

## **TERMO DE REFERÊNCIA**

Abertura de contratação de empresa especializada, via Pregão Eletrônico, com critério de julgamento menor preço global, em lote único, pelo prazo de 05 anos a contar da data da assinatura, para fornecimento de solução tecnológica de apoio à gestão de privacidade e proteção de dados pessoais, na modalidade Software como Serviço — SaaS, compreendendo disponibilização da plataforma mediante subscrição corporativa, implantação, configuração, parametrização, integração, migração inicial de informações necessárias ao início da operação, repasse de conhecimento, suporte técnico, sustentação, manutenção e serviços técnicos especializados sob demanda, com vistas a apoiar os processos institucionais de governança, conformidade, gestão de riscos, atendimento aos direitos dos titulares, registro das operações de tratamento, gestão de incidentes de privacidade, gestão de terceiros e demais atividades relacionadas à proteção de dados pessoais no âmbito do Banco da Amazônia, nos termos da Lei 13.303/2016.

### **1. DEFINIÇÃO DO OBJETO**

1.1 Contratação de empresa especializada, via Pregão Eletrônico, com critério de julgamento menor preço global, em lote único, pelo prazo de 05 anos a contar da data da assinatura, para fornecimento de solução tecnológica de apoio à gestão de privacidade e proteção de dados pessoais, na modalidade Software como Serviço — SaaS, compreendendo disponibilização da plataforma mediante subscrição corporativa, implantação, configuração, parametrização, integração, migração inicial de informações necessárias ao início da operação, repasse de conhecimento, suporte técnico, sustentação, manutenção e serviços técnicos especializados sob demanda, com vistas a apoiar os processos institucionais de governança, conformidade, gestão de riscos, atendimento aos direitos dos titulares, registro das operações de tratamento, gestão de incidentes de privacidade, gestão de terceiros e demais atividades relacionadas à proteção de dados pessoais no âmbito do Banco da Amazônia, nos termos da Lei 13.303/2016.

### **2. FORMA DE FORNECIMENTO E MODO DE DISPUTA**

- 2.1 Forma de fornecimento: o fornecimento do objeto será continuado.
- 2.2 O Modo de Disputa será aberto.
- 2.3 O levantamento realizado pela equipe de planejamento identificou que existem diversas empresas capazes de fornecer o objeto que se pretende licitar.
- 2.4 A quantidade de empresas aliado ao fato de que existem diversos modelos de soluções diferentes que podem atender a necessidade identificada, é um indicativo de que teremos competitividade no certame com probabilidade de variações no preço, podendo reduzir o valor estimado da contratação.
- 2.5 Por esse motivo entendemos que o modo de disputa que mais se adequa a essa contratação é o aberto.

### **3. FORMA DE SELEÇÃO DO FORNECEDOR E CRITÉRIO DE JULGAMENTO DA PROPOSTA**

- 3.1 O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.
- 3.2 Para efeito de julgamento, os lances ofertados deverão obedecer a composição de todos os itens que compõem o objeto, com vistas a obter o menor preço, consideradas as justificativas constantes neste Termo de Referência, deverão ser negociados os valores individualizados de cada item que compõe o lote, buscando também o menor preço unitário, tendo em vista que os itens se encontram agrupados, em razão da compatibilidade técnica/operacional intrínseca dentro do lote único.

- 3.3 Assim sendo, o julgamento das propostas será por lote único para garantir a melhor gestão do contrato, considerando que a solução deverá ser executada por um único fornecedor. Esta abordagem também leva em conta a complexidade de dividir o objeto, por se tratar de uma solução composta por itens de software e serviços. Será considerada vencedora a empresa que apresentar o menor preço global, desde que cumpra integralmente todos os requisitos estabelecidos neste Termo de Referência e apresente a Carta de Apresentação de Proposta (Anexo VII).
- 3.4 A licitação será realizada em lote único, uma vez que a solução possui natureza tecnológica integrada, composta por módulos interdependentes, fluxos automatizados e camadas comuns de segurança, governança, tratamento de dados e auditoria.
- 3.5 A execução da solução depende da implantação conjunta e coordenada de serviços especializados de parametrização, integração sistêmica, suporte técnico, manutenção evolutiva e atualização contínua frente às alterações regulatórias e orientações da Autoridade Nacional de Proteção de Dados (ANPD). O parcelamento do objeto, com a contratação de múltiplos fornecedores, introduziria riscos técnicos relevantes, tais como:
- 3.5.1 Quebra da interoperabilidade entre módulos da solução, com potencial incompatibilidade de padrões tecnológicos, APIs, modelos de dados e mecanismos de autenticação;
  - 3.5.2 Fragmentação da arquitetura de segurança da informação, aumentando a superfície de risco, dificultando a gestão de acessos, logs, trilhas de auditoria e controles de privacidade por padrão e por design;
  - 3.5.3 Risco de inconsistência metodológica na aplicação dos conceitos de LGPD, como bases legais, gestão de consentimento, atendimento aos direitos dos titulares, avaliação de impacto à proteção de dados (DPIA) e gestão de incidentes;
  - 3.5.4 Dificuldade de responsabilização contratual, com sobreposição de obrigações, conflitos de escopo e indefinição de responsabilidades em caso de falhas, incidentes de segurança ou não conformidades regulatórias;
  - 3.5.5 Comprometimento da rastreabilidade e da auditabilidade, uma vez que a consolidação de evidências, registros e indicadores de conformidade dependeria da integração de soluções distintas, potencialmente não homogêneas;
  - 3.5.6 Risco à continuidade operacional, considerando dependências técnicas entre módulos e a necessidade de respostas tempestivas a incidentes de privacidade e segurança da informação.
  - 3.5.7 Além disso, o parcelamento poderia onerar a gestão contratual, exigindo maior esforço de coordenação técnica e administrativa, aumento de custos indiretos e maior complexidade na governança da solução, sem ganho proporcional de economicidade ou competitividade.
- 3.6 Dessa forma, a contratação em lote único se mostra a alternativa mais adequada para assegurar:
- 3.6.1 Coerência técnica e operacional da solução;
  - 3.6.2 Padronização da governança de privacidade e proteção de dados no Banco;
  - 3.6.3 Rastreabilidade ponta a ponta dos processos de tratamento de dados pessoais;
  - 3.6.4 Maior segurança jurídica, técnica e regulatória;
  - 3.6.5 Eficiência na gestão contratual e no acompanhamento dos níveis de serviço (SLAs).
- 3.7 O parcelamento do objeto mostra-se tecnicamente desaconselhável, uma vez que a solução pretendida possui natureza integrada e interdependente, sendo composta por licenças, suporte técnico, manutenção, atualização tecnológica e serviços especializados que atuam de forma conjunta para assegurar a efetiva governança de privacidade e proteção de dados pessoais. A contratação em lote único proporciona maior interoperabilidade entre os componentes da solução, reduz riscos de integração, fortalece os controles de segurança da informação, simplifica a fiscalização contratual, assegura a responsabilização inequívoca do fornecedor, reduz custos administrativos e favorece a continuidade operacional dos serviços. Ademais, existem fornecedores no mercado aptos a executar

integralmente o objeto, de modo que a adoção de lote único não restringe a competitividade do certame e atende aos princípios da eficiência, economicidade e gestão de riscos previstos na Lei nº 13.303/2016.

3.8 Assim, o não parcelamento do objeto encontra respaldo nos princípios da eficiência, segurança, economicidade, interesse público e mitigação de riscos, nos termos da legislação aplicável às contratações públicas.

3.9 A adoção de lote único foi confrontada com a Súmula nº 247 do Tribunal de Contas da União, que impõe a adjudicação por item sempre que o objeto for divisível sem prejuízo para o conjunto. No caso concreto, a divisibilidade não se verifica: os itens recaem sobre a mesma plataforma e sobre a mesma base de dados, de modo que a sua atribuição a fornecedores distintos implicaria duplicidade de acesso a dados pessoais e sensíveis, indefinição de responsabilidade na hipótese de incidente e impossibilidade de aferição objetiva dos níveis mínimos de serviço.

3.10 Avaliou-se especificamente a possibilidade de segregação dos serviços técnicos especializados em item ou lote autônomo. A alternativa foi afastada porque tais serviços operam sobre as parametrizações, os fluxos, os inventários e as evidências mantidos na própria plataforma, exigindo acesso administrativo e conhecimento das configurações realizadas na implantação. A segregação produziria sobreposição de escopo com os serviços de suporte e sustentação, dificuldade de imputação de responsabilidade e ampliação do número de agentes com acesso a dados pessoais e sensíveis do Banco.

3.11 A eventual restrição à competitividade decorrente do agrupamento é mitigada por três mecanismos: a fixação de valor máximo aceitável por item, que preserva o controle sobre os preços unitários no interior do lote; a remuneração dos serviços técnicos especializados por entrega, com preço unitário próprio por faixa de complexidade; e a aferição da qualificação técnica por percentual de grupos de requisitos funcionais atendidos, admitido o somatório de atestados.

3.12 Registra-se, por fim, que o objeto é ofertado no mercado de forma integrada, conforme demonstrado no levantamento de mercado, e que a contratação pública adotada como referência principal também foi processada em lote único, com julgamento pelo menor preço global.

#### **4. PRAZO DE EXECUÇÃO/ENTREGA DO OBJETO DA CONTRATAÇÃO**

4.1 Para garantir a efetiva execução do contrato e o cumprimento dos prazos estabelecidos, foi estabelecido o cronograma abaixo, que especifica as atividades a serem realizadas, os prazos para cada atividade, os marcos iniciais e os responsáveis por cada etapa, conforme descrito a seguir:

| ATIVIDADE                                                                                         | PRAZO                         | MARCO INICIAL                                                         | RESPONSÁVEL              |
|---------------------------------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------|--------------------------|
| Reunião inicial do projeto (kick-off).                                                            | 5 dias úteis                  | Após a assinatura do contrato.                                        | CONTRATADA e CONTRATANTE |
| Apresentação do Plano de Implantação e da sua versão final após ajustes.                          | 5 dias úteis para cada versão | Reunião inicial do projeto e solicitação de ajustes pelo CONTRATANTE. | CONTRATADA               |
| Entrega da documentação comprobatória das subscrições contratadas e disponibilização dos acessos. | 5 dias úteis                  | Após a reunião inicial do projeto.                                    | CONTRATADA               |

| ATIVIDADE                                                                                                                                    | PRAZO                                                           | MARCO INICIAL                                                        | RESPONSÁVEL |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------------|-------------|
| Serviços de implantação (configuração, parametrização, estruturação de usuários e perfis, integrações, carga inicial, testes e homologação). | 90 dias corridos                                                | Reunião inicial do projeto.                                          | CONTRATADA  |
| Transferência de conhecimento (turmas de capacitação, materiais, manuais e documentação das parametrizações).                                | Conforme cronograma homologado, concluída até a emissão do TAD. | Após a homologação da implantação.                                   | CONTRATADA  |
| Serviços técnicos especializados por entrega e saldo de horas técnicas.                                                                      | Conforme o prazo da faixa de complexidade (NMS-21).             | Emissão da Ordem de Serviço.                                         | CONTRATADA  |
| Termo de Aceitação Provisório da implantação.                                                                                                | 15 (quinze) dias corridos                                       | Após a comunicação de conclusão da implantação.                      | CONTRATANTE |
| Termo de Aceitação Definitivo da implantação.                                                                                                | 15 (quinze) dias corridos                                       | Após o recebimento provisório.                                       | CONTRATANTE |
| Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação.                                                       | Durante a vigência contratual                                   | Emissão do Termo de Aceitação Definitivo, mediante Ordem de Serviço. | CONTRATADA  |
| Entrada em produção e acompanhamento assistido da operação.                                                                                  | 30 dias corridos                                                | Após a emissão do Termo de Aceitação Definitivo.                     | CONTRATADA  |

## 5. JUSTIFICATIVAS/FUNDAMENTAÇÃO DA CONTRATAÇÃO

5.1 A contratação visa atender aos objetivos estratégicos do Banco da Amazônia relacionados à governança de dados pessoais, em conformidade com a LGPD e ações de governança em privacidade e proteção de dados pessoais no âmbito da instituição. A iniciativa está alinhada às melhores práticas de gestão pública e governança de TI, baseadas nos referenciais ITIL, COBIT, ISO/IEC 20.000 e ISO/IEC 27.000, visando fortalecer a governança de TIC, promover a conformidade regulatória, modernizar os fluxos administrativos internos e aprimorar o atendimento aos usuários internos e externos, especialmente os titulares de dados pessoais.

5.2 A contratação visa resolver a carência institucional de mecanismos tecnológicos eficazes para garantir a conformidade com a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), as regulamentações do Banco Central do Brasil (Bacen) e demais normativos federais e setoriais que tratam da proteção de dados pessoais, da governança de informações sensíveis e da gestão de riscos regulatórios e reputacionais.

- 5.3 Inspirada principalmente na General Data Protection Regulation (GDPR), que regulamenta o tratamento de dados pessoais nos países membros da União Europeia, sendo inclusive de caráter impeditivo ao se operar negócios com a União Europeia, a LGPD acompanha uma tendência mundial em prol da proteção dos dados pessoais dos seus cidadãos, onde as pessoas tem o direito de controle sobre seus dados e, as pessoas jurídicas a obrigação de informar ao Titular e proteger os dados pessoais que estão sob sua tutela, tornando os processos de tratamento de dados pessoais mais transparentes e seguros.
- 5.4 A LGPD estabelece princípios fundamentais como finalidade, adequação, necessidade, segurança e prestação de contas. A contratação de uma solução de gestão de privacidade e proteção de dados permitirá à instituição implementar mecanismos sistemáticos e automatizados para garantir o cumprimento desses princípios, assegurando que o tratamento de dados seja realizado de forma ágil, ética, legal e transparente.
- 5.5 A formalização do Banco da Amazônia com parcerias internacionais, como a AFD (Agência Francesa de Desenvolvimento), reforça a necessidade de aderência ao GDPR, norma europeia que estabelece elevados padrões de transparência, responsabilização e controle sobre o tratamento de dados pessoais.
- 5.6 Essa necessidade decorre da crescente complexidade do cenário regulatório nacional e internacional. O Banco da Amazônia, por meio do seu Data Protection Officer (DPO - Artigo 41 da LGPD) que atua na Gerência de Segurança Corporativa, identificou a necessidade de uma solução integrada e automatizada que permita:
- 5.7 A gestão completa do ciclo de vida dos dados pessoais, desde a coleta e classificação até o armazenamento, compartilhamento, descarte e anonimização conforme Norma de Procedimento de Classificação e Tratamento da Informação. Isso inclui a capacidade de identificar, mapear e monitorar os fluxos de dados dentro da organização, garantindo que todas as operações de tratamento estejam alinhadas com as melhores práticas de governança e conformidade.
- 5.8 A operacionalização dos direitos dos titulares como acesso, correção, eliminação, portabilidade e revogação de consentimento. A solução contratada deverá automatizar e agilizar o atendimento a essas solicitações, garantindo que a instituição cumpra os prazos legais (artigos 18 a 22 da LGPD) e mantenha um registro auditável de todas as interações com os titulares.
- 5.9 A solução deverá fortalecer a capacidade institucional de detecção, registro, notificação e mitigação de incidentes de segurança e vazamentos de dados. Isso inclui a implementação de mecanismos de monitoramento contínuo, alertas em tempo real e planos de resposta a incidentes, reduzindo os riscos de multas e sanções por parte da Autoridade Nacional de Proteção de Dados (ANPD).
- 5.10 A solução deverá realizar elaboração de Relatórios de Impacto à Proteção de Dados (DPIA) e a manutenção de Registros das Operações de Tratamento (ROPA). A solução contratada deverá automatizar a criação e atualização desses documentos, facilitando a gestão de riscos e a prestação de contas perante a ANPD e outras instâncias fiscalizadoras.
- 5.11 A solução deverá ser aderente às melhores práticas internacionais de segurança da informação, como as normas ISO/IEC 27001 e ISO/IEC 27701, integrando controles técnicos e administrativos em conformidade com a Política de Segurança da Informação e Cibernética da instituição. Isso inclui a implementação de mecanismos de criptografia, controle de acesso, monitoramento de atividades e gestão de vulnerabilidades.
- 5.12 A solução deverá permitir a gestão de riscos envolvendo terceiros e fornecedores que tenham acesso a dados pessoais ou que operem serviços críticos. Isso inclui a avaliação de conformidade, a auditoria de contratos e a implementação de cláusulas contratuais que garantam a proteção dos dados compartilhados.
- 5.13 A ANPD e outras instâncias regulatórias estão em constante evolução, com novas normas e regulamentações setoriais sendo publicadas regularmente. A solução contratada deverá ser flexível e escalável, permitindo que a instituição se adapte rapidamente a novas exigências legais e regulatórias.

- 5.14 A má gestão de dados pessoais e a falta de controle sobre decisões automatizadas podem resultar em multas, sanções, processos judiciais e danos à reputação da instituição. A implementação de uma solução robusta de gestão de privacidade e proteção de dados reduzirá esses riscos, promovendo a integridade institucional e a confiança dos públicos atendidos
- 5.15 A Autoridade Nacional de Proteção de Dados (ANPD) possui amplos poderes para fiscalizar e aplicar sanções às organizações que descumprirem as disposições da LGPD. As multas podem chegar a 2% do faturamento da instituição, limitadas a R\$ 50 milhões por infração, além de outras penalidades, como:
- 5.16 Advertências com prazo para adequação;
- 5.17 Bloqueio ou eliminação dos dados pessoais envolvidos na infração;
- 5.18 Suspensão das atividades de tratamento de dados;
- 5.19 Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.
- 5.20 Além das sanções administrativas, o Banco da Amazônia pode enfrentar ações judiciais movidas por titulares de dados, danos à reputação e perda de confiança por parte de clientes, parceiros e stakeholders. A contratação de uma solução de gestão de privacidade e proteção de dados é, portanto, uma medida essencial para mitigar esses riscos e garantir a conformidade com a legislação vigente.
- 5.21 A presente demanda está diretamente alinhada ao Plano Estratégico do Banco da Amazônia 2023–2030, especialmente ao objetivo estratégico “Ser um banco de desenvolvimento inovador”, que visa fomentar a modernização institucional por meio da adoção de soluções tecnológicas que promovam maior eficiência operacional, segurança jurídica e sustentabilidade.
- 5.22 A contratação da solução de Gestão de Privacidade e Proteção de Dados Pessoais também reforça o comprometimento da instituição com o valor estratégico da “Inovação”, conforme definido no referido plano. Este valor orienta a transformação dos métodos de negócio do Banco, priorizando a adoção de ferramentas modernas, seguras e aderentes às melhores práticas internacionais, com foco na entrega de valor aos stakeholders e no fortalecimento da governança institucional.
- 5.23 Além disso, a iniciativa contribui para os eixos de governança digital, transformação digital e gestão de riscos, temas estruturantes para a evolução da atuação do Banco no contexto regional, nacional e internacional, sobretudo em um cenário regulatório cada vez mais exigente e complexo.
- 5.24 A iniciativa também está alinhada ao PDTI 2026–2027, ao atender objetivos relacionados à modernização da infraestrutura tecnológica, à gestão de riscos e segurança da informação, e à automação de processos corporativos. A solução contribuirá para o fortalecimento da governança de dados e da conformidade regulatória, elementos essenciais para a transformação digital da instituição.
- 5.25 A contratação dos serviços tem conformidade com o normativo interno do Banco denominado NP 025 – Processo de Seleção e Aquisição de Serviços e Produtos de TI.
- 5.26 A contratação proposta está devidamente contemplada no PAC (Plano Anual de Contratações) PAC do Banco, em conformidade com as diretrizes de planejamento, aos instrumentos de governança corporativa e ao princípio do planejamento, assegurando racionalidade na alocação de recursos, previsibilidade na execução orçamentária e aderência às estratégias institucionais.
- 5.27 A CONTRATADA deverá analisar, identificar e propor melhorias sobre os processos e documentos já existentes, garantindo que o novo trabalho se integre harmonicamente aos esforços já realizados. Esta abordagem é fundamental para evitar a perda de conhecimento institucional e manter a consistência metodológica que foi estabelecida no programa de privacidade do Banco. A evolução gradual e estruturada do programa permite que as equipes mantenham o domínio sobre os processos enquanto incorporam novas funcionalidades e melhorias.
- 5.28 Suporte técnico especializado para consolidar e manter o programa de adequação à LGPD, abrangendo múltiplas dimensões da governança de privacidade. Este suporte deve incluir a

automação do mapeamento de dados, a gestão proativa de riscos e incidentes, o atendimento eficiente aos direitos dos titulares e a capacitação contínua das equipes técnicas e administrativas.

- 5.29 O suporte especializado deve focar em três pilares principais: Governança e Estratégia, Operação e Tecnologia, e Pessoas e Processos, assegurando uma abordagem holística e integrada para a gestão da privacidade.
- 5.30 A complexidade técnica e a especificidade das atividades relacionadas à implementação e manutenção de um programa robusto de proteção de dados, aliadas à ausência de recursos humanos especializados e ferramentas tecnológicas adequadas no quadro atual do Banco da Amazônia, tornam imprescindível a contratação de empresa especializada. A natureza multidisciplinar do projeto exige conhecimentos específicos em direito digital, tecnologia da informação, gestão de riscos e governança corporativa, competências que dificilmente são encontradas concentradas em uma única equipe interna.
- 5.31 O fornecimento de soluções tecnológicas especializadas é fundamental para disponibilizar ferramentas que facilitem o mapeamento automatizado de dados, a gestão proativa de riscos, o atendimento eficiente aos titulares e o monitoramento contínuo da conformidade. Estas ferramentas devem ser integradas e interoperáveis, permitindo uma visão holística e em tempo real do programa de privacidade do Banco.
- 5.32 Os serviços técnicos especializados são essenciais para oferecer suporte qualificado na revisão e otimização de processos, na elaboração e atualização de políticas e procedimentos, bem como na implementação das medidas técnicas e administrativas necessárias para a adequação contínua à LGPD. Este suporte deve ser prestado por profissionais com experiência comprovada em projetos similares e conhecimento atualizado da legislação e das melhores práticas do mercado.
- 5.33 A capacitação e conscientização representam um componente crítico do programa, exigindo a condução de treinamentos e workshops especializados para diferentes níveis hierárquicos e áreas funcionais. O objetivo é assegurar que todos os envolvidos no tratamento de dados pessoais compreendam plenamente suas responsabilidades e estejam capacitados para executar suas funções em conformidade com os requisitos legais e as políticas internas do BASA.
- 5.34 A estratégia de contratação busca alinhar tecnologia, segurança da informação e eficiência operacional, garantindo que o Banco da Amazônia seja referência na prestação de serviços públicos de qualidade. O alinhamento com os marcos regulatórios vigentes e as melhores práticas internacionais de governança assegura que a solução contribua efetivamente para a melhoria da qualidade dos serviços prestados, proporcionando maior controle, rastreabilidade e agilidade nas rotinas administrativas institucionais e financeiras da instituição.
- 5.35 Além disso, a contratação deve ser aderente aos requisitos de sustentabilidade do Banco que possui como compromisso o desenvolvimento econômico em harmonia com a preservação ambiental, atuando de forma sustentável dentro da organização e apoiando projetos com esse caráter.
- 5.36 Por tratar-se de serviço SaaS “unificado” entende-se a solução deva possuir/entregar todo o conjunto mínimo de funcionalidades, conforme descrito no Anexo V, prontos e integrados de forma nativa, contemplando todos os requisitos técnicos mínimos solicitados.
- 5.37 Assim sendo, a contratação da solução tecnológica para proteção de dados pessoais na modalidade SaaS pode trazer os seguintes benefícios ao Banco da Amazônia:
- a) Apoiar nas ações de governança de dados pessoais, proporcionando conformidade, garantindo a proteção dos dados pessoais, respeitando os direitos dos cidadãos, clientes e atendendo aos requisitos legais;
  - b) Diagnosticar as necessidades de adequação, propor e executar medidas para adequar a instituição à LGPD e aos demais padrões de segurança recomendados às instituições financeiras;

- c) Mitigar o risco da ocorrência de incidentes de segurança que representem violações de dados e implementar processos para tratamento de incidentes e violações de dados, caso ocorram;
- d) Aperfeiçoar os requisitos de transparência quando do tratamento de dados pessoais nos serviços prestados aos cidadãos e clientes;
- e) Eliminação de trabalho manual no tratamento e consolidação de dados, reduzindo problemas de estruturas e dados causados por processos manuais;
- f) Garantir a rastreabilidade, a auditabilidade e a automação dos controles técnicos e administrativos exigidos pela legislação, fortalecendo a governança de dados pessoais do BASA;
- g) Aprimorar a tomada de decisão, fornecendo informações precisas e seguras dos dados sob a custódia da instituição;
- h) Reduzir os riscos operacionais decorrentes da manipulação de dados para geração de informações gerenciais e regulatórias;
- i) Automatizar tarefas para otimizar o trabalho das equipes do Banco da Amazônia.
- j) Disseminar a cultura de privacidade no âmbito da instituição por meio de treinamentos e campanhas de conscientização.

