidades e a cobertura indireta desses ativos deverá ser explicitada.

> *Premissa metodológica: este documento não substitui o ETP, o Termo de Referência (TR), o mapa de riscos nem a pesquisa de preços exigidos pela Lei nº 13.303/2016 e pelo Regulamento de Licitações e Contratos (RLC) do Banco — ele fornece a fundamentação técnica que embasa as escolhas de arquitetura e os requisitos que deverão constar desses instrumentos, especialmente a abordagem por agente, a console única, o lote único e a aplicação local e autônoma das regras de proteção. Não são importados para esta contratação benchmarks, limiares de eficácia ou fundamentos próprios de soluções de proteção de aplicações web.*

2. OBJETO

Fornecimento, implantação e suporte técnico especializado de solução de microssegmentação por software baseada em agente, com vigência contratual única de 60 (sessenta) meses e ativação por ondas, contemplando, de forma nativamente integrada:

- **Agente no sistema operacional:** aplicação local das regras de proteção em servidores físicos e virtuais, instâncias em nuvem pública (OCI e Azure), nós da plataforma OpenShift, *database servers* do Oracle Exadata e estações de trabalho, independentemente do hipervisor, do hardware de rede e do provedor de nuvem;
- **Visibilidade e mapa de dependências:** registro das comunicações entre ativos, com identificação de processo, serviço e usuário, para construção de regras baseadas no comportamento real das aplicações;
- **Regras por rótulos e menor privilégio:** modelo de lista de permissão por escopo, com simulação de impacto, aplicação gradual, versionamento, reversão e exceções temporárias;
- **Contenção de incidentes:** isolamento de ativo ou grupo pela console e por API integrada ao ServiceNow SIR, preservando o canal de investigação;

- **Console única de gerenciamento:** administração, rotulagem, regras, eventos e relatórios de todos os tipos de ativo em uma única console, em modelo SaaS ou *on-premises*;
- **Serviços associados:** planejamento, implantação, integração e homologação; operação assistida por 90 dias; capacitação oficial de 12 profissionais; suporte técnico especializado 24x7 por 60 meses; atualizações; e transição de saída.

Os itens possuem preços próprios dentro do lote, conforme o Quadro 2.1. O banco de horas é opcional e somente integrará o fornecimento após a definição de quantidade fundamentada.

Quadro 2.1 — Itens da contratação

Item	Descrição	Unidade	Qtd.	Pagamento
1	Subscrição de microssegmentação por agente — servidor (físico, virtual ou instância em nuvem), 60 meses	Servidor	863	Mensal, pelas licenças ativadas
2	Subscrição de microssegmentação por agente — nó de cluster OpenShift (de trabalho, de controle e de infraestrutura), 60 meses	Nó	71	Mensal, pelas licenças ativadas
3	Subscrição de microssegmentação por agente — estação de trabalho (desktop ou notebook), 60 meses	Estação	4.066	Mensal, pelas licenças ativadas
4	Planejamento, implantação, integração e homologação	Serviço	1	Por marco aceito
5	Operação assistida (90 dias)	Serviço	1	Ao término, com relatório aceito
6	Capacitação técnica oficial e transferência de conhecimento	Vaga	12	Após emissão dos certificados
7	Suporte técnico especializado 24x7	Mês	60	Mensal, com glosa por nível de serviço

3. FUNDAMENTAÇÃO LEGAL E NORMATIVA

A presente sustentação observa o ordenamento jurídico aplicável às contratações do Banco da Amazônia, sociedade de economia mista, e a regulação de segurança cibernética das instituições financeiras, notadamente:

3.1. Lei nº 13.303/2016 (Lei das Estatais) e Regulamento de Licitações e Contratos do Banco

- Regime aplicável — as contratações do Banco regem-se pela Lei nº 13.303/2016 e pelo RLC, e não pela Lei nº 14.133/2021, cujos dispositivos citados em modelos de outros órgãos não se aplicam automaticamente à estatal;
- Art. 32, inciso III — parcelamento do objeto quando tecnicamente viável e economicamente vantajoso, base da justificativa de lote único com itens de preço próprio apresentada na Seção 5;

- Modalidade e julgamento — seleção do fornecedor por pregão eletrônico, com critério de menor preço global do lote, observados requisitos técnicos objetivos, critérios de aceitabilidade de preços global e unitários, comprovação de capacidade técnica, Prova de Conceito com resultado binário (atende/não atende), critérios de aceite e níveis de serviço compatíveis com a criticidade do objeto.

3.2. Referenciais metodológicos de planejamento e pesquisa de preços

A Instrução Normativa SEGES/ME nº 65/2021 é adotada como referencial metodológico para a pesquisa de preços, condicionado à sua compatibilidade com o RLC, e não como obrigação automática da estatal. Referências de preço com mais de um ano exigem exame de execução, vigência e atualidade, e a idade dos preços não foi corrigida por índice arbitrário. As normas gerais citadas em modelos de proteção de aplicações (como a IN SGD/ME nº 94/2022) não são tratadas como regime aplicável ao Banco, podendo ser consultadas apenas como boa prática quando compatíveis com o RLC.

3.3. Lei Geral de Proteção de Dados Pessoais — LGPD (Lei nº 13.709/2018)

- Art. 46 — medidas de segurança técnicas e administrativas aptas a proteger dados pessoais, fundamento dos requisitos de criptografia, controle de acesso e trilha de auditoria da própria solução (Seção 6.3);
- Arts. 33 e seguintes — transferência internacional de dados, que exige, no modelo SaaS, declaração da localização de processamento e armazenamento, dos suboperadores e do mecanismo de transferência adotado;
- Art. 49 — sistemas de tratamento estruturados para atender aos requisitos de segurança e aos padrões de boas práticas e governança, com direito de auditoria do Banco sobre o ambiente do fornecedor.

3.4. Regulação de segurança cibernética e referenciais técnicos

A solução contribui para o atendimento à Resolução CMN nº 4.893/2021, com a redação dada pela Resolução CMN nº 5.274/2025 — em especial ao art. 3º, § 11, I (segmentação de rede) e à parcela lógica do isolamento dos ambientes Pix e STR prevista no art. 3º-A —, à LGPD e às políticas internas do Banco. Em SaaS, aplicam-se ainda as exigências da mesma Resolução sobre contratação de serviços de processamento e armazenamento de dados em nuvem, inclusive o acesso do Banco Central.

O NIST Cybersecurity Framework 2.0 e os CIS Critical Security Controls v8 são referenciais voluntários de boas práticas, utilizados para demonstrar a aderência técnica da solução; não constituem obrigação legal nem critério de julgamento. A matriz completa por requisito consta do Anexo de Especificações Técnicas. A solução contribui, em seu perímetro funcional, para as medidas de segurança do art. 46 da LGPD e, se houver escopo, para a segmentação exigida pelo PCI DSS, mas não assegura, isoladamente, a conformidade com essas normas.

3.5. Controle da competitividade e fundamentação da modelagem

- Súmula TCU nº 247 — adjudicação por item quando o objeto for divisível, ressalvada a hipótese de prejuízo para o conjunto ou perda de economia de escala; a modelagem adotada preserva itens com preço próprio dentro de lote único (Seção 5.2);

- Consulta ao mercado — as contratações públicas registradas no ETP evidenciam a existência de fornecimento público da solução e dos serviços, mas não comprovam, por si, que cada fornecedor possa atender a todo o escopo do Banco. O lote único, a console única e a eventual vedação a consórcio deverão ser confirmados pela consulta ao mercado, com verificação de competitividade e justificativa segundo o RLC;
- Fontes autorizadas — não se reproduzem acórdãos ou fundamentos específicos de proteção de aplicações web que não integrem as fontes do planejamento desta contratação.