5.38 A contratação visa melhorar a governança de dados do Banco da Amazônia, sendo um componente tecnológico indispensável para a mitigação de riscos. A solução centraliza e otimiza atividades críticas que, de outra forma, demandariam um esforço manual intensivo e descentralizado.

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

6.1 As especificações da solução estão descritas no Anexo V, deste Termo de Referência, contendo os requisitos técnicos definidos, e no Anexo VI, contendo os Requisitos de Teste de Prova de Conceito-POC da Solução.

6.2 O objeto é constituído por um lote único, formado pelos itens indicados na tabela abaixo, e o julgamento será pelo menor preço global, observados os valores máximos aceitáveis por item fixados no instrumento convocatório:

| ITEM | DESCRIÇÃO                                                                                                                                                                           | UNIDADE | QTD. |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| 1    | Subscrição corporativa de solução tecnológica para apoio à governança, gestão, monitoramento e conformidade em privacidade e proteção de dados pessoais.                            | Mês     | 60   |
| 2    | Subscrição corporativa de solução para identificação, mapeamento, inventário, classificação e monitoramento de dados pessoais e sensíveis em bases estruturadas e não estruturadas. | Mês     | 60   |
| 3    | Serviços de implantação da solução                                                                                                                                                  | Serviço | 1    |
| 4    | Transferência de conhecimento (capacitação de administradores e usuários, materiais de apoio, manuais, documentação das parametrizações e repasse formal das configurações)         | Serviço | 1    |
| 5    | Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação (24x7)                                                                                        | Mês     | 60   |
| 6    | Serviços técnicos especializados em privacidade e Proteção de Dados, sob demanda (itens de catálogo).                                                                               | Entrega | 290  |
| 7    | Saldo de horas técnicas especializadas para demandas supervenientes não catalogadas                                                                                                 | Hora    | 320  |

6.3 Trata-se o objeto de serviços de natureza comum, uma vez que os seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Os itens constantes do objeto estão enquadrados como solução de TIC.

6.4 A contratação prevista será de natureza continuada, pois visa atender à necessidade pública de forma permanente e prolongada, por mais de um exercício financeiro, assegurando a integridade do patrimônio público e o funcionamento das atividades da instituição, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.

6.5 Os serviços que compõem o objeto licitado são de mesma natureza, dependentes entre si, e sua divisão impactaria na execução do projeto, tornaria a contratação menos econômica, menos eficaz e mais complexa, além de impossibilitar uma execução satisfatória.

6.6 A solução permitirá ao BASA implementar as adequações necessárias, aplicar controles internos adequados e monitorar continuamente a conformidade, em alinhamento com a LGPD e as políticas de segurança que são exigidas pelo Banco Central às instituições financeiras.

6.7 A solução compreende o fornecimento de software, com serviços de implantação, customização, parametrização, suporte técnico e atualizações, além de serviços técnicos especializados atrelados à disponibilização, funcionalidade e uso da solução pelos usuários do Banco, conforme especificações e condições definidos neste Termo de Referência e seus Anexos.

6.8 O objeto prevê a manutenção corretiva, legal, adaptativa, atualização de versões, suporte técnico pelo prazo de vigência contratual, após customização/implementação da solução em produção.

6.9 A definição dos quantitativos baseou-se no prazo de vigência contratual, para os itens medidos em meses; na natureza não recorrente das entregas, para os itens de implantação e de transferência de conhecimento; e na demanda anual projetada por faixa de complexidade, para os serviços técnicos especializados. A volumetria do ambiente de dados e a estrutura organizacional do Banco foram tratadas como requisitos mínimos de capacidade impostos à solução, e não como quantidade licenciada.

6.10 A definição também se baseou em contratações similares de outras instituições públicas que possuem as mesmas necessidades de conformidade impostas pela LGPD e normas de segurança e privacidade.

6.11 A contratação dos serviços técnicos especializados em privacidade e proteção de dados pessoais será remunerada por entrega, a partir de catálogo de serviços que define, para cada tipo de demanda, o escopo, os produtos esperados, os critérios de aceite, o prazo e a faixa de complexidade, na forma do Anexo V deste Termo de Referência.

6.12 As demandas relacionadas à gestão de privacidade e proteção de dados pessoais envolvem atividades de elevada complexidade técnica, frequentemente desencadeadas por eventos específicos, tais como a análise de novos fluxos de tratamento, a elaboração de relatórios de impacto à proteção de dados, a avaliação de riscos, as adequações normativas, o apoio ao tratamento de incidentes, o atendimento a solicitações de titulares de maior complexidade e a avaliação de operadores e terceiros. A variabilidade recai sobre a quantidade e a oportunidade das demandas, e não sobre a natureza dos produtos, que são previamente identificáveis e verificáveis.

6.13 Por essa razão, a mensuração dos serviços é realizada por produto entregue e aceite, e não por tempo empregado, em observância à Súmula TCU nº 269, ao art. 26, item 2, do Regulamento de Licitações e Contratos do Banco da Amazônia e ao art. 3º, inciso III, da Resolução CGPAR nº 45/2022. O quantitativo estimado de entregas constitui limite máximo, não gera direito subjetivo à execução integral e não impõe consumo mínimo.

6.14 Subsidiariamente, e apenas para demandas supervenientes relacionadas à privacidade e à proteção de dados pessoais que não se enquadrem em nenhum dos serviços catalogados, prevê-se saldo de horas técnicas especializadas, de acionamento excepcional, condicionado à justificativa prévia da inexistência de serviço catalogado equivalente e da ausência de sobreposição com os serviços de implantação, de transferência de conhecimento e de suporte e sustentação, na forma do Anexo V.

6.15 O acionamento, a execução, o registro, a comprovação, o aceite e o pagamento dos serviços técnicos especializados observarão os seguintes controles:

6.16 Ordem de Serviço Formal

6.16.1 Toda demanda deverá ser previamente autorizada pelo CONTRATANTE mediante Ordem de Serviço, que indicará o serviço catalogado, a faixa de complexidade, o objeto específico, os produtos esperados, os critérios de aceite, o prazo de entrega e os responsáveis pelo acompanhamento.

6.17 Relatório e evidências por entrega

6.17.1 A CONTRATADA deverá apresentar, para cada entrega, relatório técnico contendo:

- a) identificação da Ordem de Serviço e do serviço catalogado;
- b) escopo executado e método adotado;
- c) produtos entregues e respectivas evidências;
- d) profissionais responsáveis e respectivas qualificações;
- e) demonstração do atendimento aos critérios de aceite e ao prazo pactuado.

6.18 Validação Técnica da Contratante

6.18.1 O pagamento será realizado exclusivamente sobre as entregas efetivamente aceitas pelo CONTRATANTE, mediante Termo de Aceite da Entrega emitido pela área técnica, admitida a glosa de produtos não aderentes ao escopo autorizado.

6.19 Gestão do quantitativo estimado

6.19.1 As entregas não demandadas em determinado exercício poderão ser realizadas em períodos subsequentes, respeitados o quantitativo total estimado e o prazo contratual, sem que o quantitativo estimado gere obrigação de contratação.

6.20 Todo o histórico de acionamento, execução, aceite e pagamento será documentado e estará disponível para auditoria interna e externa, assegurando transparência, rastreabilidade e controle efetivo da execução.

6.21 As especificações técnicas do objeto, bem como a descrição dos serviços que compõem a solução foram descritas no Anexo V deste Termo de Referência.

## **7 INDICAÇÃO DE EVENTUAL CONTRATAÇÃO DE CORRELATAS OU INTERDEPENDENTES**

7.1 Serão de inteira responsabilidade e as expensas da CONTRATADA, sem nenhum custo adicional para o Banco:

7.1.1 Alocação de profissionais qualificados, incluindo todas as obrigações trabalhistas relacionadas à solução, caso haja a necessidade de um técnico da CONTRATADA.

7.1.2 Apoio e suporte técnico e logístico eventualmente necessário ao adequado funcionamento da solução.

7.1.3 Todos os custos relativos a transporte, alimentação e hospedagem de profissionais, transporte dos equipamentos, ligações telefônicas e aberturas de chamados para suporte técnico, montagem física dos equipamentos que compõem a solução, disponibilização de ferramentas e insumos diversos requeridos.

7.1.4 Configurações e customizações requeridas para mitigar ocorrências de indisponibilidade da solução, motivadas por falhas de desempenho e de disponibilidade.

7.1.5 Executar o serviço de acordo com as normas técnicas aplicáveis, obedecendo às recomendações dos fabricantes dos equipamentos e dos insumos/materiais e dentro do estabelecido nas especificações disponíveis, bem como em conformidade com outras informações/disposições fornecidas pela CONTRATANTE.

7.1.6 Fornecer a seus prepostos o ferramental necessário à execução dos serviços, inclusive os manuais técnicos dos fabricantes dos equipamentos (sobre os quais incidirem a prestação dos serviços) que permitam a seus PROFISSIONAIS identificarem rapidamente os insumos/materiais e consultar procedimentos recomendados para solução dos problemas.

7.2 Para garantir a adequada manutenção, a CONTRATADA deverá disponibilizar uma infraestrutura de Suporte Técnico em período integral, ou seja, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, nas seguintes modalidades:

7.2.1 Suporte técnico remoto (*on-line*): compreendendo a assistência à CONTRATANTE, prestada por meio de chamadas telefônicas, sistemas de chamados de suporte ou e-mail;

7.2.2 Suporte técnico local (*on-site*): compreendendo o atendimento de campo, prestado por técnico(s) capacitados, no(s) local(is) de instalação ou em trechos correspondentes a execução do objeto, incidência dos serviços.

## **8 REQUISITOS DA CONTRATAÇÃO**

8.1 Os requisitos da contratação, bem como a descrição dos serviços que compõem a solução foram descritas no Anexo V deste Termo de Referência.

8.2 Os critérios de habilitação jurídica, fiscal, trabalhista estão previstos no Termo de Referência padronizado pelo Banco da Amazônia.

8.3 Os critérios de qualificação técnica estão previstos no termo de referência.

8.4 As demais condições para contratação estão previstas neste Termo de Referência.

## **9 ESCOLHA DA SOLUÇÃO**

9.1 A solução dever ser na modalidade *SaaS – Software as a Service* (Software como Serviço), em ambiente de nuvem de responsabilidade da CONTRATADA, devendo seguir todas as regulamentações aplicadas ao objeto, normas de segurança e privacidade e demais condições definidas em Edital e seus Anexos.

9.2 A solução propõe a subscrição do software com o apoio externo, implementando o software para automatizar atividades que são humanamente impossíveis de serem executadas com alto grau de precisão, bem como levariam muito tempo para serem concluídas, e apoio externo para serviços agregados que irão apoiar no diagnóstico e adequação à LGPD, implementando medidas e estruturando um programa de privacidade, no software ofertado.

9.3 A solução se mostra mais adequada, já que o componente de software desempenhará um papel fundamental na manutenção da conformidade legal a ser obtida, contando ainda com o auxílio de serviços técnicos especializados.

9.4 O objeto é proposto em lote único, considerando que se trata de uma única solução de TIC, compreendendo o fornecimento de software e serviços técnicos especializados.

9.5 As análises e justificativas de escolha da solução encontram-se detalhada do Estudo Técnico que concluiu pela viabilidade da contratação na forma proposta.

## **10 PLANO DE SUSTENTAÇÃO**

### **10.1 Recursos necessários à continuidade do negócio durante e após a execução do contrato**

- i. Recursos Materiais a serem fornecidos pelo Banco: Não há recursos materiais a serem fornecidos pelo Banco.
- ii. Recursos de TI a serem fornecidos pelo Banco: Disponibilização de VPN (VIRTUAL PRIVATE NETWORK) para execução do serviço remotamente pela CONTRATADA, conforme necessidade.
- iii. Recursos Humanos: a Contratada deverá alocar (remotamente) profissionais qualificados, na forma exigida na licitação.

10.2 O Banco alocará analistas da área técnica, caso seja solicitado pela CONTRATADA, ou na forma estabelecida no contrato para acompanhar o contrato, absorver conhecimentos e fiscalizar a execução dos serviços.

10.3 Após a execução do contrato, o Banco já deverá ter adotado todas as providências para renovação, ou realizar nova licitação ou ainda absorver o serviço por equipe própria.

10.4 Estratégia de continuidade contratual

10.4.1 Constará em contrato que a empresa contratada será obrigada a manter durante toda a vigência contratual, garantia contratual ao CONTRATANTE, em qualquer das modalidades previstas em lei (caução em dinheiro, fiança bancária ou seguro-garantia), nos termos da Lei nº 13.303/2016, com todas as condições previstas na referida lei.

10.5 Plano de continuidade de negócios

10.5.1 A CONTRATADA deverá possuir processo de gestão de continuidade de negócio, para mitigar graves perdas decorrentes de riscos operacionais que possam comprometer o Níveis Mínimos de Serviço previstos na contratação.

10.6 Ações para transição e encerramento contratual

10.6.1 Receber comunicado da área responsável sobre o encerramento legal do contrato e informar sobre a inexistência de pendências e providências para nova contratação, se for o caso.

## **11 INDICAÇÃO SE O CONTRATO É COM OU SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA**

11.1 Esta contratação não possui dedicação exclusiva de mão de Obra.

## **12 MODELO DE GESTÃO DO CONTRATO**

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

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

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

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

12.5 Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

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

### **12.6.1 Fiscalização Técnica**

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

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

- 12.6.1.3 Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.
- 12.6.1.4 O fiscal técnico do contrato informará ao gestor do serviço, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.
- 12.6.1.5 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do serviço.
- 12.6.1.6 O fiscal técnico do contrato comunicará ao gestor do serviço, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

## **12.6.2 Fiscalização Administrativa**

12.7 O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada.

- 12.7.1.1 Caso ocorra descumprimento das obrigações administrativas contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do serviço para que tome as providências cabíveis, quando ultrapassar a sua competência.

## **12.7.2 Gestor do Serviço**

- 12.7.2.1 O gestor do serviço coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.
- 12.7.2.2 O gestor do serviço acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.
- 12.7.2.3 O gestor do serviço acompanhará a manutenção das condições de habilitação da contratada, para fins de pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.
- 12.7.2.4 O gestor do serviço emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e negócios quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.
- 12.7.2.5 O gestor do serviço tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela área competente para tal, conforme o caso.
- 12.7.2.6 O gestor do serviço deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.
- 12.7.2.7 O gestor do serviço deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

## **13 ESTIMATIVAS DOS PREÇOS**

13.1 O valor estimado da contratação será consolidado após a conclusão da pesquisa de preços e registrado, por item, no quadro abaixo: [A PREENCHER APÓS CONCLUSÃO DA PESQUISA DE PREÇOS]

| ITEM | DESCRIÇÃO                                                                                                                                                                           | UNIDADE | QTD. | Valor Unitário | Valor Anual | Valor Global |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|----------------|-------------|--------------|
| 1    | Subscrição corporativa de solução tecnológica para apoio à governança, gestão, monitoramento e conformidade em privacidade e proteção de dados pessoais.                            | Mês     | 60   |                |             |              |
| 2    | Subscrição corporativa de solução para identificação, mapeamento, inventário, classificação e monitoramento de dados pessoais e sensíveis em bases estruturadas e não estruturadas. | Mês     | 60   |                |             |              |
| 3    | Serviços de implantação da solução                                                                                                                                                  | Serviço | 1    |                |             |              |
| 4    | Transferência de conhecimento (capacitação de administradores e usuários, materiais de apoio, manuais, documentação das parametrizações e repasse formal das configurações)         | Serviço | 1    |                |             |              |
| 5    | Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação (24x7)                                                                                        | Mês     | 60   |                |             |              |
| 6    | Serviços técnicos especializados em Privacidade e Proteção de Dados, sob demanda (itens de catálogo).                                                                               | Entrega | 290  |                |             |              |
| 7    | Saldo de horas técnicas especializadas para demandas supervenientes não catalogadas                                                                                                 | Hora    | 320  |                |             |              |

Deverão ser descritos os valores do item 6 Serviços técnicos especializados em Privacidade e Proteção de Dados (itens de catálogo).

| Cód.  | Serviço                                                       | Qtd./ano | Qtd./60 meses | Valor Unitário | Valor Ano | Valor Global |
|-------|---------------------------------------------------------------|----------|---------------|----------------|-----------|--------------|
| CS-01 | Elaboração ou revisão de instrumento normativo de privacidade | 4        | 20            |                |           |              |
| CS-02 | Diagnóstico do programa de privacidade e plano de evolução    | 1        | 5             |                |           |              |

|       |                                                                                            |    |     |  |  |  |
|-------|--------------------------------------------------------------------------------------------|----|-----|--|--|--|
| CS-03 | Análise e registro de operação de tratamento no inventário (ROPA)                          | 10 | 50  |  |  |  |
| CS-04 | Revisão integral do inventário de macroprocesso                                            | 2  | 10  |  |  |  |
| CS-05 | Elaboração de Relatório de Impacto à Proteção de Dados                                     | 4  | 20  |  |  |  |
| CS-06 | Avaliação de riscos de privacidade e plano de tratamento                                   | 3  | 15  |  |  |  |
| CS-07 | Avaliação de privacidade desde a concepção                                                 | 6  | 30  |  |  |  |
| CS-08 | Apoio técnico à análise, contenção, documentação e comunicação de incidente de privacidade | 6  | 30  |  |  |  |
| CS-09 | Apoio técnico ao atendimento de solicitação de titular de alta complexidade                | 10 | 50  |  |  |  |
| CS-10 | Avaliação de privacidade de operador, suboperador ou terceiro                              | 4  | 20  |  |  |  |
| CS-11 | Análise de impacto de ato normativo superveniente e plano de adequação                     | 3  | 15  |  |  |  |
| CS-12 | Integração da solução com sistema ou fonte de dados não prevista na implantação            | 2  | 10  |  |  |  |
| CS-13 | Capacitação técnica complementar sobre a solução ou sobre processos de privacidade         | 3  | 15  |  |  |  |
|       |                                                                                            | 58 | 290 |  |  |  |

13.2 O faturamento dos itens 1, 2 e 5 terá início no mês subsequente à emissão do Termo de Aceitação Definitivo da implantação, não sendo devido pagamento por subscrições não disponibilizadas e efetivamente implantadas, nem pagamento antecipado.

13.3 A estimativa do valor da contratação será consolidada após a conclusão da pesquisa de preços, que contemplará levantamento de contratações públicas similares e consulta estruturada ao mercado por meio de Request for Proposal – RFP, cujos resultados integrarão a memória de cálculo e o Mapa Comparativo de Preços da contratação.

13.4 Ressalta-se, ainda, que a elevação do status da Autoridade Nacional de Proteção de Dados (ANPD) à condição de agência nacional resultou em maior robustez regulatória, intensificação das ações de fiscalização e maior exigência técnica sobre os agentes de tratamento. Esse cenário fomentou significativamente o mercado de soluções de privacidade, impactando diretamente a estrutura de custos, o nível de especialização demandado e os preços praticados atualmente.

13.5 Foram identificadas, para fins de levantamento de mercado, contratações realizadas pelo Superior Tribunal de Justiça – STJ, pelo Banco do Nordeste – BNB, pelo Tribunal Regional Federal da 3ª Região, pela Câmara Municipal de Lorena/SP, pelo PRODERJ, pela SEAD/PI, pela MTI/MT e pela PRODEPA, as quais serão submetidas a análise crítica individualizada, com registro das referências consideradas comparáveis, das descartadas e das respectivas justificativas.

13.6 Diante desse contexto, a metodologia da pesquisa de preços contempla duas frentes combinadas:

13.6.1 Mapa Comparativo de Preços de Contratações Públicas, elaborado a partir de contratos, atas, editais, termos de referência e resultados de licitações relativos a objetos comparáveis, com análise crítica individualizada de cada referência, registro das referências válidas e das descartadas com as respectivas justificativas, e normalização e segregação dos componentes de preço — subscrição, implantação, parametrização, integrações, transferência de conhecimento, suporte, manutenção, serviços técnicos especializados e saldo de horas —, na forma detalhada no Estudo Técnico Preliminar;

13.6.2 Request for Proposal – RFP encaminhada ao mercado, organizada pelos mesmos componentes econômicos da contratação, com registro da quantidade de fornecedores consultados, das respostas recebidas, da estrutura das propostas, dos valores apresentados e das eventuais ressalvas comerciais.

13.7 As evidências dos resultados das consultas e planilhas consolidadas dos cálculos utilizados estão contidas no processo de contratação.

13.8 Integrarão os autos, após a conclusão das pesquisas: o Mapa Comparativo de Preços de Contratações Públicas; o resultado consolidado da RFP; a memória de cálculo da estimativa; e o quadro de composição do valor estimado, segregado por subscrição, implantação, transferência de conhecimento, suporte e sustentação, serviços técnicos especializados e saldo de horas técnicas.

#### **14 NÍVEL MÍNIMO DE SERVIÇO OU SERVICE LEVEL AGREEMENT (SLA)**

14.1 A execução contratual será orientada por Níveis Mínimos de Serviço (NMS), que funcionam como referências objetivas de qualidade, tempestividade e eficiência das entregas e condicionam a remuneração devida, na forma da Súmula TCU nº 269. Os indicadores são organizados em série numérica única, aplicável a este Termo de Referência, aos seus anexos, ao Estudo Técnico Preliminar e à minuta contratual.

14.2 A contratação deverá contemplar Níveis Mínimos de Serviço — NMS, ou Service Level Agreement — SLA, compatíveis com a natureza da solução contratada, com a modalidade Software como Serviço — SaaS, com a criticidade dos processos de privacidade e proteção de dados pessoais apoiados pela plataforma, com os requisitos de segurança da informação, continuidade operacional, suporte técnico, rastreabilidade e conformidade regulatória aplicáveis ao Banco da Amazônia

14.3 Os NMS/SLA deverão ser definidos de forma objetiva, mensurável, auditável, proporcional e vinculada a resultados efetivamente controláveis pela contratada, evitando-se indicadores genéricos, inexecutáveis, excessivamente restritivos ou sem relação direta com a qualidade, disponibilidade, segurança, suporte, desempenho e continuidade da solução contratada.

| REFERÊNCIA | MÉTRICA                             | DESCRIÇÃO                                                                                                                      | DEFINIÇÃO                                                                                                                                           | NMS - VALORES REFERÊNCIA |
|------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| NMS-01     | Disponibilidade mensal da solução   | Percentual de tempo em que as funcionalidades contratadas permanecem disponíveis aos usuários autorizados, em regime 24x7.     | Apurado mensalmente, excluída a janela de manutenção programada de até 2 (duas) horas por mês, previamente comunicada e acordada com o CONTRATANTE. | Mínimo de 99,0% ao mês   |
| NMS-02     | Tempo objetivo de recuperação (RTO) | Tempo máximo para restabelecimento da solução após evento de indisponibilidade que exija acionamento do plano de continuidade. | Medido entre a declaração do evento e o restabelecimento do serviço em condições de uso.                                                            | Até 4 (quatro) horas     |

| REFERÊNCIA | MÉTRICA                                               | DESCRIÇÃO                                                                                                                                       | DEFINIÇÃO                                                                                 | NMS - VALORES REFERÊNCIA                                                                                                                          |
|------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| NMS-03     | Ponto objetivo de recuperação (RPO)                   | Perda máxima de dados admitida, medida em tempo, na recuperação posterior a evento de indisponibilidade.                                        | Intervalo máximo entre o último ponto de recuperação íntegro e o momento do evento.       | Até 1 (uma) hora                                                                                                                                  |
| NMS-04     | Comunicação de incidente ao CONTRATANTE               | Prazo para comunicar incidente de segurança da informação ou de privacidade, violação de dados pessoais, falha de segregação ou perda de dados. | Medido entre a ciência do evento pela CONTRATADA e a comunicação formal ao CONTRATANTE.   | Comunicação inicial em até 2 (duas) horas; relatório preliminar em até 24 (vinte e quatro) horas; relatório conclusivo em até 10 (dez) dias úteis |
| NMS-05     | Desempenho da solução                                 | Tempo de resposta das funcionalidades interativas contratadas.                                                                                  | Apurado mensalmente sobre as transações registradas na solução.                           | Até 5 (cinco) segundos em 95% das transações                                                                                                      |
| NMS-06     | Alteração de configurações                            | Solicitações de gestão de acesso, registros de auditoria da ferramenta ou outras configurações administrativas.                                 | Tempo decorrido entre a abertura do chamado e a implementação da solicitação.             | 8 horas após abertura de chamado                                                                                                                  |
| NMS-07     | Construção de dashboards                              | Solicitações de criação ou alteração de gráficos e disponibilização de painéis.                                                                 | Tempo decorrido entre a abertura do chamado e a disponibilização do acesso ao painel.     | 48 horas após abertura de chamado                                                                                                                 |
| NMS-08     | Construção de relatórios                              | Solicitações de criação de novos modelos de relatórios automatizados na ferramenta.                                                             | Tempo decorrido entre a abertura do chamado e a disponibilização do acesso ao relatório.  | 5 dias corridos após abertura de chamado                                                                                                          |
| NMS-09     | Construção de formulários                             | Solicitações de criação de novos modelos de formulários automatizados na ferramenta.                                                            | Tempo decorrido entre a abertura do chamado e a disponibilização do acesso ao formulário. | 5 dias corridos após abertura de chamado                                                                                                          |
| NMS-10     | Atendimento a chamados para esclarecimento de dúvidas | Suporte a dúvidas e questões relacionadas à solução ou aos serviços contratados.                                                                | Tempo decorrido entre a abertura do chamado e a resposta da solicitação.                  | 48 horas após abertura de chamado                                                                                                                 |

| REFERÊNCIA | MÉTRICA                             | DESCRIÇÃO                                                                                                          | DEFINIÇÃO                                                               | NMS - VALORES REFERÊNCIA                         |
|------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------|
| NMS-11     | Atualização de segurança da solução | Implementação de correções e atualizações de segurança, incluído o tempo de homologação do pacote pela CONTRATADA. | Tempo decorrido entre a liberação da atualização e a sua implementação. | 30 dias corridos após a liberação da atualização |
| NMS-12     | Configuração de integração          | Configuração de integração mediante conector ou interface já contemplada na solução contratada.                    | Tempo decorrido entre a solicitação e a conclusão da integração.        | 10 dias                                          |
| NMS-13     | Troca de informações                | Resposta a solicitações de informação formuladas pelos analistas do CONTRATANTE aos analistas da CONTRATADA.       | Tempo decorrido entre a solicitação e o recebimento da informação.      | 1 hora                                           |

14.4 Os indicadores mínimos deverão abranger, ao menos as seguintes dimensões:

- disponibilidade mensal da solução SaaS;
- tempo de resposta e de atendimento a chamados de suporte técnico, conforme nível de severidade;
- tempo de solução, contorno ou encaminhamento para tratamento de incidentes, falhas, indisponibilidades ou degradações de desempenho;
- tempo de comunicação ao Banco sobre incidentes de segurança da informação, privacidade, indisponibilidade relevante, falha de segregação, perda de dados ou suspeita de violação de dados pessoais;
- desempenho mínimo da solução, considerando tempo de resposta, estabilidade, acesso às funcionalidades contratadas e experiência de uso compatível com a finalidade da contratação;
- cumprimento dos prazos de implantação, configuração, parametrização, integração, migração inicial, repasse de conhecimento e entrada assistida em produção;
- cumprimento dos prazos de atualização, correção, manutenção e tratamento de vulnerabilidades que possam afetar a solução ou as informações do Banco;
- cumprimento dos requisitos de backup, restauração, continuidade, recuperação de desastres, RTO, RPO, portabilidade, exportação de dados e reversibilidade contratual;
- atendimento aos prazos de disponibilização de relatórios, logs, evidências, trilhas de auditoria, indicadores e demais informações necessárias à fiscalização contratual;
- qualidade dos serviços técnicos especializados sob demanda, considerando entrega, aceite, aderência ao escopo, documentação, tempestividade e atendimento aos critérios definidos pelo Banco.

14.5 Os chamados, incidentes, solicitações e demandas deverão ser classificados por níveis de severidade, considerando impacto, urgência, criticidade, indisponibilidade, risco à segurança da informação, risco à privacidade, risco regulatório, quantidade de usuários afetados, extensão dos dados envolvidos e potencial impacto à operação do Banco.

14.6 Para fins de definição dos níveis de severidade, deverão ser considerados, no mínimo, os seguintes agrupamentos:

| REFERÊNCIA | SEVERIDADE                       | DESCRIÇÃO                                                                                                                        | PRAZO MÁXIMO PARA PRIMEIRA RESPOSTA DE ATENDIMENTO REMOTO | PRAZO MÁXIMO DA SOLUÇÃO REMOTA                                   |
|------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------|
| NMS-14     | Urgente / Crítica / Severidade 1 | A solução está totalmente parada ou inoperante.                                                                                  | Até 2 (duas) horas após a abertura do chamado remoto.     | Até 24 (vinte e quatro) horas após a abertura do chamado remoto. |
| NMS-15     | Alta / Severidade 2              | A solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando impacto negativo no ambiente de produção. | Até 4 (quatro) horas após a abertura do chamado remoto.   | Até 2 (dois) dias após a abertura do chamado remoto.             |
| NMS-16     | Normal / Severidade 3            | A solução está operativa, mas suas funcionalidades são executadas com restrições.                                                | Até 8 (oito) horas após a abertura do chamado remoto.     | Até 4 (quatro) dias após a abertura do chamado remoto.           |
| NMS-17     | Baixa / Severidade 4             | A solução está operativa e a falha não compromete suas funcionalidades.                                                          | Até 12 (doze) horas após a abertura do chamado remoto.    | Até 6 (seis) dias após a abertura do chamado remoto.             |

14.7 Integram o conjunto de Níveis Mínimos de Serviço da contratação, em série numérica única com as tabelas acima, os seguintes indicadores:

- k) NMS-18 – Cumprimento do cronograma de implantação: atendimento integral dos marcos do Plano de Implantação homologado pelo CONTRATANTE, apurado na emissão do Termo de Aceitação Definitivo.
- l) NMS-19 – Entrega da documentação técnica e operacional da implantação, inclusive da documentação das parametrizações realizadas: até 10 (dez) dias úteis contados da entrada em produção.
- m) NMS-20 – Realização das turmas de capacitação e entrega dos materiais de apoio previstos no item de transferência de conhecimento: conforme cronograma homologado, com índice mínimo de 95% (noventa e cinco por cento) das turmas realizadas nas datas pactuadas.
- n) NMS-21 – Prazo de entrega dos serviços técnicos especializados, contado da emissão da Ordem de Serviço: 5 (cinco) dias úteis para entregas de complexidade baixa, 10 (dez) dias úteis para complexidade média e 20 (vinte) dias úteis para complexidade alta, salvo prazo diverso pactuado na própria Ordem de Serviço.
- o) NMS-22 – Índice de aceite das entregas dos serviços técnicos especializados na primeira apresentação: mínimo de 90% (noventa por cento) das entregas apuradas no trimestre.
- p) NMS-23 – Prazo para correção de entrega devolvida de forma motivada pelo CONTRATANTE: 5 (cinco) dias úteis contados da devolução.
- q) NMS-24 – Entrega do Relatório de Serviços Prestados: até o 5º (quinto) dia útil do mês subsequente, sendo a sua apresentação condição para o pagamento.
- r) NMS-25 – Atendimento a solicitação de exportação ou devolução de dados: até 10 (dez) dias úteis, em formato estruturado, aberto ou amplamente utilizado, acompanhado de dicionário de dados e leiaute.

14.8 A numeração dos indicadores é única e vinculante para o Estudo Técnico Preliminar, para o Termo de Referência, para os seus anexos e para a minuta contratual, vedada a reutilização da mesma referência para obrigações distintas.

14.9 O descumprimento dos NMS/SLA deverá sujeitar a contratada às glosas, descontos, multas, sanções ou demais consequências contratuais previstas no Termo de Referência e na minuta contratual, observados os princípios da proporcionalidade, razoabilidade, gradação da penalidade, materialidade do descumprimento, reincidência, impacto causado, nexo causal e direito ao contraditório e à ampla defesa.

14.9.1 As glosas ou penalidades decorrentes do descumprimento dos NMS/SLA deverão incidir preferencialmente sobre a parcela do serviço afetado, evitando-se dupla penalização pelo mesmo fato e assegurando-se correlação entre a obrigação descumprida, o impacto produzido e a sanção aplicada.

14.9.2 Os NMS/SLA não afastam a responsabilidade da contratada pela adoção de medidas corretivas, preventivas e de melhoria contínua, especialmente em caso de falhas recorrentes, incidentes relevantes, degradação de desempenho, descumprimento de prazos, fragilidades de segurança, indisponibilidade da solução ou risco à proteção de dados pessoais.

14.9.3 O descumprimento dos indicadores NMS-18 a NMS-20 sujeita a CONTRATADA a desconto de 0,5% (cinco décimos por cento) do valor do respectivo item por dia útil de atraso, limitado a 10% (dez por cento) do valor do item.

14.9.4 O descumprimento do indicador NMS-21 sujeita a CONTRATADA a desconto de 2% (dois por cento) do valor da entrega por dia útil de atraso, limitado a 20% (vinte por cento) do valor da entrega. O descumprimento do NMS-22, apurado trimestralmente, sujeita a CONTRATADA a desconto de 5% (cinco por cento) sobre o valor das entregas aceitas no trimestre.

14.9.5 Os descontos por descumprimento de Nível Mínimo de Serviço constituem adequação do pagamento ao serviço efetivamente prestado, na linha do Acórdão nº 717/2010-Plenário do Tribunal de Contas da União, e não se confundem com as sanções administrativas previstas neste instrumento, vedada a dupla incidência pelo mesmo fato.

## **15 DOTAÇÃO ORÇAMENTÁRIA**

15.1 Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto desta contratação estão previstos no orçamento do Banco da Amazônia, na(s) rubrica(s) abaixo, cujo valor será retificado após a conclusão da pesquisa de preços e a definição do valor estimado da contratação:

| ITEM | RUBRICAS                                                                                      | OBJETO                                                                                                                                                       | PRAZO        |
|------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1    | 8.1.7.39.00.00.0036 – 82.117-9 - DESPESAS DE PROC DADOS_GESTÃO PRIVAC PROTEÇÃO DADOS PESSOAIS | Subscrição corporativa (SaaS), implantação, transferência de conhecimento, suporte e sustentação, serviços técnicos especializados e saldo de horas técnicas | Até 60 meses |

## **16 PRAZO DE VIGÊNCIA**

16.1 O prazo de vigência do Contrato será de 05 (cinco) anos contados a partir da data de sua assinatura, nos termos do Artigo 71, da Lei nº 13.303/2016.

16.2 A cada ciclo anual de vigência, o contrato será avaliado quanto à manutenção da vantajosidade, mediante comparação do preços contratado com os preços praticados no mercado e verificação da aderência funcional da solução às necessidades do Banco, podendo resultar em redimensionamento dos quantitativos, renegociação de preços ou não prorrogação, observados os limites do art. 81 da Lei nº 13.303/2016 e o art. 92, item 5, do Regulamento de Licitações e Contratos do Banco da Amazônia.

## **17 CONDIÇÕES DE REAJUSTE DE PREÇOS**

17.1 Os preços serão reajustados com intervalo mínimo de um ano, contado da data do orçamento estimado a que a proposta se referir, pelo índice ICTI/IPEA apurado no período ou, na sua extinção ou indisponibilidade, pelo IPCA/IBGE.

17.2 Os reajustes subsequentes observarão o interregno mínimo de um ano a contar da data base de reajuste do ano anterior.

17.3 A variação cambial de natureza ordinária permanece alocada à CONTRATADA, decisão gerencial adotada de forma consciente e registrada na Matriz de Riscos, cabendo à licitante considerá-la na formação do preço. A variação cambial de natureza extraordinária e imprevisível, que onere excessivamente a execução, poderá ensejar a revisão contratual para restabelecimento do equilíbrio econômico-financeiro, mediante requerimento fundamentado e demonstração do impacto sobre a planilha de custos.

## **18 ALTERAÇÃO DO CONTRATO**

18.1 A alteração incidente sobre o objeto do Contrato deve ser consensual e pode ser quantitativa, quando importa acréscimo ou diminuição do objeto do Contrato, ou qualitativa, quando a alteração diz respeito a características e especificações técnicas do objeto do Contrato.

18.2 A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do artigo 81 da Lei nº 13.303/2016, devendo observar o seguinte:

a) a aplicação dos limites deve ser realizada separadamente para os acréscimos e para as supressões, sem que haja compensação entre os mesmos;

b) deve ser mantida a diferença, em percentual, entre o valor global do Contrato e o valor orçado pelo BANCO DA AMAZÔNIA S.A.

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

a) os encargos decorrentes da continuidade do Contrato devem ser inferiores aos da rescisão contratual e aos da realização de um novo procedimento licitatório;

b) as consequências da rescisão contratual, seguida de nova licitação e contratação, devem importar prejuízo relevante ao interesse coletivo a ser atendido pela obra ou pelo serviço;

c) as mudanças devem ser necessárias ao alcance do objetivo original do Contrato, à otimização do cronograma de execução e à antecipação dos benefícios sociais e econômicos decorrentes;

d) a capacidade técnica e econômico-financeira da CONTRATADA deve ser compatível com a qualidade e a dimensão do objeto contratual aditado;

e) a motivação da mudança contratual deve ter decorrido de fatores supervenientes não previstos e que não configurem burla ao processo licitatório;

f) a alteração não deve ocasionar a transfiguração do objeto originalmente contratado em outro de natureza ou propósito diverso.

18.4 As alterações incidentes sobre o objeto devem ser:

a) instruídas com memória de cálculo e justificativas de competência do fiscal técnico e do fiscal administrativo do BANCO DA AMAZÔNIA S.A., que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites.

b) as justificativas devem ser ratificadas pelo gestor do Serviço do BANCO DA AMAZÔNIA S.A.

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

18.5 As alterações contratuais incidentes sobre o objeto e as decorrentes de revisão contratual devem ser formalizadas via termo aditivo firmado pela mesma autoridade que firmou o contrato, devendo o extrato do termo aditivo ser publicado no sítio eletrônico do BANCO DA AMAZÔNIA S.A.

18.6 Não caracterizam alteração do contrato e podem ser registrados por termo de apostilamento, dispensando a celebração de termo aditivo:

- a) a variação do valor contratual para fazer face ao reajuste de preços;
- b) as atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no Contrato;
- c) a correção de erro material havido no instrumento de Contrato;
- d) as alterações na razão ou na denominação social da CONTRATADA;

## **19 CRITÉRIOS DE MEDIÇÃO E PAGAMENTO**

- 19.1 Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.
- 19.2 No ato de recebimento o fiscal técnico emitirá um Termo de Recebimento Provisório no prazo estipulado no item anterior
- 19.3 Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 dias consecutivos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.
- 19.4 O recebimento definitivo ocorrerá no prazo de 15 dias consecutivos, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.
- 19.5 No ato de recebimento o fiscal técnico emitirá um Termo de Recebimento Definitivo no prazo estipulado no item anterior
- 19.6 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.
- 19.7 O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.
- 19.8 O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.
- 19.9 Os critérios de medição observarão a natureza de cada item, na forma a seguir.
- 19.10 Itens 1 e 2 – subscrição corporativa: medição mensal, a partir do mês subsequente à emissão do Termo de Aceitação Definitivo da implantação, mediante verificação da disponibilidade da solução e apuração do indicador NMS-01.
- 19.11 Item 3 – serviços de implantação: medição em parcela única, mediante Termo de Aceitação Definitivo, condicionado à verificação do atendimento integral do escopo, dos testes, da homologação e da entrega da documentação técnica e operacional.
- 19.12 Item 4 – transferência de conhecimento: medição em parcela única, mediante comprovação da realização das turmas previstas, das respectivas listas de presença e da entrega dos materiais, manuais e documentação das parametrizações.
- 19.13 Item 5 – serviços continuados de suporte técnico, manutenção, operação assistida e sustentação: medição mensal, a partir do mês subsequente à emissão do Termo de Aceitação Definitivo, mediante apuração dos indicadores aplicáveis e apresentação do Relatório de Serviços Prestados.

- 19.14 Item 6 – serviços técnicos especializados: medição por entrega aceita, mediante Ordem de Serviço, relatório técnico com evidências e Termo de Aceite da Entrega emitido pela área técnica do CONTRATANTE.
- 19.15 Item 7 – saldo de horas técnicas especializadas: medição por hora previamente autorizada via Ordem de Serviço, efetivamente executada, registrada, comprovada e aceita, vedado o pagamento de horas não autorizadas ou não comprovadas.
- 19.16 Não haverá pagamento por subscrições, módulos ou serviços não disponibilizados ou não efetivamente implantados, nem pagamento antecipado, em observância ao art. 3º, incisos I a IV, da Resolução CGPAR nº 29/2022.

## **20 PAGAMENTO AO FORNECEDOR**

20.1 O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados a partir da emissão do termo de recebimento definitivo, emitido pelos fiscais do contrato. O referido termo deve atestar o recebimento do serviço e/ou bem, o cumprimento do disposto nos itens abaixo, além de expressamente autorizar a emissão da nota fiscal.

20.2 O faturamento dos itens 1, 2 e 5 terá início no mês subsequente à emissão do Termo de Aceitação Definitivo da implantação; os itens 3 e 4 serão faturados em parcela única após o mesmo Termo; e os itens 6 e 7 serão faturados por entrega aceita e por hora autorizada, executada e aceita, respectivamente.

20.3 Notas Fiscais emitidas após o 25º do mês subsequente a prestação do serviço e/ou entrega do bem não serão aceitas pelo contratante, devendo o contratado emití-las a partir do 1º dia útil do mês seguinte

20.4 No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA/IBGE de correção monetária.

20.5 Forma de pagamento

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

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

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

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

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

20.5.6 Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de trinta dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

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

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) o valor a pagar; e

f) eventual destaque do valor de retenções tributárias cabíveis.

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

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

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

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

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

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

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

## **21 DA GARANTIA DO CONTRATO**

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

- a) Garantia contratual de 5% (cinco por cento) do valor global do Contrato;
- b) A garantia oferecida pela CONTRATADA deve assegurar o cumprimento tanto do objetivo contratado, quanto das obrigações acessórias, inclusive trabalhistas;
- c) A CONTRATADA deverá providenciar a garantia contratual impreterivelmente em 10 (dez) dias úteis, contados a partir da assinatura do Contrato.
- d) No caso de CAUÇÃO EM DINHEIRO, o valor depositado será administrado pelo CONTRATANTE e devolvido à CONTRATADA após o ateste pelo Banco da inexistência de pendências contratuais de qualquer natureza e ainda do término e extinção do Contrato.
- e) Utilizada a garantia, por qualquer que seja o motivo, a CONTRATADA fica obrigada a integralizá-la no prazo de 5 (cinco) dias úteis contados da data em que for notificada formalmente pelo CONTRATANTE, sob pena de rescisão do Contrato.

- f) A garantia somente será devolvida à CONTRATADA quando do término ou rescisão do Contrato, desde que a CONTRATADA não possua dívida com o CONTRATANTE mediante expressa autorização deste.
- g) No caso de SEGURO-GARANTIA o CONTRATANTE deverá ser indicado como beneficiário do seguro-garantia e ter prazo de validade de pelo menos 3 (três) meses após o prazo previsto para término do contrato.
- h) O seguro-garantia deverá assegurar o pagamento de todas as obrigações contratuais previstas.
- i) A CONTRATADA obriga-se a apresentar nova apólice, até 5 (cinco) dias úteis após o vencimento da anterior e a comprovar o pagamento do prêmio respectivo, até 2 (dois) dias úteis após o seu vencimento.

21.2 No caso da FIANÇA BANCÁRIA deverão constar do instrumento os seguintes requisitos:

- a) Prazo de validade correspondente ao período de vigência do Contrato, acrescentado de 3 (três) meses após o prazo previsto para término do contrato.
- b) Expressa afirmação do fiador de que, como devedor solidário e principal pagador, fará o pagamento, ao CONTRATANTE, dos prejuízos por este sofridos, em razão do descumprimento das obrigações da CONTRATADA, independente de interpelação judicial; e Cláusula que assegure a atualização do valor afiançado.

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

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

## **22 DAS OBRIGAÇÕES DA CONTRATADA**

22.1 Executar o objeto do contrato de acordo com todos os termos estabelecidos no Termo de Referência e demais documentos que amparam a contratação.

22.2 Obedecer rigorosamente a todos os prazos contratados.

22.3 Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE e atender prontamente a eventuais solicitações/reclamações.

22.4 Dispor-se a toda e qualquer fiscalização do CONTRATANTE, no tocante ao cumprimento dos serviços e prazos contratados.

22.5 Prover todos os meios necessários à garantia da plena operacionalidade dos bens e serviços objeto do contrato.

22.6 Manter absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados que venham a ser disponibilizados pelo CONTRATANTE à CONTRATADA, em razão da execução dos serviços contratados.

22.7 Exercer suas atividades em conformidade com a legislação vigente.

22.8 Não se utilizar direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, de trabalho ilegal e/ou análogo ao escravo.

22.9 Não se utilizar de práticas de discriminação negativa e limitativa para o acesso e manutenção do emprego, tais como por motivo de sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar, estado gravídico, etc.