4. CONTEXTUALIZAÇÃO TÉCNICA DA NECESSIDADE

4.1. Da movimentação lateral e da aplicação do menor privilégio

O cenário de referência é um incidente de *ransomware* com propagação lateral a partir de uma estação ou de um servidor comprometido, alcançando servidores de aplicação, bancos de dados e a infraestrutura de backup. A segurança de rede atual concentra-se no perímetro e na separação entre macrozonas; dentro de cada zona, os ativos comunicam-se com pouca restrição. Deverão ser estimados, com a área de riscos, as horas de indisponibilidade dos canais e sistemas críticos, o custo de recuperação, o impacto em transações e clientes e a exposição regulatória e reputacional [PREENCHER com GERIS e GPROD].

Dentro de seu perímetro funcional, a solução contribuirá para mitigar:

- movimentação lateral após comprometimento inicial;
- propagação de *ransomware* entre estações, entre estações e servidores e até a infraestrutura de backup;
- acesso indevido entre ambientes de produção e não produção, inclusive entre os clusters de produção e de qualidade do Exadata;
- exposição de serviços administrativos (RDP, SSH, WinRM) a origens não autorizadas;
- violação do isolamento de ambientes regulados (Pix, STR/RSFN);
- exfiltração a partir de ambientes sensíveis, como a máquina virtual do projeto de IA.

A microssegmentação reduz a probabilidade de propagação e o número de sistemas afetados, e não a probabilidade do comprometimento inicial. A solução não substitui EDR, gestão de vulnerabilidades, backup, recuperação de desastres ou ZTNA, e não lhe serão atribuídos benefícios fora desse perímetro sem demonstração da relação técnica.

4.2. Da cobertura híbrida e da autonomia da aplicação das regras

A solução deverá proteger, sob console única e com aplicação local das regras, servidores virtuais do ambiente hiperconvergente VMware vSphere 8.0.3 nos sites principal e de contingência, instâncias na Oracle Cloud Infrastructure e no Microsoft Azure, nós da plataforma Red Hat OpenShift, *database servers bare metal* do Oracle Exadata e estações de trabalho. O gerenciamento poderá ser oferecido em qualquer dos dois modelos, sem exigência de adoção simultânea:

- SaaS: nenhum componente local além dos agentes e, se necessário, de conectores ou coletores leves, com declaração de localização de dados, suboperadores e transferência internacional (Seção 6.3);

- *On-premises*: a proposta deverá listar os recursos de infraestrutura exigidos (vCPU, memória, disco e rede), que serão providos pelo Banco, com alta disponibilidade entre os sites.

Soma-se a essas razões um requisito de **autonomia e continuidade da proteção**: a aplicação das regras deve permanecer ativa, com a última regra válida, quando houver perda de comunicação entre o agente e a console, com comportamento seguro em falha configurável por grupo, sem bloquear o tráfego legítimo nem liberar indevidamente o tráfego. Não é aceitável que a proteção dos ativos críticos dependa da disponibilidade contínua da console ou da conectividade com o provedor do serviço. Esse requisito é operacionalizado nas Seções 6.2 e 7.1.

Os 18 hosts físicos do ambiente hiperconvergente, os 4 servidores físicos de backup de terceiro, as interfaces de gerenciamento e os *storage cells* do Exadata não recebem agente. A proteção indireta (*ring-fencing*) atua sobre as comunicações originadas ou destinadas a ativos com agente; não protege diretamente o equipamento sem agente nem controla fluxos entre dois ativos sem agente. Os cerca de 9.990 contêineres, 55 CDBs e 195 instâncias de banco são contexto de operação, e não unidades adicionais de licença.

Quadro 4.1 — Ambiente tecnológico de referência

Ambiente	Dado informado	Fonte
HCI VMware vSphere 8.0.3 (vCenter)	18 hosts físicos (9 no site principal e 9 no de contingência); cerca de 800 VMs em produção, homologação e desenvolvimento, sem contar as cópias de replicação	GPROD, 30/09/2026
OpenShift	4 clusters: produção 18 nós; contingência 25; qualidade/homologação 19; gerenciamento (ACM) 9 — total de 71 nós, incluindo *masters* e infraestrutura. Os 62 nós de produção, contingência e qualidade são VMs no vCenter; os 9 do ACM são VMs na OCI. Cerca de 9.990 contêineres	GPROD, 30/09/2026
OCI	132 VMs (122 em execução, incluindo os 9 nós do ACM, e 10 paradas)	GPROD, 30/09/2026
Azure	1 VM, dedicada a projeto de IA	GPROD, 30/09/2026
Oracle Exadata	3 clusters RAC *bare metal*: produção 4 e qualidade 3 *database servers* (matriz); contingência 4 (site de backup). 55 CDBs e 195 instâncias	GPROD, 30/09/2026
Backup	Solução contratada como serviço: 2 racks com 2 servidores físicos cada, de propriedade do fornecedor	GPROD, 30/09/2026
Estações de trabalho	Desktops e notebooks — quantidade por tipo, sistema operacional, localização e regime de uso (rede corporativa, remoto)	Área demandante; inventário de estações

4.3. Do risco de operação fragmentada

Licenças, implantação, operação assistida e suporte são tecnicamente interdependentes: as regras são construídas sobre os mapas de comunicação gerados pelos próprios agentes, a implantação depende do conhecimento do produto ofertado e o suporte responde pelo funcionamento da mesma plataforma. A contratação de fornecedores ou consoles distintos para essas parcelas produziria riscos concretos: (i) diluição da responsabilidade por bloqueios indevidos e por falhas de proteção; (ii) ampliação dos pontos

de integração entre ferramentas; (iii) divergência de rótulos, regras e registros entre ambientes; e (iv) duplicidade de esforço de administração, capacitação e auditoria. Esses riscos fundamentam, no plano técnico, a console única e o lote único tratados na Seção 5.

4.4. Da console única, do fabricante único e do lote único

Decorre dos riscos apontados na Seção 4.3 a conveniência de que a solução seja gerenciada por console única para todos os tipos de ativo, com todos os componentes do mesmo fabricante, para garantir regras, rótulos e telemetria consistentes entre data center, nuvem, plataforma de contêineres e estações de trabalho. A combinação de produtos de fabricantes distintos exigiria integração e manutenção contínua de camada intermediária pelo Banco ou por terceiro, fragilizaria a cadeia de suporte e comprometeria a rastreabilidade em caso de incidente.

Essa exigência é **estritamente funcional e arquitetural**, não indica marca e não impõe simultaneamente os modelos SaaS e *on-premises*. Ela será mantida somente se a consulta ao mercado confirmar que múltiplos fabricantes a atendem (Seção 5.4).

Por identidade de razões, a aquisição deve ser realizada em **lote único**, exclusivo de microssegmentação e de seus serviços diretamente associados, com itens de preço próprio. A separação em lotes permitiria a adjudicação a integradores diferentes para itens tecnicamente interdependentes, dificultando a apuração de responsabilidade em caso de falha. As contratações públicas de microssegmentação registradas no planejamento reuniram licenciamento e serviços associados sob um mesmo fornecedor (Quadro 4.2).