22.10 Proteger e preservar o meio ambiente, prevenindo práticas danosas e executando seus serviços em observância à legislação vigente, principalmente no que se refere aos crimes ambientais.

22.11 Providenciar a imediata correção das deficiências apontadas pelo CONTRATANTE, quanto ao objeto do contrato.

22.12 A CONTRATADA será responsável pelos danos de qualquer natureza que acarretar ao CONTRATANTE ou a terceiros em decorrência de negligência, imperícia ou imprudência por parte de seus empregados ou prepostos, na administração e execução dos serviços contratados, desde que devidamente comprovado.

22.13 Entrega dos serviços de implantação e manutenção da solução de acordo com especificações técnicas, garantindo funcionamento contínuo, atualizado e seguro, com suporte integrado.

22.14 Caberá integralmente à CONTRATADA a responsabilidade pelo suporte técnico, manutenção e sustentação da solução, abrangendo:

- a) Licenciamento de todos os componentes necessários à operação;
- b) Suporte técnico especializado;
- c) Aplicação de atualizações, correções e evoluções no sistema, durante a vigência do contrato.

22.15 A CONTRATADA deve ser integralmente responsável pelo suporte da solução, incluindo todos os elementos necessários para seu pleno funcionamento e manutenção - como licenças de software, infraestrutura e ambientes computacionais. Quaisquer ajustes no ambiente interno do Banco devem ser, obrigatoriamente, alinhados, acordados e validados previamente com a área de infraestrutura e produção da CONTRATANTE.

22.16 Executar os serviços de implantação e de transferência de conhecimento na forma, nos prazos e com os produtos definidos no Anexo V, arcando com todos os custos correspondentes.

22.17 Entregar a documentação técnica e operacional da implantação, incluindo a documentação das parametrizações realizadas, e promover o repasse formal das configurações à equipe do CONTRATANTE, com registro em ata.

22.18 Disponibilizar ambiente de homologação independente do ambiente de produção, sem custo adicional.

22.19 Não cobrar valores adicionais pela inclusão de usuários, perfis, unidades organizacionais, operações de tratamento, titulares, registros, evidências ou fontes de dados durante a vigência contratual, observados os limites de capacidade previstos no Anexo V.

22.20 Executar os serviços técnicos especializados exclusivamente mediante Ordem de Serviço, apresentando relatório técnico e evidências dos produtos entregues.

22.21 Registrar, de forma individualizada por profissional e atividade, as horas do saldo de horas técnicas efetivamente utilizadas, disponibilizando o registro ao CONTRATANTE.

22.22 Manter plano de reversibilidade atualizado e, ao término do contrato ou quando solicitado, exportar e devolver os dados em formato estruturado, aberto ou amplamente utilizado, acompanhados de dicionário de dados e leiaute, comprovando a eliminação segura das cópias remanescentes.

22.23 Observar as medidas de mitigação previstas no Relatório de Impacto à Proteção de Dados Pessoais da Contratação, em especial quanto à minimização dos dados coletados nas varreduras, ao mascaramento dos valores identificados, ao regime de acesso às bases de produção e à execução das varreduras em janelas ajustadas com o CONTRATANTE.

## **23 DAS OBRIGAÇÕES DO CONTRATANTE**

23.1 Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

23.2 Exercer a Fiscalização dos serviços por empregados especialmente designados, na forma prevista na Lei nº 13.303/2016 e Art. 99 do Regulamento do Banco da Amazônia.

23.3 Atestar através do Fiscal Técnico do Contrato as Notas Fiscais / Fatura de Serviços correspondentes às etapas executadas, após a verificação da conformidade dos serviços, para efeito de pagamento.

23.4 Rejeitar, no todo ou em parte, os serviços executados em desacordo com as respectivas especificações.

23.5 Efetuar o pagamento da Nota Fiscal / Fatura emitida pela CONTRATADA, desde que receba com antecedência mínima de 30 (trinta) dias do vencimento daquela Nota Fiscal / Fatura e que a realização dos serviços esteja devidamente comprovada pelo setor competente e de acordo com o requerido no Contrato.

23.6 Receber o preposto do CONTRATADO, devidamente identificados, devendo tomar as providências administrativas que garantam o livre desempenho de suas atividades.

23.7 Cuidar para que os empregados do CONTRATADO somente recebam ordens para a execução de tarefas, do Preposto da CONTRATADA.

23.8 Notificar a CONTRATADA, por escrito, da aplicação de eventuais penalidades ou acerca de falhas ou irregularidades encontradas na execução dos serviços, fixando-lhe prazo para corrigi-las.

23.9 Antes da assinatura do contrato ou da autorização para início de implantação, a solução deverá ser avaliada tecnicamente pelas áreas técnicas da CONTRATANTE, que validarão sua aderência aos requisitos de arquitetura, segurança, infraestrutura e integração.

23.10 Designar formalmente o gestor e os fiscais do contrato e comunicar à CONTRATADA os respectivos contatos.

23.11 Disponibilizar os acessos, ambientes, informações e interlocutores necessários à execução dos serviços de implantação, integração e transferência de conhecimento.

23.12 Homologar o Plano de Implantação e o cronograma das capacitações, manifestando-se nos prazos pactuados.

23.13 Emitir as Ordens de Serviço, avaliar as entregas e manifestar-se sobre o aceite nos prazos definidos, motivando eventual devolução.

23.14 Realizar, a cada ciclo anual de vigência, a avaliação da manutenção da vantajosidade da contratação.

## **24 DAS SANÇÕES ADMINISTRATIVAS**

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

- a) Advertência;
- b) Multa de 10% (dez por cento) sobre o valor global da contratação, pela inexecução total do ajuste;
- c) Multa diária de 0,2% (dois décimos por cento), calculado sobre o valor da respectiva fatura, quando houver atraso parcial na execução do objeto do contrato enquanto perdurar o inadimplemento;
- d) Suspensão do direito de licitar e de contratar com o Banco pelo prazo de até 2 (dois) anos;

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

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

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

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

24.6 As glosas e os descontos decorrentes do descumprimento dos Níveis Mínimos de Serviço constituem adequação do pagamento ao serviço efetivamente prestado, na linha do Acórdão nº 717/2010-Plenário do Tribunal de Contas da União, e não se confundem com as sanções administrativas previstas nesta seção, vedada a dupla incidência pelo mesmo fato.

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

24.8 Inexistindo pagamento devido ao Banco, ou sendo este insuficiente, caberá à parte contrária efetuar o pagamento do que for devido, no prazo máximo de 10 (dez) dias consecutivos, contados da data da comunicação de confirmação da multa, em depósito em conta corrente própria em nome do Banco.

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

## **25 DA RESCISÃO DO CONTRATO**

25.1 A rescisão poderá ocorrer:

- I. Mediante distrato pela inexecução total ou parcial das cláusulas contratuais;
- II. Por acordo entre as partes, reduzida a termo no processo de contratação desde que haja conveniência para o Banco, precedida de autorização escrita e fundamentada mediante aviso prévio por escrito de 30 (trinta) dias consecutivos; e
- III. Judicialmente nos termos da legislação. Sem prejuízo de outras sanções, constituem motivos para rescisão do Contrato, oriundo da contratação, as situações descritas nos subitens abaixo:
  - a) Paralisação injustificada dos serviços;
  - b) O não cumprimento de cláusulas contratuais, especificações ou prazos;
  - c) A subcontratação, ainda que parcial, dos serviços objeto do Contrato não autorizada pelo Contratante.
  - d) A subcontratação autorizada prévia e formalmente, com identificação do Suboperador, das atividades, dos dados envolvidos e da localização do tratamento, mantida a responsabilidade integral da contratada, não constituem motivos para rescisão do contrato.
  - e) A cessão ou transferência do contrato;
  - f) O desatendimento às determinações da FISCALIZAÇÃO designada para acompanhar e fiscalizar a execução dos serviços;
  - g) O cometimento reiterado de faltas na execução dos serviços;
  - h) A decretação de falência, o pedido de recuperação judicial ou extrajudicial;
  - i) A dissolução da sociedade;
  - j) A alteração societária que modifique a finalidade ou o controle acionário ou, ainda, a estrutura da CONTRATADA que, a juízo da CONTRATANTE, inviabilize ou prejudique a execução deste Contrato;
  - k) A prática de qualquer ato que vise fraudar ou burlar o fisco ou CONTRATANTE arrecadador/credor dos encargos sociais e trabalhistas ou de tributos;
  - l) O descumprimento de quaisquer das condições ajustadas no Contrato;

- m) A utilização pela CONTRATADA de mão-de-obra de menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendizes, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal (Emenda Constitucional nº 20, de 1998);
- n) O conhecimento, ainda que, “a posteriori”, de fato ou ato que afete a idoneidade da CONTRATADA ou de seus sócios/cotistas ou de seus gestores ou ainda de seus representantes;
- o) Razões de interesse público;
- p) Ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução deste Contrato;
- q) Deixar de comprovar sua regularidade fiscal, trabalhista, inclusive contribuições previdenciárias e depósitos de FGTS para com seus empregados; e
- r) Utilizar em benefício próprio ou de terceiras informações sigilosas às quais tenha acesso por força de suas atribuições.

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

25.3 Também poderá ocorrer rescisão quando:

- a) Não prestar garantia suficiente para assegurar o cumprimento das obrigações contratuais;
- b) Deixar de comprovar sua regularidade, trabalhista, fiscal, inclusive contribuições previdenciárias e depósitos do FGTS dos seus funcionários;
- c) Vier a ser declarada inidônea por qualquer órgão ou entidade da Administração Pública;
- d) Vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira;
- e) Utilizar em benefício próprio ou de terceiros, informações sigilosas às quais tenha acesso por força de suas atribuições contratuais.

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

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

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

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

## **26 DOS CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL, SOCIAL E TRABALHISTA E ECONÔMICA FINANCEIRA**

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

### **Habilitação Jurídica**

26.2 Para sua habilitação jurídica, o proponente deve comprovar a possibilidade de exercer direitos e assumir obrigações, devendo comprovar essa condição através por meio de carteira de identificação, contrato social, estatuto social ou outro documento constitutivo compatível com o objeto da contratação, bem como documento que comprove os poderes de seus representantes e decreto de autorização de funcionamento para empresas estrangeiras, conforme exigido neste Termo de Referência.

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

#### **Habilitação Fiscal, Social e Trabalhista**

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

- I. A inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ) – Cartão CNPJ;
- II. A inscrição no cadastro de contribuintes estadual e municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual – Comprovante de Inscrição na Fazenda Municipal e Estadual ou Distrital;
- III. A regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei – Certidão Negativa ou Positiva com efeito de Negativa de Regularidade perante a Fazenda Federal, Estadual e Municipal ou Distrital;
- IV. A regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei - Certidão Negativa ou Positiva com efeito de Negativa de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União / Certidão de Regularidade do FGTS (CRF).
- V. A regularidade perante a Justiça do Trabalho - Certidão Negativa ou Positiva com efeito de Negativa de Débitos Trabalhistas - CNDT;
- VI. Declaração de não empregar menor – Art. 7º, inciso XXXIII, CF;
- VII. Declaração de Conhecimento do decreto nº 7.203 de 04/06/2010;

26.5 Os documentos referidos no parágrafo anterior poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico, desde que por meios legalmente idôneos.

#### **Habilitação Econômico-Financeira**

26.6 Para fins de habilitação econômico-financeira, apresentar o balanço patrimonial e demonstrações contábeis referentes ao último exercício social, exigíveis na forma da lei, que comprove a boa situação financeira por meio da satisfação de índices de liquidez geral (LG), liquidez corrente (LC), e solvência geral (SG) superiores a 1 (um), com indicação dos seus cálculos, que deverão ser realizados de acordo com as seguintes fórmulas:

ativo circulante + realizável a longo prazo LG =

passivo circulante + passivo não circulante

ativo circulante

LC =

passivo circulante

ativo total

SG =

passivo circulante + passivo não circulante

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

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

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

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

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

26.12 Microempresas e empresas de pequeno porte deverão atender a todas as exigências de habilitação previstas neste Termo de Referência.

## **27 CONDIÇÕES DE PARTICIPAÇÃO**

27.1 A propensa contratada deverá apresentar “Declaração de conhecimento do Art. 38 da Lei 13.303/16”, na forma do anexo estabelecido no processo de contratação do Banco.

27.2 A propensa contratada deverá apresentar “Declaração de Inexistência de Fato Impeditivo ou Superveniente”, na forma do anexo estabelecido no processo de contratação do Banco.

27.3 A propensa contratada deverá apresentar “Declaração de não existência em seu quadro empregado do Banco”, na forma do anexo estabelecido no processo de contratação do Banco.

27.4 A propensa contratada deverá apresentar “Declaração de conhecimento da Lei de Improbidade Administrativa”, na forma do anexo estabelecido no processo de contratação do Banco.

27.5 A propensa contratada deverá apresentar “Declaração de ME e EPP” na forma do anexo estabelecido no processo de contratação do Banco.

27.6 O Banco da Amazônia realizará consultas à lista restritivas de Prevenção e Lavagem de Dinheiro (PLD), sendo que a propensa contratada não poderá apresentar restrições nas referidas listas, sob pena de desclassificação, salvo se deliberado pelo comitê competente do Banco.

## **28 DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA**

28.1 A licitante deverá apresentar, no mínimo, 1 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em documento timbrado, que comprove a sua aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da presente contratação, admitido o somatório de atestados.

28.2 A comprovação a que se refere o item anterior deverá abranger 50% (cinquenta por cento) dos grupos de requisitos funcionais previstos no Anexo V deste Termo de Referência, percentual fixado com fundamento no art. 79, itens 2 e 3, do Regulamento de Licitações e Contratos do Banco da Amazônia.

28.2.1 Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de fornecimento de solução e prestação de serviços em características e quantidades compatíveis com a presente licitação, mediante apresentação de ATESTADO (S) DE CAPACIDADE TÉCNICA que deverão comprovar o atendimento aos seguintes requisitos:

28.2.2 Fornecimento de solução de governança, gestão e conformidade em privacidade e proteção de dados pessoais na modalidade Software como Serviço e de componente de descoberta e classificação de dados pessoais em bases estruturadas e não estruturadas, admitida a

comprovação por atestados distintos e o somatório de quantitativos, não se exigindo que ambos os componentes constem de um mesmo atestado.

28.2.3 Comprovação da experiência mínima de 1 (um) ano na execução dos serviços contínuos de suporte técnico relacionado a solução ofertada, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de serem ininterruptos; e

28.2.4 Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação.

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

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

28.5 As propensas CONTRATADAS disponibilizarão todas as informações necessárias à comprovação da legitimidade dos atestados apresentados.

28.6 A critério do CONTRATANTE, nas situações em que julgar necessário, poderão ser realizadas inspeções e diligências com a finalidade de entender, esclarecer e/ou comprovar as informações contidas no (s) ATESTADO (S) DE CAPACIDADE TÉCNICA entregue (s) – nos termos da Lei nº 13.303/2016. Assim como poderão ser solicitadas cópias de documentos complementares como contratos, notas fiscais e notas de empenho. Porém, não serão executadas diligências para acrescentar informações obrigatórias ausentes no (s) atestado (s) apresentado (s). A eventual recusa do (s) emitente (s) do (s) ATESTADO (S) em prestar esclarecimentos e/ou fornecer documentos comprobatórios, ou sofrer diligências, ou a constatada inexatidão das informações atestadas, desconstituirá o (s) ATESTADO (S) – o que poderá, inclusive, configurar prática criminosa, ensejando comunicação ao órgão competente.

28.7 A proposta deverá ser encaminhada juntamente com os documentos da solução ofertada e com planilha ponto a ponto que permita comprovar o atendimento aos requisitos técnicos exigidos no Anexo V deste Termo de Referência, contendo, no mínimo:

28.7.1 Id e descrição do Requisito;

28.7.2 Nome do Produto Ofertado;

28.7.3 Nome do documento de referência onde é possível verificar evidência do atendimento ao requisito;

28.7.4 Página do documento referência onde é possível verificar evidência do atendimento ao requisito;

28.7.5 Outras informações necessárias.

## **29 DOS CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA**

29.1 A licitante mais bem classificada deverá encaminhar a proposta de preço adequada ao último lance, no prazo de 2 (duas) horas, prorrogável por igual período, contado da convocação efetuada pelo Pregoeiro.

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

29.3 Serão objeto de análise de exequibilidade as propostas que apresentem indícios de insuficiência para cobertura dos custos da contratação. A Administração poderá promover diligências e exigir documentos comprobatórios da formação dos custos ofertados.

- 29.4 O Pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor estimado e à compatibilidade da proposta com as especificações técnicas do objeto, inclusive no que tange aos preços unitários cotados pelo Banco da Amazônia.
- 29.5 O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do Banco da Amazônia ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.
- 29.6 Não se considerará qualquer oferta de vantagem não prevista no edital, inclusive financiamentos subsidiados ou a fundo perdido.
- 29.7 Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.
- 29.8 Não serão aceitas propostas com valor unitário ou global superior ao estimado, seja por item ou global.
- 29.9 A licitante deverá apresentar planilha de composição do preço segregando os componentes de subscrição, implantação, transferência de conhecimento, suporte e sustentação, serviços técnicos especializados por faixa de complexidade e saldo de horas técnicas, vedada a compensação entre itens que resulte em preço unitário incompatível com o mercado.
- 29.10 Os critérios de aceitabilidade são cumulativos, verificando-se tanto o valor global quanto os valores unitários estimativos da contratação.
- 29.11 Será desclassificada a proposta que:
- 29.11.1 Contiver vícios insanáveis;
- 29.11.2 Não obedecer às especificações técnicas pormenorizadas no edital;
- 29.11.3 Apresentar preços inexequíveis ou permanecer acima do orçamento estimado para a contratação;
- 29.11.4 Não tiver sua exequibilidade demonstrada, quando exigido pelo Pregoeiro;
- 29.12 Será desclassificada a proposta que:
- 29.13 Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão.
- 29.14 Apresentar desconformidade com quaisquer outras exigências do edital, desde que insanável;
- 29.15 Não corrigir ou não justificar eventuais falhas apontadas pelo Pregoeiro. A licitante que abandonar o certame, deixando de enviar a documentação indicada no edital, será desclassificada e sujeitar-se-á às sanções previstas no instrumento convocatório.

### **30 PROVA DE CONCEITO/AMOSTRA**

- 30.1 As condições de prova de conceito/amostra estão previstas no Anexo VI do presente termo de referência.

### **31 DA OBRIGAÇÃO DE MANUTENÇÃO DOS CRITÉRIOS DE HABILITAÇÃO JURÍDICA, FISCAL, TRABALHISTA E ECONÔMICO FINANCEIRO E QUALIFICAÇÃO TÉCNICA EXIGIDAS**

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

### **32 DO SIGILO E RESTRIÇÕES**

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

### **33 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS**

- 33.1 A CONTRATADA, por si e por seus colaboradores, deverá:

- 33.1.1 atuar em conformidade com a Legislação vigente sobre proteção de dados pessoais;

33.1.2 atuar em conformidade com as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial à Lei 13.709/2018 (Lei Geral de Proteção de Dados) sempre que lhe couber, em virtude da execução do objeto deste contrato; e

33.1.3 atender às demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos Dados da CONTRATANTE, o que inclui os Dados dos clientes desta.

33.2 Todo tratamento de dado pessoal decorrente da implementação deste contrato deve seguir as exigências da Lei Geral de Proteção de Dados Pessoais e as diretrizes abaixo elencadas:

33.3 A CONTRATADA observará as medidas de mitigação previstas no Relatório de Impacto à Proteção de Dados Pessoais da Contratação, integrante do Estudo Técnico Preliminar, em especial quanto à minimização dos dados coletados nas varreduras, ao mascaramento dos valores identificados, ao regime de acesso às bases de produção e à execução das varreduras em janelas ajustadas com a CONTRATANTE.

**33.3.1 Diretrizes de tratamento:** Considerando que competirá à CONTRATANTE as decisões referentes ao tratamento dos Dados Pessoais (sendo portanto Controladora) e que a CONTRATADA realizará o tratamento dos Dados Pessoais sem nome da CONTRATANTE (sendo portanto Operadora), a CONTRATADA seguirá estritamente as instruções recebidas da CONTRATANTE em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, devendo a CONTRATADA garantir sua licitude e idoneidade, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis.

33.3.2 A CONTRATADA deverá corrigir, completar, excluir e/ou bloquear os Dados Pessoais, caso seja solicitado pela CONTRATANTE.

**33.3.3 Solicitações de Titulares:** A CONTRATADA deverá notificar a CONTRATANTE sobre quaisquer reclamações e solicitações dos Titulares de Dados Pessoais que ocorram em virtude deste Contrato, no prazo máximo de 24h.

**33.3.4 Confidencialidade dos Dados Pessoais:** A CONTRATADA, incluindo todos os seus colaboradores, deverá tratar todos os Dados Pessoais a que tiver acesso por meio deste Contrato, como confidenciais, ainda que este Contrato venha a ser resolvido, e independentemente dos motivos que derem causa ao seu término ou resolução.

**33.3.5 Governança e segurança:** A CONTRATADA deverá adotar medidas, ferramentas e tecnologias necessárias para garantir a segurança dos dados e cumprir com suas obrigações adotando sempre as mais eficazes práticas de mercado. A CONTRATADA deverá cumprir com os requisitos das medidas de segurança técnicas e organizacionais para garantir a confidencialidade, pseudonimização e a criptografia dos Dados Pessoais, inclusive no seu armazenamento e transmissão.

33.3.6 Sempre em observância à melhores práticas de mercado, a CONTRATADA deverá utilizar tecnologias visando à proteção das informações em todas as comunicações, especialmente nos compartilhamentos de Dados Pessoais pela CONTRATADA à CONTRATANTE, a exemplo de padrão seguro de transmissão dados e criptografia.

33.3.7 A CONTRATADA deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado por ela para o tratamento de Dados Pessoais são estruturados de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos em Lei e às demais normas regulamentares aplicáveis.

**33.3.8 Registo de atividades:** A CONTRATADA deverá realizar o registro de todas as atividades realizadas em seus sistemas/ambientes enquanto vigor este Contrato, incluindo qualquer

atividade relativa à Dados Pessoais tratados sob determinação da CONTRATANTE, de modo a permitir a identificação de quem as realizou.

**33.3.9 Conformidade da CONTRATADA:** A CONTRATADA deverá monitorar, por meios adequados, sua própria conformidade e a de seus empregados com as respectivas obrigações de proteção de Dados Pessoais em relação aos Serviços e deverá fornecer à CONTRATANTE relatórios sobre esses controles sempre que solicitado por ela.

**33.3.10** Os relatórios acima citados deverão incluir, pelo menos:

- a) o status dos sistemas de processamento de Dados Pessoais;
- b) as medidas de segurança;
- c) o tempo de inatividade registrado das medidas técnicas de segurança;
- d) a (não) conformidade estabelecida com as medidas organizacionais;
- e) quaisquer eventuais violações de dados e/ou incidentes de segurança;
- f) as ameaças percebidas à segurança e aos Dados Pessoais; e
- g) as melhorias exigidas e/ou recomendadas.

**33.3.11 Monitoramento de conformidade:** A CONTRATANTE terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da CONTRATADA com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a CONTRATADA possui perante a Lei e este Contrato.

**33.3.12 Notificação:** A CONTRATADA deverá notificar a CONTRATANTE em até 24h (vinte e quatro) horas em caso de:

- a) qualquer descumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais;
- b) qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais;
- c) qualquer violação de segurança na CONTRATADA;
- d) quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; e
- e) ou em período menor, se necessário, de qualquer ordem de Tribunal, ou em período menor, se necessário, de qualquer ordem de Tribunal.

**33.3.13 Colaboração:** A CONTRATADA compromete-se a auxiliar a CONTRATANTE:

- a) com a suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados Pessoais aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e
- b) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.

**33.3.14 Propriedade dos Dados:** a presente contratação não transfere a propriedade ou controle dos dados da CONTRATANTE ou dos clientes desta, inclusive Dados Pessoais, para a CONTRATADA. Os Dados gerados, obtidos ou coletados a partir da prestação dos Serviços a serem contratados são e continuarão sendo de propriedade da CONTRATANTE, inclusive sobre qualquer novo elemento de Dados, produto ou subproduto que seja criado a partir do tratamento de Dados estabelecido por essa contratação.

**33.3.15 Tratamento de dados no exterior:** todo e qualquer tratamento de dados fora do território nacional dependerá de autorização prévia, formal e específica da CONTRATANTE, e

somente poderá ocorrer mediante observância dos arts. 33 a 36 da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 19/2024, com identificação dos países envolvidos, do mecanismo de transferência adotado, das garantias contratuais aplicáveis e das medidas de segurança correspondentes, preservados o acesso da CONTRATANTE e dos órgãos reguladores competentes e observada a Resolução CMN nº 4.893/2021.

33.3.16 **Atuação restrita:** A CONTRATADA não estará autorizada pela CONTRATANTE a usar, compartilhar ou comercializar quaisquer eventuais elementos de Dados, produtos ou subprodutos que se originem ou sejam criados a partir do tratamento de Dados estabelecido por esta contratação.

33.3.17 **Adequação legislativa:** Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços à CONTRATANTE ou na execução das atividades ligadas a esta contratação, a CONTRATADA deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a CONTRATADA deverá notificar formalmente este fato à CONTRATANTE, que terá o direito de resolver o Contrato sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

33.3.18 Se qualquer legislação nacional ou internacional aplicável ao tratamento de Dados Pessoais no âmbito desta contratação vier a exigir adequação de processos e/ou instrumentos contratuais por forma ou meio determinado, a CONTRATADA desde já acorda em celebrar termo aditivo escrito neste sentido.

33.3.19 **Solicitação de Dados ou Registros:** Sempre que Dados ou Registros forem solicitados pela CONTRATANTE à CONTRATADA, a mesma deverá disponibilizá-los em até 48 (quarenta e oito) horas, podendo ser em menor prazo nos casos em que a demanda judicial, a norma aplicável, ou o pedido de autoridade competente assim o exija. Caso a CONTRATADA receba diretamente alguma ordem judicial para fornecimento de quaisquer Dados, deverá comunicar a CONTRATANTE antes de fornecê-los, se possível.

33.3.20 **Devolução dos Dados:** A CONTRATADA deverá devolver todos os Dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que:

- a) a CONTRATANTE solicitar;
- b) o Contrato for rescindido; ou
- c) com o término do contrato.

33.3.21 A CONTRATADA não deverá guardar, armazenar ou reter os Dados por tempo superior ao prazo legal ou necessário para a execução do Contrato.

33.3.22 Caso os Dados da CONTRATADA estejam contidos em um banco de Dados, além de restituir este banco de Dados de inteira propriedade da CONTRATANTE em qualquer hipótese de extinção do contrato, a CONTRATADA deverá remeter em adição o dicionário de dados que permita entender a organização do banco de Dados, em até 10 (dez) dias ou em eventual prazo acordado entre as Partes.

33.3.23 **Regresso:** Fica assegurado à CONTRATANTE, nos termos da lei, o direito de regresso em face da CONTRATADA no caso de danos causados por esta em decorrência do descumprimento das obrigações assumidas em relação à Proteção dos Dados. A responsabilidade da CONTRATADA diante do referido descumprimento é ilimitada, não produzindo nenhum efeito qualquer outra cláusula que disponha de forma contrária.

## 34 FISCALIZAÇÃO DO CONTRATO

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

34.2 A fiscalização da entrega do objeto da contratação será realizada pelo CONTRATANTE que designará representante para o gerenciamento do cumprimento das obrigações previstas neste contrato.

34.3 A ausência ou omissão da Fiscalização do CONTRATANTE não eximirá a CONTRATADA das responsabilidades previstas neste Termo de Referência.

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

### **35 MATRIZ DE RISCO**

35.1 Fica consignado para presente contratação a divisão dos riscos conforme Matriz de Riscos constante no Anexo I, deste Termo de Referência, repartindo os riscos assumidos por cada uma das partes na celebração da presente contratação.

### **36 DAS VEDAÇÕES**

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

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

### **37 DA INTEGRIDADE, DA CONDUTA ÉTICA E DOS PROCEDIMENTOS ANTICORRUPÇÃO**

37.1 O contrato oriundo da presente contratação deverá prever que as Partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa - Lei nº 8.429, de 02 de junho de 1992 e a Lei Anticorrupção

37.2 Lei nº 12.846, de 01 de agosto de 2013 e seus regulamentos e se comprometem a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores, bem como exigir o seu cumprimento pelos terceiros por elas contratados. Adicionalmente, as Partes declaram que tem e manterão até o final da vigência do contrato, oriundo desta contratação, um código de ética e conduta próprio, cujas regras se obriga a cumprir fielmente.

37.3 Sem prejuízo da obrigação de cumprimento das disposições de seus respectivos códigos de ética e conduta, ambas as Partes desde já se obrigam, no exercício dos direitos e obrigações previstos no Contrato e no cumprimento de qualquer uma de suas disposições:

- I. Não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente;
- II. Adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados;
- III. Respeitar e exigir que seus empregados respeitem, no que couber, os princípios éticos e os compromissos de conduta definidos no Código de Conduta Ética do BASA, cujo teor poderá ser acessado no site: <https://bancoamazonia.com.br/component/edocman/relacoes-investidores/governanca-corporativa/codigo-etica> .

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

37.5 A aplicação das sanções previstas na Lei nº 12.84, de 2013 não afeta os processos de responsabilização e aplicação de penalidades decorrentes de atos ilícitos.

### **38 DOS CRITÉRIOS DE SUSTENTABILIDADE**

38.1 A CONTRATADA se compromete a atender às diretrizes da Política de Responsabilidade Socioambiental do Banco da Amazônia – PRSAC, disponível em <https://www.bancoamazonia.com.br/component/edocman/prsac/viewdocument/5204> e a Política Geral de Contratações, disponível em <https://www.bancoamazonia.com.br/component/edocman/politica-geral-de-contratacoes/viewdocument/5727>, considerando os requisitos a seguir:

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

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

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

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

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

38.1.6 Desenvolver suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados a proteções dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se:

- a) “Condições ultrajantes”: condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo.
- b) “Condições sub-humanas”: tudo que está abaixo da condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano, situação abaixo da linha da pobreza.
- c) “Condições degradantes de trabalho”: condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão.

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

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

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

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

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

### 39 FORO

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

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

**X**

Eduardo da Costa Dias Junior  
Gerente Executivo - GESEC

**X**

Leandro Eduardo Valente dos Santos  
Coordenador-COFRA

**X**

Janio Heron Polmeier Neves  
Coordenador - COPIL

**X**

Alexandre Henrique Ichihara Pires  
Analista

- Anexo I - Matriz de Risco
- Anexo II e III - Termo de Confidencialidade e Sigilo, quando for o caso;
- Anexo IV - Requisitos mínimos de segurança para sistemas adquiridos
- Anexo V – Especificações Técnicas da Solução
- Anexo VI – Roteiro do Teste de Prova de Conceito - POC
- Anexo VII - Carta de apresentação de proposta.
- Anexo VIII – Catálogo de serviços.

**ANEXO I**  
**MATRIZ DE RISCOS**

| ID. | CATEGORIA DO RISCO                                     | DESCRIÇÃO                                                                                                                          | CONSEQUÊNCIA                                                                                                                                                               | MEDIDAS MITIGADORAS                                                                                                                                                                                                                                                                                                                                                                                                                                                    | ALOCÇÃO DO RISCO |
|-----|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| R1  | Risco atinente à solução (Planejamento da Contratação) | Dimensionamento inadequado do volume de bens/serviços a serem contratados.                                                         | Volume subdimensionado ou superdimensionado dos itens que compõem a solução e possível realização de aditivos contratuais extemporâneos num cenário de subdimensionamento. | a) Definir parâmetros objetivos para a definição da volumetria, com base no ambiente tecnológico do órgão e suas necessidades. b) Evidência de implementação: substituição da métrica de licenciamento por subscrição corporativa medida em meses, conversão da volumetria das bases em requisito mínimo de capacidade e registro da memória de dimensionamento na seção "Descrição da solução como um todo".                                                          | Contratante      |
| R2  | Risco atinente à solução (Planejamento da Contratação) | Necessidade de adequação e/ou não aprovação dos artefatos de planejamento da contratação decorrentes da análise jurídica/tribunal. | Atraso no processo da contratação e retrabalho da equipe de planejamento.                                                                                                  | a) Considerar na elaboração dos artefatos de planejamento soluções similares em outros órgãos. b) Considerar na elaboração do TR e do Edital os pontos recorrentes passíveis de questionamentos e recomendações. c) Evidência de implementação: incorporação das providências indicadas na análise jurídica e registro do tratamento de cada achado do Acórdão nº 1.441/2026-Plenário no Estudo Técnico Preliminar.                                                    | Contratante      |
| R3  | Risco atinente à solução (Planejamento da Contratação) | Dependência Tecnológica e Indisponibilidade da solução por erro e/ou falha na instalação e parametrização.                         | Indisponibilidade da solução ou falhas/erros e/ou inoperantes com dependência Tecnológica.                                                                                 | a) Definir no TR requisitos tecnológicos e níveis de serviço adequados que a solução deverá atender. b) Prever solução de continuidade dos serviços com a utilização de outras ferramentas disponíveis no ambiente tecnológico do CONTRATANTE. c) Evidência de implementação: inclusão dos indicadores NMS-01 a NMS-05, das exigências de portabilidade e reversibilidade e da avaliação de dependência tecnológica prevista no art. 5º da Resolução CGPAR nº 29/2022. | Contratante      |

| ID. | CATEGORIA DO RISCO                                      | DESCRIÇÃO                                                                                                                               | CONSEQUÊNCIA                                                                                                                             | MEDIDAS MITIGADORAS                                                                                                                                                                                                                                                                                                                                                                    | ALOCÇÃO DO RISCO           |
|-----|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| R4  | Risco atinente à Licitação (Seleção do Fornecedor)      | Questionamentos, impugnações, recursos e representações; ocorrência do certame deserto ou fracassado.                                   | Atraso e/ou suspensão do processo de contratação.                                                                                        | a) Definição dos critérios de seleção de fornecedores com base nas melhores práticas de mercado e nas recomendações dos órgãos jurídico e de controle.<br>b) Realizar novo processo licitatório com base na experiência do anterior e mercado.                                                                                                                                         | Contratante                |
| R5  | Risco atinente à Licitação (Seleção do Fornecedor)      | A licitante vencedora não atender as especificações exigidas no Termo de Referência.                                                    | Retardo no processo licitatório.                                                                                                         | a) Definição dos critérios de Teste de Prova de Conceito-POC, com base nos requisitos essenciais e melhores práticas de mercado fornecedor da solução.<br>b) Convocação das empresas na ordem de classificação.                                                                                                                                                                        | Contratante                |
| R6  | Risco atinente ao Tempo da Execução (Gestão Contratual) | Atraso no início dos serviços atrelados à solução após os processos de entrega, instalação, configuração e parametrização/customização. | Comprometimento do cronograma para atendimento das necessidades e indisponibilidade dos serviços aos usuários do Banco da Amazônia.      | a) Estabelecer prazos de entrega, instalação, configuração e demais serviços agregados, adequados à solução e usuais no mercado;<br>b) Diligenciar a Contratada e exigir o cumprimento dos prazos estabelecidos para a contratação.                                                                                                                                                    | Contratada                 |
| R7  | Risco atinente ao Tempo da Execução (Gestão Contratual) | Falta de dotação orçamentária e/ou financeira para execução do contrato.                                                                | Comprometimento no atendimento aos usuários de serviços do Banco da Amazônia, com impacto nas atividades relacionadas ao uso da solução. | a) Observar durante a elaboração da contratação a estimativa prevista no Plano de Contratações Anual – PCA do órgão para o objeto e manutenção da previsão orçamentária nos exercícios seguintes;<br>b) Sempre que possível formalizar uma negociação com a Contratada/Fabricante, a fim de obter a redução dos valores dos itens que compõe a solução, reduzindo o valor do contrato. | Contratante/<br>Contratada |

| ID. | CATEGORIA DO RISCO                         | DESCRIÇÃO                                                                                                                                                                                                                    | CONSEQUÊNCIA                                                                                                                                            | MEDIDAS MITIGADORAS                                                                                                                                | ALOCÇÃO DO RISCO |
|-----|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| R8  | Riscos da Atividade Empresarial            | Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos que compõem a prestação dos serviços e a solução. | Aumento do valor do contrato em decorrência das soluções de software e prestação dos serviços.                                                          | a) Reajuste no desdobramento de reajustes e/ou repactuação de preços.                                                                              | Contratante      |
| R9  | Riscos da Atividade Empresarial            | Variação cambial de natureza ordinária (Dólar, Euro ou outra moeda reconhecidamente nacional), que impactam no valor da solução.                                                                                             | Aumento do valor da solução atrelada à variação cambial.                                                                                                | a) Planejamento empresarial na composição dos custos, considerando os fatores previsíveis.                                                         | Contratada       |
| R10 | Riscos Trabalhistas e Previdenciários      | Responsabilização do Banco da Amazônia por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na execução do objeto contratual.                                                                  | Geração de custos trabalhistas e/ou previdenciários para o Banco da Amazônia, além de eventuais honorários advocatícios, multas e verbas sucumbenciais. | a) Ressarcimento, pela Contratada, ou retenção de pagamento e compensação com valores a este devido, da quantia despendida pelo Banco da Amazônia. | Contratada       |
| R11 | Risco Tributário e Fiscal (Não Tributário) | Responsabilização do Banco da Amazônia por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do Banco da Amazônia.                     | Débito ou crédito tributário ou fiscal (não tributário).                                                                                                | a) Ressarcimento, pelo Contratado, ou retenção de pagamento e compensação com valores a este devido, da quantia despendida pelo Banco da Amazônia. | Contratada       |

| ID. | CATEGORIA DO RISCO                                          | DESCRIÇÃO                                                                                                             | CONSEQUÊNCIA                                                                                                                                         | MEDIDAS MITIGADORAS                                                                                                                                                                                                                                                                                                                                            | ALOCUÇÃO DO RISCO          |
|-----|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| R12 | Risco atinente à Licitação (Formação do preço)              | Contaminação do orçamento estimativo por cotação viciada, desatualizada ou não representativa do mercado.             | Manutenção de valor estimado incompatível com o objeto, com risco de antieconomicidade, de impugnação e de responsabilização dos agentes envolvidos. | a) Afastar expressamente as cotações sob apuração por órgão de controle. b) Priorizar contratações públicas vigentes ou encerradas há até 120 dias. c) Combinar mapa comparativo de contratações públicas e RFP. d) Aplicar tratamento estatístico com coeficiente de variação e justificar variações superiores a 40%.                                        | Contratante                |
| R13 | Risco atinente à Licitação (Seleção do Fornecedor)          | Suspensão cautelar ou anulação do certame por determinação de órgão de controle externo.                              | Interrupção do processo, atraso na disponibilização da solução e permanência dos riscos de privacidade sem tratamento tecnológico.                   | a) Registrar nos autos o enfrentamento de cada achado do Acórdão nº 1.441/2026-Plenário. b) Submeter os artefatos à análise jurídica antes da publicação. c) Publicar, com o edital, os critérios objetivos de aceitabilidade e de exequibilidade.                                                                                                             | Contratante                |
| R14 | Risco atinente à execução (Privacidade e Proteção de Dados) | Incidente de privacidade decorrente da varredura das bases de produção pelo componente de descoberta e classificação. | Exposição de dados pessoais e sensíveis, comunicação obrigatória à ANPD e aos titulares, sanção administrativa e dano reputacional.                  | a) Observar as medidas do Relatório de Impacto à Proteção de Dados da contratação. b) Exigir minimização, mascaramento e segregação nos resultados das varreduras. c) Restringir o acesso da contratada por perfil, com autenticação multifator e trilha de auditoria. d) Executar varreduras em janelas ajustadas, com possibilidade de interrupção imediata. | Contratante/<br>Contratada |
| R15 | Risco atinente à execução (Continuidade)                    | Indisponibilidade prolongada da plataforma em nuvem ou do provedor de infraestrutura.                                 | Interrupção dos processos de privacidade apoiados pela solução, perda de tempestividade no atendimento a titulares e na comunicação de incidentes.   | a) Fixar indicadores de disponibilidade mensal (NMS-01), RTO (NMS-02) e RPO (NMS-03) aferíveis. b) Exigir plano de continuidade testado periodicamente. c) Vincular a remuneração ao cumprimento dos níveis de serviço, com glosas graduadas.                                                                                                                  | Contratada                 |

| ID. | CATEGORIA DO RISCO                          | DESCRIÇÃO                                                                      | CONSEQUÊNCIA                                                                                                                | MEDIDAS MITIGADORAS                                                                                                                                                                                                                                                                              | ALOCÇÃO DO RISCO |
|-----|---------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| R16 | Risco atinente ao Planejamento (Governança) | Responsabilização de agentes do Banco pela elaboração do orçamento estimativo. | Apuração de responsabilidade individual perante o órgão de controle externo e insegurança na condução da fase preparatória. | a) Designar formalmente os responsáveis pela nova estimativa, com segregação entre a elaboração da estimativa e a especificação técnica do objeto. b) Documentar a metodologia, as fontes e a memória de cálculo. c) Submeter a estimativa a validação por instância distinta da que a elaborou. | Contratante      |

## **TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE E SIGILO**

Este Termo de Compromisso é celebrado entre:

CONTRATANTE e a CONTRATADA qualificado nos termos do preâmbulo do contrato, na forma de seu contrato social e pelo seu Preposto, todos abaixo assinados,

CONSIDERANDO QUE as Partes, por meio do Contrato 20XX/XXX estão estabelecendo uma relação de CONTRATANTE e CONTRATADA para a prestação dos serviços objeto do contrato, que para ser executada necessariamente inclui o acesso, o conhecimento e o tratamento de dados e informações corporativas da CONTRATANTE, o uso de equipamentos, de recursos computacionais e outros que envolvam a possibilidade de divulgação de informações restritas, de exclusivo interesse da CONTRATANTE, sob a posse, guarda e domínio da CONTRATADA;

CONSIDERANDO QUE a expressão “informações internas, restritas e/ou sigilosas” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

CONSIDERANDO QUE as Partes podem divulgar entre si informações internas, restritas e/ou sigilosas, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios;

CONSIDERANDO QUE as Partes desejam ajustar as condições de revelação das Informações internas, restritas e/ou sigilosas, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as Partes celebrar o presente TERMO DE RESPONSABILIDADE CONFIDENCIALIDADE E SIGILO, o qual se regerá pelas considerações acima, bem como, pelas considerações que forem pertinentes constantes na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

- a) Assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações do BANCO DA AMAZÔNIA no desenvolvimento dos serviços prestados;
- b) Tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que forem fornecidas pelo BANCO DA AMAZÔNIA e preservar o seu sigilo, de acordo com a legislação vigente e a NP Classificação e Tratamento da Informação;
- c) Manter as informações do BANCO DA AMAZÔNIA em segurança e sob sigilo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem autorização, a qualquer terceiro estranho a este Instrumento por si e por parte de seus Profissionais, ou utilizar de forma contrária ao aqui estabelecido;
- c) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;
- d) Não copiar ou reproduzir, por qualquer meio ou modo: (i) informações classificadas em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito do BANCO DA AMAZÔNIA, salvo autorização da autoridade competente.
- f) Quando as informações recebidas, criadas ou acessadas pelos profissionais da CONTRATADA, em razão dos serviços contratados, forem de uso exclusivo do BANCO DA AMAZÔNIA, importará no reconhecimento deste fato pela parte da CONTRATADA.



GESEC – GERÊNCIA DE SEGURANÇA CORPORATIVA

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

**Belém-PA, Data da última assinatura eletrônica.**

**BANCO DA AMAZÔNIA S.A.**

---

**XXXXXXXXXXXXX**

Representante do Banco da Amazônia

**NOME DA CONTRATADA**

---

**XXXXXXXXXXXXX**

Representante Legal da Contratada

**ANEXO III****TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE DO EMPREGADO  
TERCEIRIZADO**

Eu, [NOME DO EMPREGADO], portador do CPF nº [NÚMERO DO CPF], declaro, como empregado da [RAZÃO SOCIAL DA CONTRATADA], estar ciente de minhas responsabilidades profissionais quanto à segurança dos recursos computacionais e das informações corporativas do Banco da Amazônia S.A., cujos acessos me serão franqueados para desempenho, exclusivo, das funções para as quais fui expressamente contratado e designado.