Quadro 4.2 — Contratações públicas de microssegmentação com licenças e serviços sob o mesmo fornecedor

Órgão / instrumento	Composição do objeto	Fornecedor
PRODEB — ARP 002/2025	Servidores, nós, implantação e capacitação, em ata de 36 meses de cobertura	Comdados
PCDF — Contrato 48/2026	Servidores, *endpoints*, Kubernetes, instalação e capacitação, em contrato único	INB
ANM — PE 90005/2026 / Contrato 47/2026	Servidores, nós, *endpoints*, implantação, turma de capacitação e suporte mensal	INB
MPSC — PE 17/2024	Servidores, *endpoints*, Kubernetes e configuração	PTLS

> *Os casos acima evidenciam que o mercado público tem contratado licenças e serviços de microssegmentação de forma conjunta; a estrutura de lotes de cada edital deverá ser confirmada nos documentos-fonte antes de sua citação como precedente. Recomenda-se que a equipe de planejamento junte aos autos os documentos referenciados no Anexo I, para uso complementar pela assessoria jurídica.*

5. JUSTIFICATIVA TÉCNICA PARA CONTRATAÇÃO EM PLATAFORMA ÚNICA

Nos termos do art. 32, inciso III, da Lei nº 13.303/2016, do RLC do Banco e da Súmula TCU nº 247, a opção por não parcelar o objeto em lotes — isto é, por exigir que subscrições, implantação, operação assistida, capacitação e suporte sejam entregues sob uma única solução e um único contratado — deve ser tecnicamente demonstrada, e não apenas afirmada. Apresenta-se a seguir essa demonstração.

5.1. Sistema integrado e interdependência técnica

A visibilidade, as regras e a contenção dependem de um plano de controle comum: os mapas de dependências produzidos pelos agentes alimentam a recomendação de regras; as regras aprovadas são distribuídas pela mesma console a todos os tipos de ativo; e a contenção acionada pelo SOC ou pelo ServiceNow SIR depende da mesma API. A contratação fracionada exigiria que o Banco integrasse e arbitrasse produtos e prestadores distintos, sem que nenhum deles assumisse a responsabilidade pelo resultado final. Nesse cenário, o parcelamento representaria risco técnico ao conjunto da solução.

5.2. Transparência de preços e eficiência de gestão contratual

O parcelamento foi tratado pela segregação em itens com preço próprio dentro do mesmo lote — subscrição por unidade de licenciamento, implantação, operação assistida, capacitação, suporte e banco de horas —, o que preserva a transparência de preços e a fiscalização por item sem fragmentar a responsabilidade técnica. A gestão de um único contrato, com um único conjunto de níveis de serviço e de canais de suporte, reduz o custo de gestão contratual, o número de pontos de contato na resposta a incidentes e a necessidade de capacitação em múltiplas interfaces.

O lote será exclusivo de microssegmentação e de seus serviços diretamente associados, evitando o agrupamento de produtos sem interdependência técnica. Preços ou percentuais de desconto de outras licitações, isoladamente, não demonstram a intensidade da competição nem justificam a modelagem do lote.

5.3. Preservação da competitividade — requisito funcional, não marca

As marcas citadas nos requisitos identificam componentes do ambiente do Banco com os quais a solução deve interoperar (por exemplo, EDR, vCenter, ServiceNow, OCI, Azure e Oracle Exadata); não indicam preferência quanto ao fabricante da solução. A exigência de console única é **funcional e de arquitetura** e será mantida somente se a consulta ao mercado confirmar que múltiplos fabricantes a atendem. As provas de conceito realizadas anteriormente pelo Banco não escolhem fabricante nem dispensam a verificação objetiva da solução ofertada no certame.

5.4. Consulta ao mercado e validação das alternativas

O estudo de alternativas do ETP concluiu que a plataforma de microssegmentação por software baseada em agente é a única abordagem que atende, no conjunto, à cobertura híbrida (vSphere, OCI, Azure, OpenShift, Exadata e estações de trabalho), com granularidade por processo, simulação, contenção integrada e regras e console únicas, observadas a compatibilidade do agente com o Exadata (AGT-12) e a comparação de custo das estações com o EDR. Por atuar no sistema operacional, de forma independente do hipervisor, do hardware de rede e do provedor de nuvem, a abordagem também reduz a dependência tecnológica e preserva a possibilidade de troca de infraestrutura ao longo dos 60 meses.

Quadro 5.1 — Modelos de microssegmentação avaliados

Modelo	Características e vantagens	Limitações e riscos	Enquadramento
Baseado em agente no ativo (software)	Granularidade por processo e identidade; independente de hipervisor, rede e nuvem; cobre VM, *bare metal*, nuvem, nós de contêiner e estações, inclusive fora da rede corporativa	Gestão do ciclo de vida dos agentes; dependência de suporte a sistemas operacionais; convivência com outros agentes	Objeto da contratação
Sem agente (orquestração remota do firewall do SO)	Menor pegada; compatível com legados	Menor granularidade; sem identificação de processo; depende de credenciais privilegiadas e do firewall nativo	Descartado como modelo principal; ativos que não admitem agente são protegidos por *ring-fencing*
Baseado em rede/*fabric* (SDN, *switches*, DPU)	Sem software no servidor	Depende de hardware específico; granularidade por segmento; não cobre nuvem pública nem processo	Descartado; a solução de rede em uso permanece na segmentação de macrozonas, de forma complementar
Baseado em hipervisor (firewall distribuído)	Baixa latência; integração nativa com a virtualização	Restrito ao ambiente virtualizado; não cobre OCI, Azure nem *bare metal*; dependência do licenciamento do hipervisor	Descartado; o recurso implantado e não utilizado não integra a solução
Nativo de nuvem e de Kubernetes	Sem custo adicional de licença	Regras dispersas em várias consoles; sem mapa de dependências unificado	Descartado como solução; *security groups* e *NetworkPolicies* seguem como controles de base

Quadro 5.2 — Fabricantes da abordagem por agente identificados no planejamento

Fabricante / linha de produto	Presença nas contratações públicas consultadas	Pontos a confirmar na consulta ao mercado
Akamai — Guardicore Segmentation	Sim — PRODEMGE (PE 013/2025) e MPSC (PE 17/2024)	Cobertura de Exadata e estações; métrica de nó OpenShift; modelo SaaS ou *on-premises*
Illumio — Core / Endpoint	Não identificada nas fontes do planejamento	Idem; presença de integradores no Brasil
Cisco — Secure Workload	Não identificada nas fontes do planejamento	Idem; cobertura de estações de trabalho
ColorTokens — Xshield	Não identificada nas fontes do planejamento	Idem; presença de integradores no Brasil
Outros fabricantes da abordagem por agente (ex.: TrueFort, Unisys)	Não identificada nas fontes do planejamento	Aderência ao escopo híbrido e às estações

Fabricante / linha de produto	Presença nas contratações públicas consultadas	Pontos a confirmar na consulta ao mercado
Fabricantes de PCDF, ANM e PRODEB	Sim — fornecedores INB e Comdados	Identificação do fabricante e da edição ofertados

Este estudo é preliminar e ilustrativo da pluralidade de mercado — não é lista exaustiva nem fechada. A equipe de planejamento deve: (i) confirmar e atualizar estes dados na consulta ao mercado, com convite amplo a fabricantes da abordagem por agente; (ii) verificar, para cada fabricante, a capacidade de atender ao lote, ao Exadata e às estações sem restrição indevida; e (iii) manter a pesquisa e suas fontes anexadas ao processo. Este estudo é evidência de diligência para o processo administrativo e não deve ser transcrito ao edital, cuja especificação permanece estritamente funcional.

6. REQUISITO CENTRAL: CONSISTÊNCIA DE REGRAS E APLICAÇÃO LOCAL

A consistência das regras entre todos os tipos de ativo e a aplicação local e autônoma pelos agentes são os requisitos técnicos que viabilizam, na prática, a console única justificada na Seção 5. Sem eles, a coexistência de ambientes distintos seria apenas nominal. Esta seção define o que deve permanecer consistente, com quais garantias mínimas, e como o tratamento de dados pessoais atende à LGPD. A exigência de sincronismo de inteligência entre duas modalidades de WAF, própria do modelo de referência, não é transposta para esta contratação.

6.1. Objetos de gestão sujeitos a consistência

- Regras de proteção, exceções e versões, distribuídas pela console a todos os agentes afetados;
- Rótulos e taxonomia de classificação dos ativos, inclusive os importados por conectores (vCenter, OCI, Azure, OpenShift);
- Inventário de ativos protegidos e de ativos sem agente descobertos a partir dos fluxos;
- Eventos, fluxos de comunicação e alertas, para correlação e envio ao SIEM;
- Trilha de auditoria das ações administrativas, de contenção e de exportação.

6.2. Requisitos funcionais mínimos, objetivos e mensuráveis

Recomenda-se que o Termo de Referência fixe parâmetros objetivos e verificáveis, de modo a permitir avaliação binária (atende/não atende) na Prova de Conceito ou no aceite, reduzindo a margem de subjetividade que pode ser explorada em impugnação:

Requisito	Especificação mínima de referência	Base / validação
Aplicação sem console (ARQ-03)	Última regra válida mantida na perda de comunicação com a console; comportamento seguro em falha configurável por grupo	PoC (MC02)
Canal agente–console (ARQ-06)	TLS 1.2 ou superior, com autenticação mútua ou mecanismo equivalente de identidade do agente	Documentação conforme Anexo I
Propagação de regras (DES-03)	Alteração aplicada aos agentes afetados em até 5 minutos [CALIBRAR]	PoC com método fixado

Requisito	Especificação mínima de referência	Base / validação
Contenção (RES-01)	Isolamento de ativo ou grupo em até 60 segundos [CALIBRAR], preservando o canal de investigação (EDR, coleta forense, PAM)	PoC (MC19) e aceite
Regra acompanha o ativo (ARQ-11)	Regra por rótulo mantida quando o ativo muda de IP ou migra entre data center e nuvem, sem reescrita manual	PoC
Entrega ao SIEM (INT-02)	Eventos, fluxos e auditoria por Syslog (CEF/LEEF/JSON) e/ou API, com fila e reenvio em caso de falha	PoC (MC25)
Disponibilidade da console (ARQ-04)	SaaS: mínimo de 99,9% ao mês [CALIBRAR]; *on-premises*: cluster com *failover* automático e replicação entre os sites	Documentação e aceite

6.3. Tratamento de dados pessoais (LGPD)

- Minimização: a solução deve registrar metadados de comunicação (origem, destino, porta, processo, usuário) necessários à segurança, sem captura do conteúdo do tráfego (art. 6º, III, LGPD);
- Base legal e papéis: no modelo SaaS, o contrato deve qualificar o fornecedor como operador (art. 5º, VII, LGPD) e prever acordo de tratamento de dados com as obrigações do art. 39 e as medidas do art. 46;
- Localização e transferência internacional: declaração da localização de processamento e armazenamento, dos suboperadores e do mecanismo de transferência internacional adotado (arts. 33 e seguintes da LGPD), com criptografia em trânsito e em repouso;
- Direito de auditoria: previsão contratual de auditoria pelo Banco e de acesso do Banco Central, nos termos da Resolução CMN nº 4.893/2021;
- Retenção: definida por classe de registro (auditoria administrativa, fluxos, alertas), na própria solução ou no SIEM, conforme a política do Banco, sem retenção indiscriminada, com exportação integral e eliminação segura ao término do contrato.

7. ESPECIFICAÇÃO FUNCIONAL DA SOLUÇÃO

Os requisitos abaixo resumem, em termos funcionais e de desempenho, os 104 requisitos do Anexo de Especificações Técnicas, sem menção a marca, modelo ou fabricante da solução. A classificação (obrigatório ou desejável) e o método de comprovação de cada requisito devem ser preservados na RFP e no edital; os requisitos desejáveis não se convertem em eliminatórios.

Grupo	Requisito funcional mínimo	Referência
Arquitetura e implantação	Agente no SO de cada ativo, independente de hipervisor, rede e nuvem; console SaaS ou *on-premises*; aplicação autônoma sem console; alta disponibilidade; regras que acompanham o ativo	ARQ-01 a ARQ-11
Console e administração	SSO com MFA; RBAC por papel e escopo; trilha de auditoria completa; integração com PAM; atualização dos agentes pela console, em lotes e com reversão	GER-01 a GER-09

Grupo	Requisito funcional mínimo	Referência
Agentes	Versões de Windows e Linux do inventário; instalação silenciosa em massa; consumo limitado de CPU e memória; convivência com EDR e demais agentes; proteção contra adulteração; remoção sem regras residuais; compatibilidade com o Exadata	AGT-01 a AGT-12
Ativos sem agente	Cadastro, rotulagem e proteção indireta (*ring-fencing*) de ativos que não admitem agente; descoberta a partir dos fluxos	SAG-01 e SAG-02
Contêineres	Visibilidade e regras em OpenShift e Kubernetes; licenciamento por nó, sem cobrança por contêiner; convivência com o CNI e as *NetworkPolicies*	CNT-01 a CNT-04
Estações de trabalho	Agente na mesma console; bloqueio padrão de SMB, RDP e WinRM entre estações; regras fora da rede corporativa; isolamento via ServiceNow SIR	EST-01 a EST-09
Nuvem	Conectores OCI e Azure para inventário e *tags*; proteção por agente independente do provedor	NUV-01, NUV-02 e NUV-04
Visibilidade	Mapa de dependências em tempo quase real e histórico; fluxos com processo; simulação; retenção consultável e exportação em formato aberto	VIS-01 a VIS-07
Rotulagem	Rótulos multidimensionais (ambiente, aplicação, função, localização, criticidade, marcador regulatório); rotulagem automática	ROT-01 a ROT-03
Regras e aplicação	Lista de permissão por rótulo; regras por IP, FQDN, porta, processo e identidade; recomendação, simulação, aplicação gradual, versionamento, aprovação e exceções temporárias	POL-01 a POL-14
Resposta e contenção	Isolamento pela console e por API; acionamento pelo SOAR/ServiceNow SIR; alertas de violação	RES-01 a RES-04
Integrações e API	API REST documentada; SIEM com fila e reenvio; AD/Entra ID; vCenter; ITSM e automação	INT-01 a INT-06
Registros e governança de dados	Sincronização de tempo; proteção dos registros; retenção por classe; requisitos de SaaS; exportação e eliminação ao término	LOG-01 a LOG-05
Desempenho e capacidade	Capacidade para 5.000 ativos com limites documentados; propagação de regras; impacto máximo na latência	DES-01 a DES-04
Segurança da solução	Desenvolvimento seguro; certificações do provedor SaaS; *hardening* documentado	SEG-01 a SEG-04
Relatórios e licenciamento	Relatórios de cobertura e de segregação; licenciamento segregado por tipo de ativo, realocável, com atualizações garantidas	REL-01 a REL-03; LIC-01 a LIC-04

Recomenda-se prever, no TR, Prova de Conceito para verificação objetiva do atendimento aos requisitos acima antes da adjudicação, aberta ao licitante provisoriamente classificado em primeiro lugar e, sucessivamente, aos demais, com roteiro público e critério binário, evitando o vício de restrição de competitividade.