Por esse termo de responsabilidade e confidencialidade, comprometo-me a:

- a) Manter-me atualizado com a Política de Segurança da Informação e Cibernética e demais Políticas Internas e Normas de Segurança do BANCO DA AMAZÔNIA;
- b) Manter o sigilo absoluto de minhas senhas de acesso à rede corporativa e a sistemas, estando ciente que minhas senhas são pessoais e intrasferíveis, cabendo a mim, exclusivamente, a guarda sigilosa, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de minhas senhas;
- c) Manter sigilo absoluto de informações do BANCO DA AMAZÔNIA que me sejam franqueados em função da minha atividade profissional;
- d) Manter vigilância dos materiais, máquinas, ferramentas e outros pertences de minha propriedade guardados no local dos serviços, quando forem prestados nas dependências do BANCO DA AMAZÔNIA, além de zelar pelos equipamentos, materiais e quaisquer outros recursos de propriedade do BANCO DA AMAZÔNIA colocados eventualmente à minha disposição, utilizando-os de maneira correta e cuidadosa e estritamente para os fins do cumprimento das minhas atividades;
- e) Manter sigilo das informações do BANCO DA AMAZÔNIA ou de terceiros, classificadas como sigilosas, restritas e internas, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;
- f) Não copiar, reproduzir, transferir ou usar indevidamente quaisquer informações do BANCO DA AMAZÔNIA para qualquer outra finalidade que não seja a promoção dos serviços contratados, observando-se o disposto neste termo;
- g) Não utilizar, reter ou duplicar as informações que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo BANCO DA AMAZÔNIA;
- h) Não transferir as informações corporativas do Banco da Amazônia para outros meios de armazenamento (físicos e nuvem), não autorizados pelo Banco, para fins particulares, sob pena de responsabilização por vazamento de dados;
- i) Não utilizar as informações de forma que possa configurar concorrência desleal com o BANCO DA AMAZÔNIA, tampouco explorá-las em outros negócios ou oportunidades comerciais, sem prévia e expressa autorização do BANCO DA AMAZÔNIA;
- j) Não comentar, compartilhar ou publicar na Internet ou em mídias sociais, ou qualquer plataforma de armazenagem aberta de dados, como repositórios digitais, quaisquer informações relacionadas à prestação de serviços que tem junto ao BANCO DA AMAZÔNIA a não ser que tenha havido prévia e expressa autorização;
- k) Não realizar qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências do BANCO DA AMAZÔNIA, exceto quando relacionada a atividade contratada;



l) Cessar o uso, bem como devolver, imediatamente após o término do Contrato, todos os materiais, informações, documentos, recursos (inclusive crachás, usuários de acesso a sistemas etc.) do BANCO DA AMAZÔNIA que tenham me sido emprestados ou de qualquer forma disponibilizados;

m) Acessar os ambientes do BANCO DA AMAZÔNIA, sejam eles físicos ou lógicos, estritamente para a execução da prestação dos serviços contratados;

n) Respeitar às leis vigentes de direito autoral e Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) bem como as demais leis, normas e políticas de proteção de dados pessoais corporativas;

o) Manter sigilo de dados pessoais cujo BANCO DA AMAZÔNIA figura como controlador ou operador, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;

p) Seguir as instruções recebidas do BANCO DA AMAZÔNIA em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes e aplicáveis, devendo garantir sua licitude e idoneidade;

q) Tratar todos os Dados Pessoais como restritos, exceto se já eram de conhecimento público sem qualquer contribuição sua, ainda que a relação contratual entre as Partes venha a ser resolvida, e independentemente dos motivos que derem causa;

r) Notificar o BANCO DA AMAZÔNIA assim que tomar conhecimento de qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (i) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (ii) de quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (iii) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente;

s) Ter a ciência de que o BANCO DA AMAZÔNIA monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação;

t) Comunicar imediatamente ao meu Gerente imediato ou diretamente ao fiscal do contrato qualquer falha, suspeita ou ameaça por mim detectada aos ativos do BANCO DA AMAZÔNIA, como informações, recursos de tecnologia da informação, ambientes físicos, imagem e reputação;

u) Respeitar às leis vigentes de direito autoral e no que couber, ter como ação os princípios e práticas descritos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no que tange à segurança, a privacidade e o tratamento das informações, bem como, adotar ações no presente para a plena observância da referida lei no momento de sua vigência;

Sendo estas responsabilidades estendidas:

a) Para fora das dependências do BANCO DA AMAZÔNIA e fora dos horários normais de trabalho quando na execução de trabalho remoto, em cliente ou em outra dependência do Banco;

b) Por tempo indeterminado, mesmo após o término da relação profissional da CONTRATADA com o BANCO DA AMAZÔNIA, no que tange a não divulgação e comercialização de informações sigilosas e informações pessoais;

Estou ciente que transgressões destas normas são consideráveis faltas graves e que poderei responder civil e penalmente por quaisquer prejuízos causados ao Banco da Amazônia.

[Local], XX de XXXX de XXXX.



---

[NOME DO EMPREGADO TERCEIRIZADO]

**ANEXO IV****REQUISITOS MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO**

Este Anexo divide-se em duas partes. A Parte A reúne os requisitos aplicáveis à solução contratada na modalidade Software como Serviço e ao respectivo provedor de infraestrutura em nuvem. A Parte B reúne os requisitos aplicáveis exclusivamente a eventuais componentes instalados no ambiente tecnológico do Banco e às interfaces de integração disponibilizadas, incidindo somente na hipótese de a solução ofertada demandar tais componentes.

**PARTE A — REQUISITOS APLICÁVEIS À SOLUÇÃO EM NUVEM (SaaS) E AO PROVEDOR****REQUISITOS GERAIS DE SEGURANÇA PARA A CONTRATADA**

A contratada deverá assinar, no início do contrato, o Termo de Confidencialidade e Sigilo que terá como objetivo definir as regras relativas ao tratamento, acesso, proteção e revelação das informações corporativas do Banco da Amazônia (BASA).

Todos os empregados da empresa contratada que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato deverão assinar o Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado. O referido termo deverá ser entregue ao gestor do contrato antes do início das atividades do profissional.

A contratada deverá:

adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do BASA;

comunicar com antecedência mínima de 15 (quinze) dias ao BASA qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do BASA, porventura colocados à disposição para realização dos serviços contratados;

manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo BASA a tais documentos;

não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do BASA, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;

manter seus empregados devidamente informados das normas disciplinares do BASA, bem como das normas de utilização e de segurança das instalações e do manuseio dos documentos;

manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do BASA;

garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do Banco da Amazônia;

assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;



assumir inteira responsabilidade por quaisquer danos ou prejuízos causados ao BASA e a terceiros, incluindo prejuízos financeiros, por dolo ou culpa, de seus empregados, decorrentes dos serviços ora contratados;

garantir e manter total e absoluto sigilo sobre as informações manuseadas as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;

não repassar a terceiros, em nenhuma hipótese, qualquer informação sobre a arquitetura e/ou documentação, assim como dados e/ou metadados trafegados, produtos desenvolvidos e entregues, ficando responsável juntamente com o BASA por manter a segurança da informação relativa aos dados e procedimentos durante a execução das atividades e em período posterior ao término da execução do contrato;

assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BASA através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado;

providenciar para que os produtos e artefatos da contratação sejam entregues em perfeito estado, com a segurança necessária, garantindo o transporte, o seguro, a entrega e a implantação nos locais indicados pelo BASA sem quaisquer danos, avarias ou ônus adicionais para o BASA.

#### **COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM**

A contratada deve garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo que o BASA tenha todas as garantias legais enquanto tomador do serviço e proprietário das informações, se hospedadas na nuvem.

A contratada deverá:

cumprir integralmente as diretrizes da Resolução CMN 4.893/21; fornecer acesso ao BASA aos dados e às informações a serem processados ou armazenados pela empresa contratada;

assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador;

apresentar, em nome do provedor que hospeda a solução, certificação válida na norma ABNT NBR ISO/IEC 27001 em sua versão vigente e, adicionalmente, na norma ISO/IEC 27701 ou na norma ISO/IEC 27018, admitida, alternativamente, a demonstração do atendimento aos objetivos e controles das referidas normas mediante apresentação de políticas, procedimentos, matrizes de controle e relatórios de auditoria independente, facultado ao BASA promover diligência destinada a esclarecer ou complementar informações;

fornecer ao BASA acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e aos controles utilizados na execução dos serviços a serem contratados;

fornecer informações e recursos de gestão para possibilitar o monitoramento dos serviços a serem prestados;

assegurar, enquanto o contrato estiver vigente, a identificação e a segregação dos dados dos clientes do BASA por meio de controles físicos ou lógicos e forneça ao BASA documentos e/ou relatórios que evidenciem o cumprimento desta exigência;

assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do BASA;



adotar um padrão de identidade federada para permitir o uso de tecnologia **single sign-on** no processo de autenticação dos usuários do serviço de nuvem, o qual deve ser acompanhado de autenticação multifator (MFA).

registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.

apoiar o BASA, quando necessário, nas atividades de investigação de incidentes de cibersegurança. Isso inclui fornecer prontamente informações e recursos necessários para a investigação, como logs, registros de eventos e relatórios de auditoria.

adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, caso o serviço a ser contratado seja relativo ao serviço de execução de aplicação por meio da internet;

garantir que o ambiente seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados por outros usuários do serviço em nuvem;

assegurar que toda atualização do sistema seja previamente analisada e homologada antes que possa ser instalada/configurada, além de dispor de documentação de todas as alterações realizadas no serviço e/ou sistema mediante processos formalizados de Gestão e Mudanças;

assegurar a adoção de medidas de segurança para a transmissão e armazenamento dos dados e das informações processados ou armazenados pelo prestador, e fornecer ao BASA evidências da adoção das referidas medidas;

notificar ao BASA sobre a subcontratação de serviços relevantes para a prestação do serviço contratado;

notificar ao BASA sobre a intenção de interromper a prestação de serviços com pelo menos trinta dias de antecedência da data prevista para a interrupção;

conceder o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

dispor de Plano de Comunicação de Incidentes e/ou dashboards com informações referentes a saúde dos serviços oferecidos de incidentes que possam ocorrer, informando o BASA os casos de incidentes de segurança da informação, assim considerados os eventos não previstos ou não desejados que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do BASA;

realizar a análise e a gestão de riscos de segurança da informação, com periodicidade mínima anual e sempre que houver alteração relevante de arquitetura, incidente significativo ou mudança regulatória, disponibilizando ao BASA o plano de gestão de riscos ou o respectivo sumário executivo, contendo metodologia utilizada, riscos identificados, avaliação, tratamento, monitoramento e assunção de riscos;

possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção;



desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços ou envolvendo dados pessoais de empregados e/ou clientes do BASA;

realizar regularmente testes de segurança da informação, incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de intrusão, bem como auditorias por terceira parte independente, com periodicidade mínima anual e sempre após mudanças relevantes de arquitetura ou incidentes significativos, disponibilizando ao BASA relatório ou sumário executivo comprobatório;

prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;

deverá fornecer, sempre que solicitado pelo BASA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de Application Programming Interface (API), caso haja, para análise de segurança e auditorias;

dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do BASA, incluindo os seguintes itens: solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações), solução de prevenção e detecção de intrusão (IDS/IPS), antivírus, anti-malware, solução anti-DDoS, solução de gestão de logs, solução de gestão integrada de pacotes de correção (patches), solução de correlação de eventos de segurança (SIEM);

realizar backups e salvaguardas dos dados, configurações, registros e evidências mantidos na solução, observados os requisitos de retenção, RTO, RPO, criptografia, segregação, testes periódicos de restauração e descarte seguro definidos no contrato, permitindo a consulta e a exportação desses dados pelo BASA;

garantir a exclusividade de direitos, por parte do BASA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como **backups** de segurança.

preservar os dados do BASA contra acessos indevidos e observar as regras de localização do tratamento previstas neste Anexo, informando imediata e formalmente ao BASA qualquer solicitação, tentativa ou ordem de acesso a esses dados por autoridade estrangeira ou por terceiro não autorizado, ressalvadas as hipóteses de vedação legal expressa de comunicação;

operar o serviço dentro do uso proposto, com desempenho razoável e exigindo o mínimo possível de permissões dos demais sistemas do BASA, além de proteger os dados transmitidos por meio dele, quando necessário;

atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:

as diretrizes de tratamento;

o modo de atendimento a solicitações de titulares de dados pessoais;

as medidas protetivas para garantia da confidencialidade dos dados pessoais;

as medidas protetivas durante as comunicações com o BASA;

o registro de atividades de tratamento de dados pessoais;

a solicitação de autorização na subcontratação

de terceiros para atividades de tratamento de dados pessoais;

a medidas de devolução / descarte dos dados.

A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:



inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;

inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

não fornecimento a terceiros de dados do BASA, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

fornecer ao BASA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BASA.

Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo BASA e tratados no âmbito da solução deverão ser processados e armazenados em ambiente localizado em território brasileiro, observando-se que:

pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

eventual tratamento de dados fora do território nacional dependerá de autorização prévia, formal e específica do BASA, e somente poderá ocorrer mediante observância dos arts. 33 a 36 da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 19/2024, com identificação dos países envolvidos, do mecanismo de transferência adotado, das garantias contratuais aplicáveis e das medidas de segurança correspondentes, preservados o acesso do BASA e dos órgãos reguladores competentes e observada a Resolução CMN nº 4.893/2021.

A empresa deve garantir a adequação e a adoção de medidas pelo BASA, em decorrência de qualquer determinação do Órgãos Governamentais aos quais o BASA é subordinado que impacte sobre o Contrato vigente.

A empresa deve manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

É vedado o uso de informações do BASA pela contratada para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

Em caso de extinção do contrato, a contratada deverá transferir os dados e as informações processados ou armazenados por ele ao novo prestador de serviços ou ao BASA e, após a confirmação da integridade e da disponibilidade dos dados e informações recebidos, os excluir.

Em caso da decretação de regime de resolução do Banco da Amazônia pelo Banco Central do Brasil, a contratada deverá:

conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações que estejam em poder da empresa contratada; e

notificar previamente o responsável pelo regime de resolução sobre sua intenção de interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção. A contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

## **PARTE B — REQUISITOS APLICÁVEIS A COMPONENTES INSTALADOS NO AMBIENTE DO BANCO E ÀS INTERFACES DE INTEGRAÇÃO**



Os requisitos desta Parte B incidem exclusivamente sobre componentes que a solução ofertada exija instalar no ambiente tecnológico do Banco e sobre as interfaces de integração por ela disponibilizadas. Os requisitos que pressuponham desenvolvimento de software sob encomenda ou acesso a código-fonte não se aplicam à modalidade Software como Serviço, hipótese em que o seu atendimento será aferido mediante declaração da CONTRATADA acompanhada de relatório de auditoria independente que ateste a adoção de práticas equivalentes.

## REQUISITOS DE ARQUITETURA, DESIGN E MODELAGEM DE AMEAÇAS

O sistema, com recursos web, deverá incorporar, no mínimo, proteção contra:

**Controle de acesso falho:** as restrições sobre o que os usuários autenticados têm permissão para fazer muitas vezes não são aplicadas de forma adequada. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

**Falhas criptográficas:** Muitos aplicativos da web e APIs não protegem adequadamente os dados sigilosos, como dados pessoais e financeiros. Os invasores podem roubar ou modificar esses dados fracamente protegidos para conduzir fraude de cartão de crédito, roubo de identidade ou outros crimes. Os dados sigilosos podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requerem precauções especiais quando trocados com o navegador.

**Injeção:** Injeções ocorrem quando dados informados pelo usuário são enviados para um interpretador como parte de um comando ou uma query. O dado malicioso do atacante faz o interpretador executar comandos que não deveria ou modificar dados. Algumas das injeções mais comuns são SQL, NoSQL, OS command, Mapeamento Relacional de Objeto (ORM), LDAP e Expression Language (EL) ou Object Graph Navigation Library (OGNL). O conceito é idêntico entre todos. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções.

**Design inseguro:** O design seguro é uma cultura e metodologia que avalia constantemente as ameaças e garante que o código seja desenvolvido e testado de forma robusta para evitar métodos de ataque conhecidos. O design seguro requer um ciclo de vida de desenvolvimento seguro, alguma forma de padrão de design seguro ou biblioteca ou ferramenta de componentes de estradas pavimentadas e modelagem de ameaças.

**Configuração incorreta de segurança:** geralmente é o resultado de configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas também devem ser corrigidos / atualizados em tempo hábil.

**Componentes vulneráveis e desatualizados:** componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios do aplicativo. Se um componente vulnerável for explorado, esse tipo de ataque pode facilitar a perda séria de dados ou o controle do servidor. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas do aplicativo e permitir vários ataques e impactos.

**Falhas de identificação e autenticação:** as funções do aplicativo relacionadas à autenticação e gerenciamento de sessão são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários temporária ou permanentemente.



**Falhas de software e integridade de dados:** As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Por exemplo, quando objetos ou dados são codificados ou serializados em uma estrutura que um invasor pode ver e modificar, logo é vulnerável à desserialização insegura. Outro exemplo é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs).

**Registro (logging) e monitoramento insuficientes:** registro (logging) e monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permite que os invasores ataquem ainda mais os sistemas, mantenham a persistência, ganhem acesso em mais sistemas e adulterem, extraiam ou destruam dados.

**Server-Side Request Forgery (SSRF):** As falhas de SSRF ocorrem sempre que um aplicativo web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de ACL de rede.

**Validação de entrada inadequada:** o produto recebe entradas ou dados, mas não valida ou valida incorretamente se a entrada possui as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos devam satisfazer apenas o esperado pela aplicação.

**Caracteres Especiais ou maliciosos:** caracteres especiais são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros. Garanta que apenas entradas válidas, esperadas e apropriadas sejam processadas pelo Sistema.

A solução deverá possuir conformidade com o OWASP TOP 10 vigente visando assegurar a segurança dos dados, gerar confiança entre os usuários, prevenir perdas financeiras e cumprir regulamentações de segurança, proporcionando a integridade e a credibilidade necessárias para um site ou aplicativo.

Deverá ser imposto o menor privilégio em conexões com o banco de dados ou outros sistemas de back-end.

*A Contratada deverá realizar configuração segura (hardening) do servidor web no qual a aplicação está hospedada e deverá assegurar que servidores web da aplicação estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmark mais atual.*

As seguintes flags e procedimentos relacionados deverão ser adotados em relação às configurações do cabeçalho para a comunicação entre o servidor e o cliente:

A aplicação deverá instruir o browser a só permitir acesso via HTTPS. Deverá ser ativado o HTTP Strict Transport Security (HSTS) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. O max-age deve ser de pelo menos 31536000 segundos (1 ano);

O cabeçalho X-Content-Type-Options deverá estar configurado como 'nosniff' para todas as páginas da web;

A aplicação deverá retornar o cabeçalho X-Frame-Options com o valor DENY ou SAMEORIGIN, que permitirá "framing" das páginas conforme SAME ORIGIN;

A aplicação deverá ter o CSP habilitado enviando os cabeçalhos de resposta Content-Security-Policy, conforme políticas que atenda critérios de segurança na implementação dessa diretiva;



A aplicação deverá ter o cabeçalho X-XSS-Protection desabilitado, por meio da configuração do seu valor como 0 (zero);

A aplicação não deverá possuir os cabeçalhos “fingerprinting”: X-Powered-By, Server, X-AspNet-Version;

A aplicação deverá forçar content-type para as respostas. Se a aplicação retorna json, a resposta content-type da aplicação deverá ser application/json;

Os tipos de conteúdo text/\*, /+xml e application/xml também devem especificar um conjunto de caracteres seguro (por exemplo, UTF-8, ISO-8859-1);

O conteúdo da aplicação não poderá ser incorporado a um site de terceiro por padrão;

O Cross-Origin Resource Sharing (CORS) e cabeçalho Access-Control-Allow-Origin deverão utilizar uma lista de permissão restrita de domínios e subdomínios confiáveis para correspondência e não oferecer suporte à origem "null", e validar os dados inseridos pelo usuário;

O cookie emitido pela aplicação deverá possuir os atributos SameSite, SECURE e HttpOnly;

A aplicação deverá utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações

Antes da entrada em produção, a solução passará por homologação quanto a sua segurança. Quaisquer eventuais vulnerabilidades identificadas pela equipe do BASA serão tratadas como defeito de software e deverão obrigatoriamente ser corrigidas pela CONTRATADA.

Realizar configuração segura do servidor web, também conhecido como hardening. Assegurar que servidores WEB estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmarks.

Utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.

## **REQUISITOS DE ARMAZENAMENTO DE DADOS E PRIVACIDADE**

Os recursos de armazenamento de credenciais do sistema deverão ser utilizados para armazenar dados restritos e sigilosos, como dados pessoais, credenciais de usuário ou chaves criptográficas

Dados restritos e sigilosos não deverão:

- ser exibidos em mensagens de erro;

- ser armazenados fora do contêiner da aplicação ou de recursos de armazenamento de credenciais do sistema;

- ser armazenados em texto claro, como um banco de dados não criptografado;

- aparecer nos logs de aplicação;

- ser compartilhados com terceiros, exceto se for uma parte necessária da arquitetura;

- ser expostos através de mecanismos IPC (Inter-process Communication);



ser armazenados localmente ou em arquivos temporários no dispositivo. Em vez disso, os dados deverão ser recuperados de um terminal remoto quando necessário e mantidos apenas em memória.

A aplicação não deverá exibir mensagens de erro detalhadas que possa expor informações privilegiadas.

Senhas ou PINs de acesso não deverão ser expostos através da interface de usuário.

Credenciais de acesso não deverão ser armazenadas dentro do código-fonte do sistema.

Será obrigatória a validação, a filtragem e o tratamento de todos os dados inseridos pelo usuário.

Toda requisição de acesso ao banco de dados deverá passar por processo de validação de autorização.

Será vedada a filtragem de dados no cliente.

Não deverá ser utilizado o método GET (URLs) para o envio de dados restritos ou sigilosos ou para a realização transações financeiras.

O método HTTP deverá ser utilizado de acordo com a operação: GET (read), POST (create), PUT/PATCH (replace/update), e DELETE (delete).

Será proibida a utilização de dados sensíveis (credenciais de acesso, senhas, tokens ou API keys) na URL, deverá ser utilizado cabeçalho Authorization.

Toda requisição de acesso à API deverá passar por processo de validação de autorização.

Um mecanismo de validação de entrada padrão deverá ser utilizado para validar todos os dados em tamanho, tipo, sintaxe e regras de negócio antes de exibí-los ou armazená-los.

Deverá ser utilizada a estratégia de validação do tipo Whitelist.

Será obrigatória a validação content-type de dados publicados (POST) aceitáveis (por exemplo application/x-www-form-urlencoded, multipart/form-data, application/json etc.).

Entradas inválidas deverão ser rejeitadas, ao invés de se tentar sanitizar dados impróprios/maliciosos.

## **REQUISITOS DE AUTENTICAÇÃO**

O sistema deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.

O sistema deve possuir mecanismo de múltiplo fator de autenticação (MFA);

O sistema deve ser capaz de admitir integração com MS-AD (Microsoft Active Directory) do BASA para login único de usuário (Single Sign On = SSO).

As senhas deverão ser gravadas em banco de dados de forma criptografada.

A tela de log-on não deverá exibir a senha que está sendo informada.

O sistema não deverá armazenar ou transmitir senhas em texto plano.

A tela de entrada dos sistemas deverá validar as informações fornecidas pelo usuário somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar qual parte do dado de entrada está correta ou incorreta.



Em caso de tentativa de log-on inválida, o sistema deverá exibir uma mensagem genérica e nunca exibir as mensagens "usuário inexistente" ou "senha incorreta", de modo a não fornecer mensagens que permitam a um usuário não autorizado deduzir informações de acesso.

Todo acesso administrativo deverá ser restrito e deverá ser garantido o acesso apenas aos usuários autorizados.

Deverá ser utilizado HTTPS para envio de credenciais.

Os sistemas não deverão passar ID de sessão por método HTTP GET.

Deverá ser utilizado sempre o método HTTP POST para a requisição de autenticação.

Será obrigatória a utilização do parâmetro "state" com hash aleatório no processo de autenticação do OAuth.

Será proibido o uso de Basic Authentication.

As autorizações de acesso deverão ser validadas, garantindo que nenhum usuário acessará o que não foi previamente definido em seu perfil.

O processo de login deve ser iniciado através de uma página com um novo cookie de sessão.

Todos os endpoints do sistema deverão ser protegidos por autenticação.

Será proibido o incremento de IDs automaticamente. No lugar, deverá ser utilizado UUID.

## **REQUISITOS DE GERENCIAMENTO DE SESSÃO DO USUÁRIO**

As sessões deverão ser invalidadas pelo terminal remoto após um período de, no máximo, 15 minutos de inatividade e os tokens de acessos devem expirar.

O controle de sessão deverá ser tratado pelo servidor e apenas a persistência dele no cliente.

Os sistemas deverão implementar token de sessão por requisição com alta aleatoriedade, devendo ser utilizados tokens personalizados e aleatórios em todos os formulários e URLs que não serão automaticamente enviadas pelo navegador.

Toda as páginas deverão ter um link para o logout o qual, ao clicar, o sistema deverá realizar o logout sem antes questionar o usuário. O logout deve destruir todo o estado da sessão no lado servidor e os cookies no lado cliente.

Será proibido o uso de "response\_type=token".

Dados de usuários, atributos e políticas utilizados pelos controles de acesso, não podem ser manipulados pelos usuários finais, a menos que especificamente autorizado na arquitetura do projeto.

O sistema deverá utilizar o princípio do menor privilégio, os usuários só devem ser capazes de acessar funções, arquivos de dados, URLs, controladores, serviços e outros recursos, para os quais possuam autorização específica.