7.1. Métricas objetivas e evidências de conformidade

Para reduzir a subjetividade na aferição dos requisitos, recomenda-se que o TR fixe os limiares abaixo, calibrados com a consulta ao mercado e medidos com metodologia definida pelo Banco:

Métrica	Limiar de referência	Meio de comprovação
Consumo do agente em servidores	CPU média < 5% e memória < 10% em carga representativa [CALIBRAR, inclusive valor absoluto em MB], respeitando limites configuráveis pelo Banco	PoC (MC06) e aceite (AGT-04)
Impacto na latência	Degradação da latência p95 das transações de teste ≤ 5% frente à linha de base, sob carga equivalente e com a regra aplicada [CALIBRAR]	PoC (MC06) (DES-04)
Propagação de regras	≤ 5 minutos [CALIBRAR]	PoC (DES-03)
Tempo de contenção	≤ 60 segundos [CALIBRAR]	PoC (MC19) (RES-01)
Retenção de fluxos na console	≥ 90 dias, com exportação para o SIEM ou repositório corporativo [CALIBRAR com a política de retenção]	Documentação (VIS-03)
Cobertura após a implantação	Agentes em, no mínimo, 98% dos servidores e nós em modo de visibilidade no marco M4	Aceite do marco
Disponibilidade da console SaaS	≥ 99,9% ao mês [CALIBRAR]	Relatório mensal (Anexo II)

> *Os limiares acima são parâmetros de partida. Antes do edital, deverão ser fixados as versões de SO, de UEK e do OpenShift, os limites de CPU e memória, a taxa de fluxos, a retenção, o limiar p95, os tempos de propagação e contenção, os critérios de glosa, a aplicação dos testes de Exadata e de estações e a duração dos períodos de medição. Marcadores de calibração não podem permanecer como critérios eliminatórios indeterminados. Não se importam percentuais de eficácia OWASP, benchmarks de laboratório ou limiares de proteção de aplicações, que não compõem o objeto.*

8. MODELO DE JULGAMENTO E CRITÉRIOS DE ACEITAÇÃO

Recomenda-se a adoção de pregão eletrônico com critério de julgamento pelo menor preço global do lote, nos termos da Lei nº 13.303/2016 e do RLC, com especificação técnica mínima objetiva (modelo binário atende/não atende), critérios de aceitabilidade de preços global e unitários e comprovação de capacidade técnica. Esse critério, associado a especificações funcionais claras, oferece menor margem a alegações de subjetividade ou de direcionamento.

O licitante provisoriamente classificado em primeiro lugar apresentará tabela ponto a ponto com o número do requisito, a descrição, o documento comprobatório, o endereço eletrônico (URL), a página ou seção e o trecho transcrito. Documentos internos ou inacessíveis ao Banco não serão aceitos. A Prova de Conceito verificará os requisitos críticos em laboratório do Banco isolado da produção, com 30 casos de teste e critério binário de aprovação, conforme o Anexo III.

A aceitação definitiva estará condicionada à homologação por onda, com casos de teste, critérios objetivos, evidências, responsáveis e procedimento de reversão. São testes obrigatórios: funcionamento das aplicações sem regressão; consumo de recursos do agente (AGT-04); comportamento sem console (ARQ-03); contenção e liberação (RES-01); integridade dos registros no SIEM (INT-02); *failover* da console *on-premises*, se aplicável (ARQ-04); e remoção limpa do agente (AGT-09). A homologação não se confunde com a Prova de Conceito nem substitui testes de intrusão independentes.

Quadro 8.1 — Níveis de serviço de referência para o suporte

Severidade	Definição	Atendimento	Contorno	Solução definitiva
1 — Crítica	Bloqueio indevido de tráfego em produção; falha massiva de agentes; indisponibilidade da console que impeça a contenção	1 h (24x7)	4 h	3 dias corridos, com plano de ação
2 — Alta	Degradação relevante; falha de integração com o SIEM ou o SIR; falha de agentes em grupo restrito	2 h (24x7)	8 h	10 dias corridos
3 — Média	Funcionalidade não crítica indisponível, com contorno	4 h úteis	72 h	30 dias corridos
4 — Baixa	Dúvida, configuração ou melhoria	4 h úteis	—	Resposta em até 15 dias corridos

9. GESTÃO DE RISCOS DA CONTRATAÇÃO

Os riscos abaixo reproduzem os eventos, probabilidades, impactos e medidas registrados no ETP, organizados por contratação, implantação e operação, dados e governança, e saída, e devem ser incorporados ao mapa de riscos do processo. Entre parênteses, indica-se o responsável pela medida.

Quadro 9.1 — Riscos da contratação

Risco	Probabilidade	Impacto	Mitigação proposta
A01 — Questionamento da escolha do modelo por agente, diante do recurso de virtualização implantado e da solução de rede em uso	Baixa	Média	Registrar a motivação da Seção 5.4 (cobertura de OCI, Azure e Exadata, granularidade por processo e console única); contingência: complementar a motivação na resposta a impugnações (Equipe de Planejamento / GPROD)
A02 — Exigências de agente, console única e lote único reduzem a competição	Média	Alta	Consulta ao mercado com no mínimo cinco fabricantes da abordagem por agente; requisitos neutros; contingência: flexibilizar exigências e republicar (Equipe de Planejamento / Contratações)
A03 — Pesquisa de preços com poucas referências homologadas ou escopos não comparáveis	Média	Alta	Cestas por unidade; propostas para 60 meses; acompanhar CAIXA e SERPRO; contingência: refazer a pesquisa antes da publicação (Equipe de Planejamento)
A04 — Laboratório insuficiente para a Prova de Conceito	Média	Média	Preparar laboratório com vSphere, OpenShift, OCI, Azure e ambiente equivalente ao Exadata; contingência: comprovação documental para itens não reproduzíveis (GPROD)
A05 — Inventário desatualizado ou crescimento não previsto	Média	Média	Validar no plano de implantação; quantitativo sob demanda; contingência: acréscimo contratual dentro do limite legal (GPROD)

Risco	Probabilidade	Impacto	Mitigação proposta
A06 — Inclusão das estações sem comparação com o firewall de host do EDR já contratado	Média	Alta	Comparar o custo total de 60 meses das duas opções; obter preço do item 3 na consulta; contingência: reduzir ou suprimir o item 3 antes do edital (Equipe de Planejamento)
A07 — Questionamento de direcionamento em razão das provas de conceito realizadas anteriormente	Média	Média	Requisitos por resultado; consulta ampla; Prova de Conceito com roteiro público e critério binário; registro das provas anteriores no processo; contingência: resposta fundamentada a impugnações (Equipe de Planejamento / Jurídico)

Quadro 9.2 — Riscos da implantação e da operação

Risco	Probabilidade	Impacto	Mitigação proposta
B01 — Bloqueio indevido de tráfego legítimo em produção, com indisponibilidade de serviço bancário	Média	Alta	Ondas; modo de visibilidade; simulação; aprovação dos responsáveis pelas aplicações; janelas de mudança; contingência: reversão imediata para visibilidade, severidade 1 (Contratada / GPROD)
B02 — Conflito do agente com o EDR ou outros agentes, com instabilidade de servidores	Baixa	Alta	Teste de convivência na Prova de Conceito e na Onda 0; contingência: retirada do agente do grupo afetado (Contratada)
B03 — Interferência no *interconnect* do RAC ou na rede de armazenamento do Exadata	Baixa	Alta	Exclusão das interfaces; teste específico; instalação em janela com a área de banco de dados; contingência: remoção do agente e proteção indireta (Contratada / GPROD)
B04 — Bloqueio da replicação entre produção e contingência do Exadata ou do backup	Baixa	Alta	Mapear e permitir explicitamente os fluxos de replicação e backup antes da aplicação das regras; contingência: reversão e revisão da regra (Contratada / GPROD)
B05 — Indisponibilidade da console SaaS	Baixa	Média	Aplicação local mantida (ARQ-03); nível de serviço de disponibilidade; contingência: operação em contingência e glosa (Contratada)
B06 — Baixo engajamento dos responsáveis pelas aplicações; regras permanecem em visibilidade	Média	Média	Governança com RACI; indicador de regras aprovadas; patrocínio da diretoria; contingência: escalonamento ao comitê competente (GESEC)
B07 — Proliferação de exceções permanentes	Média	Média	Exceções com expiração automática; revisão trimestral; contingência: auditoria de exceções (GESEC)
B08 — Consumo de recursos do agente acima do previsto em servidores críticos	Baixa	Alta	Limites de CPU e memória (AGT-04) medidos na Prova de Conceito e na Onda 0; contingência: ajuste de configuração, retirada do agente do grupo afetado e glosa (Contratada)