Em caso de sistemas que utilizam JWT (JSON Web Token):t

Será obrigatório o uso de chaves randômicas (JWT Secret);

Será proibido armazenar dados confidenciais em tokens JWT.

Será proibida a extração do algoritmo do cabeçalho (deverá ser validado no back-end);



Deverá ser utilizado algoritmo de assinatura de robustez equivalente ou superior à do RS256;

Será obrigatório regras de time-out de sessão do usuário de 15 minutos, access token de 3 minutos e refresh token de 8 horas.

## REQUISITOS DE COMUNICAÇÃO DE REDE

O sistema deverá ser capaz de suportar a pilha dupla IPV4 e IPV6.

Todas as comunicações externas entre os servidores do sistema e os clientes deverão ser encriptadas.

O sistema deverá utilizar criptografia para as comunicações externas entre os servidores do sistema e os clientes. Os dados deverão ser criptografados na rede utilizando somente TLS 1.2 ou superior.

O sistema não deverá permitir o uso do SSL, TLS 1.0 e TLS 1.1.

Deve-se usar os seguintes algoritmos: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 e SHAKE256.

Será vedada a utilização de cifras com vulnerabilidades divulgadas e/ou conhecidas.

As requisições deverão ser limitadas (através de rate limit ou outra solução semelhante), a fim de se evitar ataques de DoS (negação de serviço) ou força bruta.

Deverá ser utilizada a validação de "redirect\_url" no servidor para permitir apenas URL's da *whitelist*.

Tráfegos HTTP deverão ser redirecionados para HTTPS.

A propriedade "readOnly" deverá ser configurada como "true" em esquemas de objeto para todas as propriedades que podem ser recuperadas por meio de APIs, mas nunca deverão ser modificadas.

Os modos de depuração do servidor da Web ou de aplicativos e da estrutura de aplicativos deverão ser desativados em produção para eliminar recursos de depuração, consoles de desenvolvedor e divulgações de segurança não intencionais.

## REQUISITOS DE RESPOSTAS HTTP

Os cabeçalhos HTTP ou qualquer parte da resposta HTTP não deverão expor informações detalhadas da versão dos componentes do sistema.

A aplicação deverá retornar os seguintes códigos:

405 Method Not Allowed: sempre que um método solicitado não for apropriado para o recurso solicitado

406 Not Acceptable: sempre que o formato suportado não for correspondido. Requisições content-type deverão ser validadas para permitir apenas o formato suportado (por exemplo application/xml, application/json etc.)

HTTP 200: código de resposta do status de sucesso do HTTP, indica que a solicitação foi bem-sucedida;

HTTP 302: indica que o recurso solicitado foi movido temporariamente para a URL fornecida pelo cabeçalho Location.

HTTP 401: para qualquer ação não autorizada no sistema.



HTTP 429: para solicitações que excedam o limite de requisição permitido.

HTTP 415: para solicitações contendo cabeçalhos de tipo de conteúdo ausentes ou inesperados

A aplicação deverá ter defesas contra ataques de poluição de parâmetro HTTP, especialmente se a estrutura do aplicativo não faz distinção sobre a origem dos parâmetros de solicitação (GET, POST, cookies, cabeçalhos ou variáveis de ambiente).

Redirecionamentos e encaminhamentos de URL deverão permitir apenas destinos que aparecem em uma lista de permissões ou deverão mostrar um aviso ao redirecionar para conteúdo potencialmente não confiável.

A aplicação deverá ter proteção contra ataques do tipo SSRF, validando ou higienizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos, campos de entrada de URL, listas de protocolos, domínios, caminhos e portas.

## REQUISITOS DE AUDITORIA

A solução deve dispor de registros (logs) de eventos para fins de auditoria, abrangendo as ações administrativas e as operações realizadas sobre os registros, documentos e evidências mantidos na plataforma, incluindo criação, consulta, alteração, exportação e exclusão.

A solução deve dispor de logs com registro de informações a serem utilizadas na depuração e verificação de falhas da solução, mantendo o registro de toda atividade de arquivamento e recuperação realizada, inclusive para os processos de auditoria realizados.

A solução deve permitir a configuração de perfil de auditoria, com permissão de acesso somente leitura a conjuntos específicos de registros ou à totalidade das informações mantidas na plataforma, conforme definido pelo Banco.

A solução deve suportar a geração e armazenamento de logs no formato IPV4 e IPV6.

As aplicações deverão implementar um sistema de *logging* que permita auditorias e investigações de incidentes de segurança, fraudes e casos de abuso.

A identificação do usuário, ou ID, deverá ser única, isto é, cada usuário deverá ter uma identificação própria.

Os sistemas de informação e suas respectivas infraestruturas deverão ser configurados de modo a registrar um critério mínimo de informações de logging e auditoria, contendo, no mínimo:

operações de login e logout;

tentativas de login malsucedidas;

acesso a telas cujo conteúdo é sigiloso, em segredo de justiça, possua dados pessoais ou bancários;

operações de inclusão, alteração ou exclusão de registros no banco de dados;

execução de jobs e tarefas automatizadas;

criação, leitura, atualização ou exclusão de informações sigilosas;

mudanças de configurações no sistema, na rede ou em serviços (inicialização, suspensão e reinicialização de serviços), inclusive a instalação de patches e atualizações de softwares;

acesso aos bancos de dados de fonte interna e externa;



falhas que resultem no fechamento anormal da aplicação, especialmente devido à exaustão de recurso ou atingimento do limite de um recurso (como memória do CPU, conexões de rede, espaço no disco etc.);

acesso e alteração de trilhas de auditoria;

registros de tráfego de dados de fontes internas e externas; e

registros de processos internos relacionados às atividades do negócio.

Os registros dos eventos deverão incluir, no mínimo, as seguintes informações:

identificação inequívoca do autor/ativo que realizou a atividade;

sistema onde ocorreu ou foi observada a atividade (logger/observador do evento);

tela (página) do sistema de onde a operação foi realizada;

tipo de atividade ocorrida (tipo de evento/ação);

data, hora e fuso horário, observando os mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);

retorno do sistema em caso de falhas ou sucesso na ação;

identificador da instância (para sistemas clusterizados);

para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;

parâmetros informados pelo usuário (ex: parâmetros repassados aos métodos GET ou POST);

tempo de resposta do sistema;

para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada etc.; e

endereço IP, nome do dispositivo, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

A aplicação não deve registrar credenciais ou detalhes de pagamento.

Os tokens de sessão só devem ser armazenados em logs de forma irreversível e com hash.

Será vedado o envio de informações sensíveis (ex: credenciais de acesso) para logs.

Os registros de auditoria deverão ser mantidos de forma segregada e protegida contra alteração e exclusão, inclusive por usuários com perfil administrativo.

As aplicações deverão registrar logs de rastreamento distribuído (distributed tracing) de requisição.

As aplicações deverão gerar logs em formato que permita a completa identificação dos fluxos de dados

As aplicações deverão registrar eventos relevantes de segurança, incluindo eventos de autenticação bem-sucedidos e com falha, falhas de controle de acesso, falhas de desserialização e falhas de validação de entrada.

A solução deve garantir que todas as fontes de tempo estão sincronizadas com a hora e fuso horário corretos.



Dados de registro devem ser sanitizados para evitar ataques de injeção de registro.

## REQUISITOS PARA APIs

A codificação de API deverá incorporar, no mínimo, proteção contra:

- a) *Broken Object Level Authorization*
- b) *Broken User Authentication*
- c) *Excessive Data Exposure*
- d) *Lack of Resources & Rate Limiting*
- e) *Broken Function Level Authorization*
- f) *Mass Assignment*
- g) *Security Misconfiguration*
- h) *Injection (Injection flaws, tais como SQL e NoSQL, Command Injection etc.)*
- i) *Improper Assets Management*
- j) *Insufficient Logging & Monitoring*
- k) *Conformidade com o OWASP Top 10 API Security Risks em vigor*

Deverão ser adotados mecanismos de codificação e de validação de dados de entrada e de saída aderentes a boas práticas de segurança de aplicações amplamente reconhecidas no mercado.

Deve ser imposto o menor privilégio quando se conectar ao banco de dados ou outros sistemas de back-end.

O banco de dados não deverá ser acessado por outro canal que não seja a aplicação

Os URLs da API não deverão expor informações confidenciais, tais como a chave da API, tokens de sessão etc.

Objetos serializados deverão usar verificações de integridade ou criptografados para evitar a criação de objetos hostis ou adulteração de dados.

Todos os endpoints acessíveis ao público devem usar um Certificado Digital que tenha sido assinado por uma Autoridade de Certificação aprovada e dentro do prazo de utilização.

Devem ser aplicadas políticas de limitação de taxa (ratelimit) para evitar o abuso da API.

Toda entrada pelo usuário por parâmetros da aplicação ou de forma manipulada em qualquer outra parte da aplicação, deverá ser validada, garantindo as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos devam satisfazer apenas o esperado."

A solução deve garantir que apenas entradas válidas, esperadas e apropriadas sejam processadas, pois caracteres especiais ou maliciosos são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros.

**ANEXO V****ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO****1. Descrição sucinta do objeto**

- 1.1. Contratação de empresa especializada para o fornecimento de Solução de Gestão de Privacidade e Proteção de Dados Pessoais, na modalidade SaaS, incluindo serviços continuados de suporte técnico, sustentação e operação assistida, e serviços técnicos especializados sob demanda, nos termos da Lei nº 13.303/2016 e das condições estabelecidas neste instrumento e seus Anexos.

**2. Composição da solução**

| ITEM | DESCRIÇÃO                                                                                                                                                                           | UNIDADE | QTD. |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| 1    | Subscrição corporativa de solução tecnológica para apoio à governança, gestão, monitoramento e conformidade em privacidade e proteção de dados pessoais.                            | Mês     | 60   |
| 2    | Subscrição corporativa de solução para identificação, mapeamento, inventário, classificação e monitoramento de dados pessoais e sensíveis em bases estruturadas e não estruturadas. | Mês     | 60   |
| 3    | Serviços de implantação da solução                                                                                                                                                  | Serviço | 1    |
| 4    | Transferência de conhecimento (capacitação de administradores e usuários, materiais de apoio, manuais, documentação das parametrizações e repasse formal das configurações)         | Serviço | 1    |
| 5    | Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação (24x7)                                                                                        | Mês     | 60   |
| 6    | Serviços técnicos especializados em privacidade e Proteção de Dados, sob demanda (itens de catálogo).                                                                               | Entrega | 290  |
| 7    | Saldo de horas técnicas especializadas para demandas supervenientes não catalogadas                                                                                                 | Hora    | 320  |

**3. Requisitos quanto às subscrições e perfis de acesso:**

3.1 A volumetria indicada na tabela abaixo constitui requisito mínimo de capacidade de varredura e classificação imposto à solução, e não quantidade licenciada. A solução deverá comportar o crescimento natural do ambiente ao longo da vigência contratual, observado o limite de 20% (vinte por cento) sobre a volumetria inicial, sem custo adicional para o Banco.

3.2 A solução deverá ser contratada por subscrição corporativa, sem limitação por número de usuários nomeados, e deverá comportar, no mínimo, os perfis e quantitativos indicados nas tabelas abaixo, admitida capacidade superior:

| <b>SUBSCRIÇÃO ANUAL DE SOLUÇÃO TECNOLÓGICA PARA APOIO À GOVERNANÇA, GESTÃO, MONITORAMENTO E CONFORMIDADE EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.</b> |                                                                                                                                 |                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Perfil                                                                                                                                                    | Descrição                                                                                                                       | Quantitativo                 |
| Administrador                                                                                                                                             | Usuários com poder de configuração e parametrização da plataforma:<br>1 - Encarregado de dados;<br>1 - Coordenador do processo; | Mínimo de 5 (cinco) usuários |

**SUBSCRIÇÃO ANUAL DE SOLUÇÃO TECNOLÓGICA PARA APOIO À GOVERNANÇA, GESTÃO, MONITORAMENTO E CONFORMIDADE EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.**

| Perfil        | Descrição                                                                                                                                                                                                                                            | Quantitativo                                   |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
|               | 3 – Analistas de Privacidade e Proteção de dados.                                                                                                                                                                                                    |                                                |
| Demais perfis | Gestores de unidade, usuários operacionais, usuários de consulta, responsáveis pelas unidades organizacionais, usuários externos (terceiros e operadores), titulares de dados, auditores e usuários de integração por interface de programação (API) | Ilimitados, sem impacto no preço da subscrição |

**SUBSCRIÇÃO ANUAL DE SOLUÇÃO PARA IDENTIFICAÇÃO, MAPEAMENTO, INVENTÁRIO, CLASSIFICAÇÃO E MONITORAMENTO DE DADOS PESSOAIS E SENSÍVEIS EM BASES ESTRUTURADAS E NÃO ESTRUTURADAS**

| Perfil        | Descrição                                                                                                                                                                            | Quantitativo                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Administrador | Usuários com poder de configuração e parametrização da plataforma:<br>1 - Encarregado de dados;<br>1 - Coordenador do processo;<br>3 – Analistas de Privacidade e Proteção de dados. | Mínimo de 5 (cinco) usuários, sem limite máximo |
| Demais perfis | Usuários operacionais, usuários de consulta, responsáveis pelas unidades organizacionais, auditores e usuários de integração por interface de programação (API)                      | Ilimitados, sem impacto no preço da subscrição  |

| Tecnologias de Banco de Dados | Capacidade de Armazenamento Utilizada |
|-------------------------------|---------------------------------------|
| <b>Oracle</b>                 | 214.684,02 GB (≈ 214,68 TB)           |
| <b>SQL Server</b>             | 9.892,43 GB (≈ 9,89 TB)               |
| <b>MySQL</b>                  | 99,00 GB (≈ 0,10 TB)                  |

- 3.1. Todos os requisitos devem ser entregues licenciados e operacionais, sem ônus adicional à CONTRATANTE. As expressões “deve”, “permite”, “suporta”, “efetua”, “proporciona” e “possui” significam que a funcionalidade deve ser entregue operacional.
- 3.2. Todas as capacidades são especificadas em seu requisito mínimo, podendo ser entregue capacidade superior.
- 3.3. A solução deverá ser fornecida em versão estável e suportada pelo fornecedor, com manutenção e atualização durante toda a vigência contratual, não constando, no momento da proposta, em lista de descontinuidade (End-of-Life, End-of-Sale ou End-of-Support).
- 3.4. A solução deverá ser disponibilizada e entregue ativada, com os devidos acessos concedidos à equipe do CONTRATANTE.

**4. Requisitos gerais da solução**

- 4.1. A solução deverá ser disponibilizada na modalidade Software como Serviço (SaaS), em ambiente de nuvem de responsabilidade da CONTRATADA.

- 4.2. A solução deverá ser capaz de integrar-se ao ambiente tecnológico do CONTRATANTE por meio de mecanismos de integração amplamente reconhecidos no mercado (APIs, conectores, serviços web, arquivos estruturados ou meios equivalentes), independentemente de tecnologia, produto ou fornecedor específico, observados os requisitos de segurança e governança de dados do Banco.
- 4.3. A solução deverá ser capaz de realizar a descoberta e classificação de dados pessoais em fontes estruturadas e não estruturadas do ambiente do CONTRATANTE (bancos de dados relacionais e não relacionais, repositórios de arquivos, serviços de armazenamento e correio corporativo).
- 4.4. As funcionalidades que dependam de interação com o usuário devem ser disponibilizadas via interface web, sem necessidade de instalação de agentes nas estações dos usuários. Eventuais componentes de coleta em rede interna, se necessários, deverão ser compatíveis com o ambiente do CONTRATANTE.
- 4.5. As interfaces, orientações de uso e documentação devem estar disponíveis no idioma português do Brasil (PT-BR).
- 4.6. A aplicação web deve operar nas versões atuais dos principais navegadores de mercado e ser compatível com dispositivos móveis (web responsivo ou aplicativo móvel).
- 4.7. O CONTRATANTE será responsável por fornecer a infraestrutura de rede e conectividade necessária ao acesso à solução. Todas as licenças necessárias ao funcionamento da solução SaaS deverão ser fornecidas pela CONTRATADA.
- 4.8. A solução deverá disponibilizar, além do ambiente de produção, ambiente de homologação independente, sem custo adicional, destinado a testes de parametrizações, integrações e novas versões antes da sua entrada em produção.
- 4.9. A inclusão de novos usuários, perfis, unidades organizacionais, operações de tratamento, titulares, registros, evidências ou fontes de dados ao longo da vigência contratual não poderá gerar custo adicional para o CONTRATANTE, observados os limites de capacidade expressamente previstos neste Anexo.
- 4.10. Os requisitos deste Anexo classificados como desejáveis não são exigíveis para a habilitação nem para a aceitação da proposta, e a sua ausência não enseja desclassificação.

## **Item 1 – Componente de gestão e governança de conformidade com a LGPD**

### **5.1 Segurança e controle de acesso**

- 5.1.1. Autenticação segura, com possibilidade de integração aos mecanismos corporativos de autenticação e identidade do CONTRATANTE (por exemplo, diretório corporativo ou provedores de identidade de mercado).
- 5.1.2. Bloqueio de sessão ou logout automático por tempo de inatividade.
- 5.1.3. Autenticação de múltiplos fatores (MFA/2FA).
- 5.1.4. Acesso único (single sign-on) às funcionalidades e módulos da solução, sem necessidade de credenciais adicionais.
- 5.1.5. Registro (logs) de todas as atividades e tentativas de login/logout, com identificação de usuário, data, hora e endereço IP.
- 5.1.6. Geração de logs de administração e de atividades dos usuários, para fins de auditoria, com consulta e geração de relatórios.
- 5.1.7. Segregação de funções baseada em perfis/grupos configuráveis, com criação e personalização de papéis conforme necessidade do CONTRATANTE.
- 5.1.8. Acesso controlado a usuários externos (terceiros/fornecedores e titulares de dados).
- 5.1.9. Proteção das informações em trânsito e em repouso, mediante uso de criptografia e de padrões de segurança amplamente reconhecidos no mercado nas comunicações e integrações.
- 5.1.10. Aderência a boas práticas de segurança de aplicações web amplamente reconhecidas no mercado.
- 5.1.11. Atualizações periódicas para refletir mudanças na legislação e melhores práticas, além de correções de segurança e novas versões.
- 5.1.12. Suporte a hierarquias organizacionais configuráveis, com gestão centralizada e/ou distribuída e geração de relatórios consolidados respeitando a estrutura hierárquica.

## **5.2. Interface, painéis e relatórios**

5.2.1. Criação de painéis gerenciais e dashboards de forma intuitiva, sem necessidade de programação, com gráficos de diferentes tipos, filtros, drill-down e organização de layout pelo usuário.

5.2.2. Geração, impressão e exportação de relatórios em formatos amplamente utilizados (no mínimo CSV, PDF e um formato estruturado como XML).

5.2.3. Envio automático e agendado de relatórios e gráficos a usuários ou grupos.

5.2.4. Visões de acompanhamento do registro e do inventário de dados e indicadores do grau de atendimento aos requisitos legais e regulatórios aplicáveis.

5.2.5. Identificação institucional do CONTRATANTE nas comunicações, formulários e portais destinados a titulares de dados e a terceiros, mediante configuração, sem necessidade de desenvolvimento.

5.2.6. Criação de formulários e relatórios sem necessidade de programação.

## **5.3. Automação e integração**

5.3.1. Recursos de automação de processos e fluxos de trabalho por interface gráfica (low-code/no-code), com estágios, tarefas paralelas ou sequenciais e regras de decisão e aprovação, sem necessidade de programação.

5.3.2. Criação de formulários e campos personalizáveis sem necessidade de programação ou alteração de estrutura de banco de dados.

5.3.3. Integração com sistemas do CONTRATANTE e de terceiros por meio de mecanismos amplamente reconhecidos no mercado (serviços web REST/SOAP, APIs, conectores, JDBC/ODBC, LDAP, arquivos CSV/XLS/XML, e-mail ou equivalentes), com documentação em português do Brasil.

5.3.4. Comunicação criptografada nas integrações, observados padrões de segurança de mercado.

## **5.4. Inventário e registro das operações de tratamento (ROPA)**

5.4.1. Mapeamento e inventário de dados pessoais por meio de questionários integrados aos demais módulos, com modelos pré-definidos aderentes aos requisitos legais brasileiros e questionários personalizáveis.

5.4.2. Registro, atualização e consulta de critérios de decisões automatizadas.

5.4.3. Atualização do inventário diante de alterações em ativos, processos ou atividades de tratamento, com trilha de auditoria das alterações.

5.4.4. Recursos de visualização de mapeamento (mapas de calor e gráficos por processo) e emissão de relatórios em atendimento ao art. 37 da LGPD.

5.4.5. Associação de riscos, controles e bases legais a cada item do inventário e apoio à emissão de RIPD, LIA e ROPA.

## **5.5. Gestão de terceiros/fornecedores**

5.5.1. Portal para que terceiros/fornecedores respondam questionários de avaliação sobre tratamento de dados pessoais, com modelos pré-definidos e personalizáveis.

5.5.2. Emissão de relatório de conformidade contendo critérios de avaliação, riscos, planos de ação e percentual de adequação à LGPD.

5.5.3. Painel de gestão das avaliações, cadastro unitário ou em massa de fornecedores e gestão de contratos e termos aditivos.

## **5.6. Gestão de riscos à privacidade**

5.6.1. Cadastro, análise e monitoramento de riscos derivados das avaliações de inventário, terceiros, maturidade e Privacy by Design.

5.6.2. Classificação de riscos por impacto e probabilidade, registro de controles e medidas de mitigação.

5.6.3. Emissão do Relatório de Impacto à Proteção de Dados (RIPD/DPIA).

### **5.7. Gestão de incidentes de privacidade**

5.7.1. Registro de incidentes relativos à violação de dados pessoais, com identificação de atores, natureza da violação, dados e titulares envolvidos, impacto e evidências.

5.7.2. Fluxo de trabalho com aprovação de encerramento pelo Encarregado (DPO), notificações automáticas, subtarefas e rastreamento de risco.

5.7.3. Integração com sistemas de gestão de serviços de TI (ITSM) amplamente utilizados no mercado, por meio de API.

5.7.4. Geração de formulário de comunicação de incidente à ANPD conforme padrão definido pela Autoridade, e painel centralizado de monitoramento.

### **5.8. Privacy by Design, planos de ação, políticas e conformidade**

5.8.1. Avaliação de impacto à privacidade em novos projetos, serviços, processos e sistemas, com fluxo de avaliação e aprovação e monitoramento contínuo.

5.8.2. Planejamento e acompanhamento de ações corretivas e preventivas, com prazos, responsáveis, status e efetividade, em painel centralizado.

5.8.3. Criação, versionamento e gestão de políticas, normas e procedimentos de privacidade, com repositório centralizado e associação a controles e áreas.

5.8.4. Associação dos requisitos legais e regulatórios aplicáveis aos controles, políticas, planos de ação e evidências mantidos na solução, com acompanhamento do grau de atendimento de cada requisito e emissão de relatórios de conformidade.

### **5.9. Consentimentos, cookies e direitos dos titulares**

5.9.1. Coleta, armazenamento e gestão de consentimentos dos titulares em base centralizada, com múltiplos canais de coleta (formulários web, componentes para integração em sites e aplicações, APIs e importação de consentimentos existentes), versionamento e histórico de alterações.

5.9.2. Gestão de cookies com varredura periódica dos domínios do CONTRATANTE, classificação de cookies, banner personalizável, suporte a múltiplos idiomas com detecção automática, e registro de consentimento dos visitantes.