Risco	Probabilidade	Impacto	Mitigação proposta
B09 — Impacto do agente nas estações, com aumento de chamados na central de serviços	Média	Média	Grupo piloto; limites calibrados; instalação silenciosa; orientação à central de serviços; contingência: retirada do agente do grupo afetado e ajuste de regra (Contratada / GPROD)
B10 — Notebook fora da rede corporativa sem regra ou com regra que impeça o trabalho remoto	Média	Média	Perfis por localização testados na Prova de Conceito; regra mantida sem a console; contingência: reversão para visibilidade no grupo afetado (Contratada)
B11 — Sobrecarga das equipes de segurança e de infraestrutura na operação das regras	Média	Média	Recomendação automática de regras; aprovação delegada aos responsáveis pelas aplicações (POL-08); integração com ServiceNow; operação assistida; contingência: banco de horas opcional (GESEC / GPROD)

Quadro 9.3 — Riscos de dados e governança

Risco	Probabilidade	Impacto	Mitigação proposta
C01 — Telemetria em SaaS com dados pessoais tratada sem as salvaguardas da LGPD e da Resolução CMN nº 4.893/2021	Média	Alta	Cláusulas de localização, suboperadores, auditoria e acesso do Banco Central; contingência: suspender a integração e exigir adequação (GESEC / Jurídico)
C02 — Comprometimento da própria console, usada como ponto de controle privilegiado	Baixa	Alta	MFA, PAM, RBAC, trilha de auditoria e certificações do fornecedor; contingência: revogação de acessos e resposta a incidente (GESEC)
C03 — Atribuição à solução de conformidade que ela não assegura isoladamente	Baixa	Média	Delimitar o perímetro funcional e o grau de contribuição no ETP e no TR; contingência: revisão dos relatórios de conformidade (Equipe de Planejamento)
C04 — Nova alteração da Resolução CMN nº 4.893/2021 ou de norma de segurança durante a vigência	Média	Média	Atualização de versões garantida (LIC-04); relatórios configuráveis; API documentada; contingência: banco de horas para ajustes (GESEC / Jurídico)

Quadro 9.4 — Riscos de saída

Risco	Probabilidade	Impacto	Mitigação proposta
D01 — Término do contrato sem exportação de regras e sem remoção limpa dos agentes	Média	Alta	Plano de saída 90 dias antes do término; exportação periódica; contingência: retenção de pagamentos e execução da garantia (Gestor do contrato)
D02 — Descontinuidade do produto ou mudança de controle do fabricante	Baixa	Média	Declaração de ciclo de vida; obrigação de substituição sem ônus; contingência: plano de transição (Gestor do contrato)

Risco	Probabilidade	Impacto	Mitigação proposta
D03 — Dependência do fabricante dificulta a troca de solução ao fim da vigência	Média	Média	Exportação de rótulos, regras e registros em formato aberto (LOG-05); cessão de scripts e integrações; contingência: convivência temporária com a solução sucessora (Gestor do contrato)

10. MATRIZ DE MITIGAÇÃO DE RISCOS DE IMPUGNAÇÃO

Síntese, para uso da assessoria jurídica e da equipe de planejamento, das alegações de impugnação mais prováveis nesta contratação e do ponto do presente documento em que cada uma é enfrentada, a partir dos riscos do ETP e das condicionantes do Anexo de Especificações:

Possível alegação de impugnação	Onde é enfrentada neste documento	Medida antes do edital
Ausência de parcelamento restringe a competitividade	Seções 4.4, 5.1 e 5.2 — sistema integrado, itens com preço próprio e contratações públicas comparáveis	Confirmar na consulta múltiplos fabricantes e integradores aptos ao lote
Exigência de console única ou fabricante único direciona a contratação	Seções 4.4 e 5.3 — requisito funcional, mantido somente se confirmado pelo mercado	Registrar o resultado da consulta e, se necessário, flexibilizar a exigência
Abordagem por agente é desnecessária diante dos recursos já existentes	Seção 5.4 e Quadro 5.1 — comparação de modelos e cobertura híbrida	Registrar a motivação técnica e a informação da área de infraestrutura
Estações de trabalho duplicam o firewall de host do EDR	Seções 1 e 9 (risco A06) — condicionante de TCO e efetividade	Comparar efetividade e TCO; reduzir ou retirar o item 3, se apropriado
Exadata sem compatibilidade documentada	Seções 1, 4.2 e 7 (AGT-12)	Confirmar versões e admissibilidade pela Oracle; definir a cobertura indireta
Preços de referência incomparáveis	Seção 11 e Anexo I — classificação, normalização e limitações	Equalizar métricas, módulos, escala e serviços; obter propostas específicas
Prova de Conceito ou metas indeterminadas favorecem fornecedor	Seções 6.2, 7.1 e 8 — critérios binários e parâmetros a calibrar	Fixar aplicabilidade, limites, duração e evidências antes do edital
Provas de conceito anteriores indicam direcionamento	Seção 5.3 e risco A07	Registrar as provas anteriores no processo; manter roteiro público e consulta ampla

11. ESTIMATIVA DE CUSTOS E PESQUISA DE PREÇOS

Este documento não fixa valores definitivos, por não ser este o seu objeto e porque a estimativa deve refletir levantamento próprio e atual do processo. Como ponto de partida, o Anexo I apresenta as referências de preços públicos de microssegmentação consolidadas no ETP, com classificação,

normalização e ressalvas de comparabilidade. Os escopos de implantação, capacitação e suporte encontrados não formam faixa diretamente aplicável ao Banco. Recomenda-se que a equipe de planejamento:

- Solicite, na consulta ao mercado, propostas específicas para implantação híbrida, 90 dias de operação assistida, 12 vagas de capacitação e suporte especializado de 60 meses, separando o suporte do fabricante embutido na subscrição da sustentação local, para evitar dupla cobrança;
- Calcule o custo total de propriedade em 60 meses, contemplando subscrições, implantação, operação assistida, capacitação, suporte, infraestrutura da console *on-premises*, se for o caso, e eventuais integrações, com cronograma físico-financeiro por ondas de ativação;
- Instrua o orçamento formal com propostas válidas, data-base, *part numbers*, métricas, capacidade, suporte, custos de infraestrutura e tributos, justificação das exclusões, análise de independência das fontes e decisão fundamentada sobre o método estatístico.

Quadro 11.1 — Situação da estimativa por item

Item	Quantidade / unidade	Situação do preço
1 — Servidores	863 × 60 meses	Cotação equivalente pendente
2 — OpenShift	71 nós × 60 meses	Cotação pendente; apenas duas referências de nó
3 — Estações	4.066 × 60 meses, a confirmar	Cotação e comparação com o EDR pendentes
4 — Implantação	1 serviço integral	Equalizar entregas e obter cotação
5 — Operação assistida	1 serviço de 90 dias	Cotação específica pendente
6 — Capacitação	12 vagas	Equalizar carga horária e modalidade
7 — Suporte especializado	60 meses	Cotação; segregar o suporte já incluído na subscrição
8 — Banco de horas (opcional)	Quantidade com memória de cálculo	Sem quantidade ou preço definidos
Total da contratação	Licenças + serviços aplicáveis	Não consolidado; ausência de preço não é custo zero

12. CONCLUSÃO E RECOMENDAÇÃO

Com base na fundamentação técnica e normativa apresentada, conclui-se pela viabilidade, de forma condicionada ao cumprimento das condicionantes do item 16.17 do ETP, da contratação de solução de microssegmentação por software baseada em agente, em lote único com itens de preço próprio, sob console única, com vigência de 60 (sessenta) meses, mediante especificação estritamente funcional, consulta ampla ao mercado e demonstração expressa de que a não fragmentação do objeto preserva a integridade técnica da solução e a responsabilidade pelo resultado sem restringir indevidamente a competitividade.

A análise comparativa demonstra que a microssegmentação por software com agente é a alternativa que atende, no conjunto, à cobertura híbrida, à granularidade por processo, à simulação e à contenção integrada sob console única, observada a compatibilidade do agente com o Exadata (AGT-12). Recomenda-se que a equipe de planejamento prossiga com a consulta ao mercado, reconcilie o inventário e as versões, decida sobre as estações e o Exadata, consolide os parâmetros de níveis de serviço e de Prova de Conceito, obtenha preços comparáveis e confirme a competitividade e os recursos, previamente ao encaminhamento à assessoria jurídica. A viabilidade permanece condicionada: este documento não converte custos ausentes em zero nem decisões pendentes em requisitos definitivos.

REFERÊNCIAS

- BRASIL. Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais). Disponível em: planalto.gov.br.
- BANCO DA AMAZÔNIA S.A. Regulamento de Licitações e Contratos (RLC), versão vigente [CONFERIR].
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Disponível em: planalto.gov.br.
- CONSELHO MONETÁRIO NACIONAL. Resolução CMN nº 4.893, de 26 de fevereiro de 2021, com a redação dada pela Resolução CMN nº 5.274/2025. Disponível em: bcb.gov.br.
- BRASIL. Ministério da Economia. Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021 (referencial metodológico). Disponível em: gov.br/compras.
- TRIBUNAL DE CONTAS DA UNIÃO. Súmula TCU nº 247. Disponível em: pesquisa.apps.tcu.gov.br.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Cybersecurity Framework 2.0. Disponível em: nist.gov.
- CENTER FOR INTERNET SECURITY (CIS). CIS Critical Security Controls v8. Disponível em: cisecurity.org.
- BANCO DA AMAZÔNIA S.A. Estudo Técnico Preliminar — Microssegmentação, versão 6, especialmente seções 3, 4, 6 a 11, riscos e conclusão.
- BANCO DA AMAZÔNIA S.A. Anexo de Especificações Técnicas — Microssegmentação, versão 6: requisitos ARQ a LIC, serviços, matriz normativa e regras de fornecimento.
- Documentos de contratações públicas de microssegmentação listados no Anexo I, Seção I.4.

> *As fontes normativas e os documentos de contratações públicas citados são públicos e rastreáveis nos sítios oficiais indicados. As referências de preço foram transcritas do ETP, sem nova pesquisa ou atualização externa nesta elaboração.*

ANEXO I — PESQUISA DE PREÇOS PÚBLICOS CONSOLIDADA NO ETP

Este anexo apresenta as referências de preços praticados em contratações públicas de microssegmentação registradas no Portal Nacional de Contratações Públicas (PNCP) e em portais oficiais dos respectivos órgãos, consolidadas no ETP. Esta pesquisa constitui a parcela "contratações públicas similares" da estimativa de custos referida na Seção 11 e deve ser complementada, antes da instrução final do processo, por propostas formais obtidas na consulta ao mercado.

I.1. Metodologia e critérios de inclusão

- Classificação das fontes: A — contratado/registrado; B — homologado; C — estimado; P — comprovação ou equivalência pendente;
- Normalização das licenças: preço unitário × 12 ÷ prazo em meses. Para a PRODEB, cuja ata informa preço mensal, multiplica-se por 36 para a cobertura integral e por 12 para o equivalente anual. Essa conversão temporal não equaliza módulos, escala, tributação, modalidade de console, nível de serviço ou serviços;
- Regime: Lei nº 13.303/2016 e RLC do Banco, com a IN SEGES/ME nº 65/2021 como referencial metodológico condicionado. Referências com mais de um ano exigem exame de execução, vigência e atualidade; a idade do preço não foi corrigida por índice arbitrário; o desfecho de cada processo deve ser atualizado antes do edital;
- Tratamento estatístico: média, mediana, desvio-padrão amostral e coeficiente de variação são diagnósticos. Os cortes de 25% e 50% de coeficiente de variação não são limites normativos e não selecionam automaticamente o preço. Nenhuma mediana é convertida em orçamento formal sem demonstração de comparabilidade e decisão fundamentada;
- Independência: fontes com o mesmo fornecedor ou fabricante e contratos derivados de uma mesma ata não são presumidos independentes.

I.2. Registros identificados e valores de referência

Quadro I.1 — Base de cálculo (preços homologados, registrados ou contratados)

Órgão / instrumento	Situação	Fornecedor / fabricante	Itens e preços unitários	Prazo
PRODEMGE — PE 013/2025	Homologado; resultado no PNCP em 12/09/2025. R$ 8.108.000,00	Shield Security / Guardicore	1.000 servidores × R$ 8.108,00. O contrato derivado DM-286/2026 não gera nova observação de preço	24 meses
MPSC — PE 17/2024	Homologado em 22/11/2024. R$ 4.830.000,00	PTLS / Guardicore	400 servidores × R$ 8.932,25; 200 *endpoints* × R$ 1.488,70; 20 Kubernetes × R$ 37.218,00; configuração R$ 215.000,00. Métrica cluster/nó a confirmar	36 meses
PCDF — Contrato 48/2026	Assinado em 06/07/2026. R$ 1.891.514,00	INB / fabricante a confirmar	516 servidores × R$ 1.879,00; 5.000 *endpoints* × R$ 139,00; 21 Kubernetes × R$ 6.450,00; instalação R$ 39.000,00; 5 vagas × R$ 10.500,00	12 meses

Órgão / instrumento	Situação	Fornecedor / fabricante	Itens e preços unitários	Prazo
ANM — PE 90005/2026 / Contrato 47/2026	Homologado no PNCP em 23/06/2026; contrato R$ 2.562.600,00	INB / fabricante a confirmar	250 servidores × R$ 6.550,00; 12 nós × R$ 25.200,00; 200 *endpoints* × R$ 1.055,00; implantação R$ 220.000,00; turma R$ 84.300,00; suporte 12 × R$ 8.950,00	12 meses
PRODEB — PE 001/2025 / ARP 002/2025	Ata assinada em 12/02/2025. R$ 8.700.000,00	Comdados / fabricante a confirmar	500 servidores × R$ 348,23/mês; 50 nós × R$ 1.148,43/mês; implantação R$ 223.020,00 + R$ 65.353,00; 4 vagas × R$ 19.078,25	36 meses de cobertura

Quadro I.2 — Registros mantidos apenas como evidência qualitativa (excluídos da base de cálculo)

Órgão / instrumento	Objeto e valores	Motivo da exclusão
ALESP — PE 125/2026	Estimativa do edital R$ 9.958.271,19: 2.500 licenças mistas de 24 meses × R$ 3.522,31; implantação R$ 127.211,67; operação assistida R$ 26.942,00; suporte 21 × R$ 35.230,50	Homologação não confirmada; quantidade mista não forma preço de servidor ou de estação
SERPRO — PE 90227/2026	2.000 subscrições iniciais; teto de 12.000 conforme demanda; 36 meses	Orçamento sigiloso; preço final não confirmado (zero na API não representa preço gratuito)
SFB — PE 90006/2024	545 servidores × R$ 3.231,27; 6.747 estações × R$ 451,74; 12 meses	Somente estimativa confirmada; item de proteção em nuvem fora do objeto
TRT2 — Contrato 133/2024	R$ 464.168,96 de instalação e configuração de microssegmentação e antirransomware	Pacote com HCI, redes e serviços; não é preço de licença
SEEC/DF — PE 077/2023	Referência de controle: inventário, classificação e justificativa de necessidade e de preços	Fase externa cancelada; Decisão TCDF nº 4782/2024; não compõe cesta de preços
Salvador/SEMIT e CAIXA	Referências a diligenciar	Sem vinculação a resultado ou ata final e sem confirmação de escopo e métrica

Quadro I.3 — Preços normalizados de servidores

Referência	Preço / prazo	R$/servidor/ano	Escala	Limitação
PCDF	R$ 1.879,00 / 12 meses	1.879,00	516	Fabricante e modelo a confirmar
MPSC	R$ 8.932,25 / 36 meses	2.977,42	400	Marca e suporte específicos
PRODEMGE	R$ 8.108,00 / 24 meses	4.054,00	1.000	Marca; módulos e escopo a equalizar
PRODEB	R$ 348,23 por mês	4.178,76	500	Licença e suporte por 36 meses
ANM	R$ 6.550,00 / 12 meses	6.550,00	250	Menor escala; fabricante a confirmar

Quadro I.4 — Referências de estações de trabalho (endpoints)

Referência	R$/estação/ano	Escala	Limitação
PCDF	139,00	5.000	Cobertura e fabricante a confirmar
MPSC	496,23	200	36 meses; suporte do fabricante
ANM	1.055,00	200	12 meses; fabricante a confirmar

Nó OpenShift: PRODEB R$ 13.781,16/nó/ano (50 nós) e ANM R$ 25.200,00/nó/ano (12 nós). Há apenas duas observações com métrica de nó identificada, com mediana descritiva de R$ 19.490,58. A referência do MPSC (R$ 37.218,00 por 36 meses, equivalente a R$ 12.406,00/ano) fica fora da cesta de nó até o esclarecimento da métrica cluster versus nó no escopo comercial; PCDF (R$ 6.450,00 por 12 meses) e Salvador também dependem de equivalência. Não há correspondência automática entre nó, cluster, *pod* ou contêiner.

I.3. Tratamento estatístico e faixa de referência

As cinco observações de servidores do Quadro I.3 apresentam média de **R$ 3.927,84**, mediana de **R$ 4.054,00** e coeficiente de variação amostral de **44,20%**. São preços históricos de escopos distintos, mantidos para diagnóstico e análise de sensibilidade. As referências de estações apresentam coeficiente de variação amostral de 81,94%; a diferença de escala e de composição exige equalização, e as 4.066 estações do Banco são premissa residual, a validar e comparar com o firewall de host do EDR já contratado.

Cenário ilustrativo de subscrições, sem serviços: 863 servidores × R$ 4.054,00 × 5 anos + 71 nós × R$ 19.490,58 × 5 anos = **R$ 24.412.165,90**. Com 4.066 estações, o total passa a R$ 27.238.035,90 a R$ 139,00/ano; R$ 34.500.589,57 a R$ 496,23/ano; e R$ 45.860.315,90 a R$ 1.055,00/ano. A mediana de apenas duas observações de nó é ilustrativa. A extrapolação linear pressupõe ativação integral desde o início e não comprova desconto de 60 meses, reajuste ou custo global; a ativação por ondas deverá gerar cronograma físico-financeiro próprio.

Recomenda-se que a equipe de planejamento posicione a estimativa dentro das faixas acima somente após equalizar métricas, módulos, escala e serviços, evitando a aplicação mecânica de média entre objetos de escopo distinto. O mapa de preços mantém as fontes brutas, a normalização, os diagnósticos, a estimativa com entradas editáveis e os cenários; preços não informados exibem pendência e impedem um total aparentemente completo.

I.4. Fontes registradas no ETP

- PCDF — Contrato 48/2026, quadro de itens; 12 meses. https://pncp.gov.br/pncp-api/v1/orgaos/37115482000135/contratos/2026/144/arquivos/1
- PRODEB — ARP 002/2025, itens 1 a 6; cobertura de 36 meses. https://www.ba.gov.br/prodeb/sites/site-prodeb/files/migracao_2024/arquivos/repositorio-midias/documentos/2025-02/ATA_002_2025.pdf
- PRODEMGE — PE 013/2025, resultado do item 1. https://pncp.gov.br/pncp-api/v1/orgaos/16636540000104/compras/2025/27/itens/1/resultados

- MPSC — PE 17/2024, edital/TR e resultados por item. https://pncp.gov.br/pncp-api/v1/orgaos/76276849000154/compras/2024/70/arquivos/1
- ANM — PE 90005/2026, TR, itens e resultados 1 a 6. https://pncp.gov.br/pncp-api/v1/orgaos/29406625000130/compras/2026/31/arquivos/2 (homologação: substituir /1/ por /2/ a /6/ em https://pncp.gov.br/pncp-api/v1/orgaos/29406625000130/compras/2026/31/itens/1/resultados)
- ALESP — PE 125/2026, planilha estimada do edital. https://pncp.gov.br/pncp-api/v1/orgaos/59952259000185/compras/2026/139/arquivos/4
- SERPRO — PE 90227/2026, edital e anexos; orçamento sigiloso. https://pncp.gov.br/pncp-api/v1/orgaos/33683111000107/compras/2026/29/arquivos/1
- SFB — PE 90006/2024, edital e TR; preços estimados. https://pncp.gov.br/pncp-api/v1/orgaos/37115375000107/compras/2024/45/arquivos/1
- TRT2 — Contrato 133/2024; pacote HCI e serviços. https://pncp.gov.br/pncp-api/v1/orgaos/00509968000148/contratos/2024/4187/arquivos/1
- TCDF — Decisão 4782/2024, publicada no DODF 013/2025; caso SEEC/DF. https://www.sinj.df.gov.br/sinj/Diario/1d952c7d-a41c-3cae-bfbb-0f2c0a0ef9a6/DODF%20013%2020-01-2025%20INTEGRA.pdf
- Lei nº 13.303/2016 — regime do Banco; conferir RLC vigente. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm
- IN SEGES/ME nº 65/2021 — referencial metodológico, condicionado ao regime e ao RLC do Banco. https://www.gov.br/compras/pt-br/acesso-a-informacao/legislacao/instrucoes-normativas/instrucao-normativa-seges-me-no-65-de-7-de-julho-de-2021

> *Esta pesquisa é preliminar e deve ser atualizada pela equipe de planejamento à data efetiva da contratação. A memória de cálculo completa — incluindo os documentos-fonte referenciados acima — deve ser anexada ao processo administrativo, em atendimento à exigência de rastreabilidade da pesquisa de preços.*