5.9.3. Portal do Titular para exercício e acompanhamento de direitos, com fluxos configuráveis por tipo de solicitação, protocolos, prazos monitorados, comunicação segura e geração de relatórios.

5.9.4. Integração do atendimento ao titular com o componente de descoberta e mapeamento, para localização dos dados pessoais do titular nas fontes do CONTRATANTE, após revisão e aprovação do Encarregado, com ocultação de dados de terceiros quando aplicável.

5.9.5. Possibilidade de autenticação do titular por meio de serviço público de identidade digital, quando aplicável.

## **6. Item 2 – Componente de identificação, mapeamento e monitoramento de dados pessoais em bases estruturadas e não estruturadas**

O componente deverá comportar, como requisito mínimo de capacidade, a varredura e a classificação da volumetria indicada no item 3 deste Anexo, admitido o crescimento natural do ambiente ao longo da vigência contratual até o limite de 20% (vinte por cento) sobre a volumetria inicial, sem custo adicional. A quantidade de fontes de dados cadastradas e o volume varrido não constituem unidade de medida da contratação.

6.1. Painéis analíticos apresentando, de forma dinâmica, totalizadores de fontes ativas, registros catalogados, dados classificados e dados pessoais por tipo, com histórico dos escaneamentos executados.

6.2. Gestão de perfis e usuários, com criação de tipos de usuário e definição de funcionalidades acessíveis, e mecanismos de busca.

6.3. Cadastro de fontes de dados de diferentes naturezas (bancos de dados relacionais e não relacionais, repositórios de arquivos e demais fontes), admitindo-se quaisquer tecnologias equivalentes de mercado, sem indicação de produto específico.

6.4. Varredura das fontes cadastradas para criação de catálogo de dados, com registro de data/hora, barra de progresso e busca/filtragem.

6.5. Descoberta e classificação de dados por meio de etiquetas configuráveis e classificadores personalizáveis (por exemplo, PII e dados sensíveis), inclusive por expressões regulares, com escaneamento incremental, reexecução e retomada do ponto de parada.

6.6. Descoberta de dados em fontes não estruturadas com apoio de reconhecimento óptico de caracteres (OCR) e mecanismo de contingência (fallback).

6.7. Capacidade de consultas distribuídas entre diferentes fontes de dados, com escalabilidade de consultas simultâneas.

6.8. Monitoramento contínuo e reexecução programada das varreduras, para manutenção do inventário atualizado.

### **7. Item 3 – Serviços de implantação da solução**

7.1. Os serviços de implantação compreendem o conjunto de atividades necessárias à disponibilização da solução em condições de uso pelo CONTRATANTE, são contratados em parcela única e somente serão faturados após a emissão do Termo de Aceitação Definitivo (TAD).

7.2. A implantação terá prazo máximo de 90 (noventa) dias corridos, contados da reunião inicial do projeto e encerrados com a emissão do TAD.

7.3. A reunião inicial do projeto será realizada em até 5 (cinco) dias úteis contados da assinatura do contrato, em data ajustada com o CONTRATANTE.

7.4. Na reunião inicial, a CONTRATADA apresentará a relação dos profissionais alocados e a comprovação da respectiva qualificação, indicando o responsável pela gestão do projeto, com experiência comprovada em implantação de solução equivalente, e o responsável técnico pela solução, com certificação oficial no produto ofertado ou declaração equivalente emitida pelo fabricante.

7.5. A CONTRATADA apresentará Plano de Implantação em até 5 (cinco) dias úteis contados da reunião inicial, detalhando fases, atividades, responsáveis, recursos, prazos, interdependências, marcos de aceite e produtos gerados em cada etapa, em formato que permita o acompanhamento pelo CONTRATANTE.

7.6. O Plano de Implantação será submetido à homologação do CONTRATANTE, que poderá requerer ajustes; a versão final será entregue em até 5 (cinco) dias úteis contados da solicitação de ajustes.

7.7. Os serviços de implantação abrangem, no mínimo:

7.7.1. levantamento dos requisitos de configuração junto às áreas do CONTRATANTE;

7.7.2. ativação das subscrições e disponibilização dos acessos, em até 5 (cinco) dias úteis contados da reunião inicial;

7.7.3. configuração e parametrização de todos os módulos contratados;

7.7.4. cadastro e estruturação de usuários, perfis de acesso, unidades organizacionais e hierarquias, conforme a estrutura do CONTRATANTE;

7.7.5. configuração do ambiente de produção e do ambiente de homologação;

7.7.6. integração com o mecanismo corporativo de autenticação e identidade, de modo a permitir o acesso único dos usuários;

7.7.7. configuração do serviço de envio de mensagens, de modo que as comunicações com titulares e terceiros utilizem domínio do CONTRATANTE;

7.7.8. configuração das interfaces de integração necessárias à comunicação com o ambiente do CONTRATANTE;

7.7.9. apoio à carga inicial e à migração das informações já existentes no CONTRATANTE, incluindo inventário de operações de tratamento, políticas, riscos, planos de ação, fornecedores e evidências, a partir de planilhas, arquivos estruturados ou solução preexistente;

- 7.7.10. cadastro e configuração das fontes de dados a serem varridas pelo componente de descoberta e execução da primeira varredura;
- 7.7.11. execução de testes funcionais e de integração, com registro dos resultados;
- 7.7.12. homologação, mediante configuração e execução completa de, no mínimo, 3 (três) processos ou fluxos por módulo contratado, com acompanhamento e validação da equipe do CONTRATANTE;
- 7.7.13. entrada em produção;
- 7.7.14. acompanhamento assistido da operação por 30 (trinta) dias corridos contados da entrada em produção;
- 7.7.15. entrega da documentação técnica e operacional da implantação, contemplando arquitetura implantada, parâmetros configurados, integrações realizadas, perfis criados, fluxos construídos, procedimentos de operação e registros das reuniões, testes e homologações.
- 7.8. O recebimento provisório ocorrerá após a comunicação de conclusão pela CONTRATADA; o Termo de Aceitação Definitivo será emitido após a verificação do atendimento integral do escopo, dos testes, da homologação e da documentação.
- 7.9. Todas as atividades de implantação correrão às expensas da CONTRATADA, cabendo ao CONTRATANTE o apoio técnico, a disponibilização dos acessos e ambientes necessários, a indicação dos responsáveis e a avaliação dos resultados.
- 7.10. Eventual componente de coleta a ser instalado no ambiente do CONTRATANTE será fornecido, licenciado, instalado e configurado pela CONTRATADA, sem custo adicional e sem alteração do preço da subscrição contratada.

#### **8. Item 4 – Transferência de conhecimento**

- 8.1. A transferência de conhecimento é contratada em parcela única e tem por finalidade assegurar ao CONTRATANTE autonomia para administrar, parametrizar e operar a solução, mitigando a dependência da CONTRATADA.
- 8.2. A CONTRATADA realizará, no mínimo:
  - 8.2.1. capacitação dos administradores da solução, com carga horária mínima de 16 (dezesesseis) horas, abrangendo administração da plataforma, gestão de usuários e perfis, parametrização dos módulos, construção de formulários, fluxos, painéis e relatórios, configuração de integrações e rotinas de exportação de dados;
  - 8.2.2. capacitação dos usuários-chave e dos responsáveis pelas unidades organizacionais, com carga horária mínima de 8 (oito) horas, abrangendo a operação dos módulos contratados;
  - 8.2.3. capacitação específica dos responsáveis pelo componente de descoberta e classificação de dados, com carga horária mínima de 8 (oito) horas.
- 8.3. As capacitações serão realizadas em língua portuguesa do Brasil, de forma presencial ou remota, conforme definição do CONTRATANTE, em turmas e datas constantes do cronograma homologado, com material autorizado pelo fabricante da solução.
- 8.4. A CONTRATADA disponibilizará, sem custo adicional e sem restrição de uso interno pelo CONTRATANTE: material didático das capacitações; manuais de administração e de uso da solução, em português do Brasil; documentação das parametrizações realizadas na implantação; e gravação das sessões, quando realizadas de forma remota.
- 8.5. Ao término da implantação, a CONTRATADA promoverá o repasse formal das configurações realizadas, mediante apresentação e entrega da documentação das parametrizações, dos fluxos, dos perfis, das integrações e dos procedimentos de operação, com registro em ata assinada pelas partes.
- 8.6. A CONTRATADA manterá disponíveis, durante toda a vigência contratual, conteúdos de capacitação sobre o uso da solução, em português do Brasil, ao menos em formato remoto, sem custo adicional.
- 8.7. A transferência de conhecimento prevista neste item não se confunde com as ações institucionais de treinamento e conscientização em privacidade destinadas ao conjunto dos empregados do CONTRATANTE, que não integram o objeto desta contratação.

## **9. Item 5 – Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação**

9.1. Os serviços continuados de suporte, manutenção, operação assistida e sustentação visam manter e evoluir o programa de gestão de privacidade e proteção de dados pessoais do CONTRATANTE, assegurando a disponibilidade, o desempenho e a atualização da solução.

9.2. [A fase de suporte e operação será iniciada após a emissão do Termo de Aceitação Definitivo da implantação, mediante Ordem de Serviço específica emitida pelo CONTRATANTE.](#)

9.3. A prestação será baseada em remuneração por resultados, com pagamento mensal, após mensuração e validação de métricas quantitativas e qualitativas conforme os Níveis Mínimos de Serviço (NMS) definidos neste documento.

9.4. O modelo contempla atividades demandadas pelo CONTRATANTE (abertura de chamados técnicos, consultas) e atividades desenvolvidas periodicamente pela CONTRATADA (monitoramento da solução, parametrização de regras e políticas, apresentação tempestiva de relatórios), conforme periodicidade e níveis de serviço definidos.

9.5. A CONTRATADA prestará serviços em regime 24x7 para atividades de administração, monitoramento da saúde da solução, backup e restore, sustentação, resolução de problemas, troubleshooting e atualizações conforme disponibilização pelo fornecedor; e em regime 8x5 para atendimento a dúvidas técnicas, diagnóstico e resolução de problemas, criação e manutenção de políticas e regras, parametrização, identificação de melhorias e elaboração de relatórios executivos, gerenciais e operacionais.

9.6. A CONTRATADA será responsável pela gestão, manutenção, configuração, suporte e administração da solução, mantendo-a atualizada (patches, correções e novas versões), realizando o ajuste fino (tuning) e a gerência de segurança da solução.

9.7. A CONTRATADA disponibilizará canal para abertura de chamados via web, sem limite mensal de quantidade, com número único de identificação, notificações por e-mail, escalonamento conforme prioridade e sistema de controle de chamados acessível ao CONTRATANTE para acompanhamento e auditoria.

9.8. Os chamados somente poderão ser fechados após autorização do CONTRATANTE. Para apuração do NMS, serão desconsiderados os períodos em que o CONTRATANTE for responsável por executar ações necessárias ao atendimento.

9.9. Integram os serviços continuados, sem custo adicional: a criação e a alteração de painéis, relatórios e formulários; a configuração de integrações mediante conector ou interface já contemplada na solução; a alteração de configurações administrativas; a gestão de usuários e perfis; e a aplicação de atualizações, correções e novas versões, observados os indicadores NMS-06 a NMS-13.

## **10. Itens 6 e 7 – Serviços técnicos especializados por entrega e saldo de horas técnicas**

10.1. Os serviços técnicos especializados caracterizam-se pelo elevado nível de conhecimento necessário à execução de atividades relativas à privacidade e à proteção de dados pessoais e são remunerados por entrega, a partir do catálogo constante do item 10.11, que define, para cada serviço, o escopo, o produto esperado, os critérios de aceite, o prazo e a faixa de complexidade.

10.2. [A remuneração por entrega decorre do fato de os produtos de cada serviço serem previamente identificáveis e verificáveis, em observância à Súmula TCU nº 269, ao art. 26, item 2, do Regulamento de Licitações e Contratos do Banco da Amazônia e ao art. 3º, inciso III, da Resolução CGPAR nº 45/2022. A variabilidade da demanda recai sobre a quantidade e a oportunidade dos acionamentos, e não sobre a natureza dos produtos.](#)

10.3. Toda demanda será previamente autorizada mediante Ordem de Serviço emitida pelo CONTRATANTE, que indicará o serviço catalogado, a faixa de complexidade, o objeto específico, os produtos esperados, os critérios de aceite, o prazo de entrega e os responsáveis pelo acompanhamento.

10.4. Para cada entrega, a CONTRATADA apresentará relatório técnico contendo a identificação da Ordem de Serviço, o escopo executado, o método adotado, os produtos entregues e as respectivas evidências, os profissionais responsáveis e a demonstração do atendimento aos critérios de aceite e ao prazo. O pagamento será realizado exclusivamente sobre as entregas aceitas, mediante Termo de Aceite da Entrega emitido pela área técnica do CONTRATANTE.

10.5. As faixas de complexidade são definidas objetivamente: complexidade baixa, para entregas que recaiam sobre uma única operação de tratamento, solicitação ou fornecedor, com esforço de referência de até 8 (oito) horas e um único produto; complexidade média, para entregas que envolvam mais de uma unidade organizacional ou até 3 (três) produtos, com esforço de referência superior a 8 (oito) e até 24 (vinte e quatro) horas; e complexidade alta, para entregas que envolvam múltiplas unidades ou sistemas, produto submetido a instância de governança ou revisão integral de macroprocesso, com esforço de referência superior a 24 (vinte e quatro) e até 60 (sessenta) horas. O esforço de referência é parâmetro de enquadramento e não constitui unidade de medida da remuneração.

10.6. O quantitativo estimado de entregas constitui limite máximo, não gera direito subjetivo à execução integral e não impõe consumo mínimo. As entregas não demandadas em determinado exercício poderão ser realizadas em períodos subsequentes, respeitados o total estimado e o prazo contratual.

10.7. A estimativa de demandas anuais tomou por base as obrigações permanentes decorrentes da Lei nº 13.709/2018, o Mapa de Riscos LGPD anexo, a estrutura organizacional do CONTRATANTE e o ciclo de evolução do seu ambiente tecnológico, tendo sido compatibilizada com as probabilidades atribuídas aos riscos R-04, R-06 e R-07 do referido Mapa, em especial quanto ao atendimento a titulares e ao tratamento de incidentes de privacidade.

10.8. As atividades de criação e alteração de painéis, relatórios e formulários e a configuração de integrações mediante conector já contemplado na solução integram os serviços continuados de suporte e sustentação e não são passíveis de acionamento como serviço técnico especializado, vedada a duplicidade de remuneração pelo mesmo fato.

10.9. Os profissionais alocados aos serviços técnicos especializados deverão possuir formação superior e experiência comprovada na matéria objeto da entrega, admitindo-se, como referência de qualificação, certificações profissionais em privacidade e proteção de dados, em segurança da informação ou em governança de tecnologia da informação, sem que a ausência de certificação específica constitua critério de habilitação ou de aceitação da proposta.

10.10. A execução dos serviços técnicos especializados será aferida pelos indicadores NMS-21 a NMS-23, aplicando-se os descontos previstos neste Anexo em caso de descumprimento.

10.11. Catálogo de serviços técnicos especializados, organizado por macrotema, com o respectivo produto principal, faixa de complexidade e quantitativo anual estimado:

| <b>Cód.</b> | <b>Macrotema e serviço</b>                                                                                                              | <b>Produto principal (entregável)</b>                                                                                       | <b>Complex.</b> | <b>Qtd./ano</b> |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------|
| CS-01       | Governança de Privacidade –<br>Elaboração ou revisão de<br>instrumento normativo de<br>privacidade (política, norma<br>ou procedimento) | Minuta do<br>instrumento<br>normativo revisada e<br>validada, com o<br>respectivo registro e<br>versionamento na<br>solução | Média           | 4               |
| CS-02       | Evolução da maturidade em<br>privacidade – Diagnóstico do<br>programa de privacidade e<br>plano de evolução                             | Relatório de<br>diagnóstico e plano<br>de evolução com<br>ações, prazos e<br>responsáveis                                   | Alta            | 1               |

| Cód.  | Macrotema e serviço                                                                                                                          | Produto principal (entregável)                                                                                                           | Complex. | Qtd./ano |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------|----------|
|       |                                                                                                                                              | registrados na solução                                                                                                                   |          |          |
| CS-03 | Inventário e Mapeamento de Dados – Análise e registro de operação de tratamento no inventário (ROPA)                                         | Operação registrada no inventário, com finalidade, base legal, categorias de dados, ciclo de vida, compartilhamentos e riscos associados | Baixa    | 10       |
| CS-04 | Inventário e Mapeamento de Dados – Revisão integral do inventário de macroprocesso                                                           | Inventário do macroprocesso revisado e atualizado, com relatório de lacunas e plano de correção                                          | Alta     | 2        |
| CS-05 | RIPD/DPIA – Elaboração de Relatório de Impacto à Proteção de Dados                                                                           | RIPD emitido na solução, com identificação dos riscos, medidas mitigadoras e conclusão                                                   | Alta     | 4        |
| CS-06 | Gestão de Riscos de Privacidade – Avaliação de riscos e plano de tratamento, inclusive avaliação de legítimo interesse quando aplicável      | Avaliação de riscos registrada na solução e plano de tratamento com controles, prazos e responsáveis                                     | Média    | 3        |
| CS-07 | Privacy by Design – Avaliação de privacidade desde a concepção em produto, serviço, processo ou sistema, inclusive tratamentos automatizados | Parecer técnico de privacidade por concepção, com requisitos e recomendações registrados na solução                                      | Média    | 6        |
| CS-08 | Gestão de Incidentes – Apoio técnico à análise, contenção, documentação e comunicação de incidente de privacidade                            | Incidente registrado na solução, relatório de análise e minutas das comunicações ao titular e à ANPD                                     | Média    | 6        |
| CS-09 | Atendimento aos Titulares – Apoio técnico ao atendimento de solicitação de titular de alta complexidade                                      | Resposta técnica fundamentada, com evidências da localização e do                                                                        | Baixa    | 10       |

| Cód.         | Macrotema e serviço                                                                                                          | Produto principal (entregável)                                                                   | Complex. | Qtd./ano                                                 |
|--------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------|----------------------------------------------------------|
|              |                                                                                                                              | tratamento dos dados do titular                                                                  |          |                                                          |
| CS-10        | Gestão de Terceiros – Avaliação de privacidade de operador, suboperador ou terceiro                                          | Relatório de avaliação com riscos, plano de ação e percentual de adequação registrado na solução | Média    | 4                                                        |
| CS-11        | Adequação normativa – Análise de impacto de ato normativo ou regulatório superveniente e plano de adequação                  | Nota técnica de impacto e plano de adequação com ações, prazos e responsáveis                    | Média    | 3                                                        |
| CS-12        | Apoio técnico especializado – Integração da solução com sistema ou fonte de dados do CONTRATANTE não prevista na implantação | Integração configurada, testada, homologada e documentada                                        | Alta     | 2                                                        |
| CS-13        | Treinamentos e Conscientização – Capacitação técnica complementar sobre a solução ou sobre processos de privacidade          | Turma realizada, com material, lista de presença e avaliação de aproveitamento                   | Média    | 3                                                        |
| <b>TOTAL</b> | Total estimado por ano e para a vigência contratual                                                                          | —                                                                                                | —        | <b>58 entregas/ano;<br/>290 entregas em<br/>60 meses</b> |

10.12. Para fins de composição da proposta e de medição, as entregas são agrupadas por faixa de complexidade, com os seguintes quantitativos estimados: complexidade baixa — 20 (vinte) entregas por ano, 100 (cem) entregas em 60 (sessenta) meses; complexidade média — 29 (vinte e nove) entregas por ano, 145 (cento e quarenta e cinco) entregas em 60 (sessenta) meses; e complexidade alta — 9 (nove) entregas por ano, 45 (quarenta e cinco) entregas em 60 (sessenta) meses.

10.13. Item 7 – Saldo de horas técnicas especializadas. Para o atendimento de demandas supervenientes relacionadas à privacidade e à proteção de dados pessoais que não se enquadrem em nenhum dos serviços catalogados, fica previsto saldo de 64 (sessenta e quatro) horas técnicas por ano de vigência, totalizando 320 (trezentas e vinte) horas, de acionamento subsidiário e excepcional.

10.14. O acionamento do saldo de horas observará as seguintes regras: solicitação formal da área demandante, com descrição do resultado pretendido; manifestação técnica do gestor do contrato atestando a inexistência de serviço catalogado equivalente e a ausência de sobreposição com os serviços de implantação, de transferência de conhecimento e de suporte e sustentação; apresentação, pela CONTRATADA, de proposta técnica com escopo, produtos, cronograma, perfis profissionais e estimativa de horas; autorização prévia mediante Ordem de Serviço, que fixará o teto de horas e os critérios de aceite; registro diário das horas efetivamente utilizadas, por profissional e atividade; apresentação de relatório de execução com evidências dos produtos; aceite formal do CONTRATANTE, que poderá glosar horas não comprovadas ou

não aderentes ao escopo autorizado; e faturamento exclusivamente das horas autorizadas, executadas, comprovadas e aceitas.

10.15. O saldo de horas não poderá ser utilizado para a execução de serviços catalogados, para atividades compreendidas nos serviços de implantação, de transferência de conhecimento ou de suporte e sustentação, nem para o atendimento de obrigações já remuneradas na subscrição.

10.16. O gestor do contrato manterá controle do saldo de horas remanescente, com registro de cada autorização, execução e aceite, disponibilizado à fiscalização e à auditoria interna e externa.

## 11. Níveis Mínimos de Serviço

### 11.1. Indicadores da plataforma e dos serviços de suporte e operação

| Ref.   | Métrica                                 | Descrição                                                                                                                                                                                                                                                                      | NMS de referência                                                                                                                                 |
|--------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| NMS-01 | Disponibilidade mensal da solução       | Percentual de tempo em que as funcionalidades contratadas permanecem disponíveis aos usuários autorizados, em regime 24x7. Apurado mensalmente, excluída a janela de manutenção programada de até 2 (duas) horas por mês, previamente comunicada e acordada com o CONTRATANTE. | Mínimo de 99,0% ao mês                                                                                                                            |
| NMS-02 | Tempo objetivo de recuperação (RTO)     | Tempo máximo para restabelecimento da solução após evento de indisponibilidade que exija acionamento do plano de continuidade. Medido entre a declaração do evento e o restabelecimento do serviço em condições de uso.                                                        | Até 4 (quatro) horas                                                                                                                              |
| NMS-03 | Ponto objetivo de recuperação (RPO)     | Perda máxima de dados admitida, medida em tempo, na recuperação posterior a evento de indisponibilidade. Intervalo máximo entre o último ponto de recuperação íntegro e o momento do evento.                                                                                   | Até 1 (uma) hora                                                                                                                                  |
| NMS-04 | Comunicação de incidente ao CONTRATANTE | Prazo para comunicar incidente de segurança da informação ou de privacidade, violação de dados pessoais, falha de segregação ou perda de dados. Medido entre a ciência do evento pela CONTRATADA e a comunicação formal ao CONTRATANTE.                                        | Comunicação inicial em até 2 (duas) horas; relatório preliminar em até 24 (vinte e quatro) horas; relatório conclusivo em até 10 (dez) dias úteis |
| NMS-05 | Desempenho da solução                   | Tempo de resposta das funcionalidades interativas contratadas. Apurado mensalmente sobre as transações registradas na solução.                                                                                                                                                 | Até 5 (cinco) segundos em 95% das transações                                                                                                      |
| NMS-06 | Alteração de configurações              | Solicitações de gestão de acesso, registros de auditoria da ferramenta ou outras configurações administrativas. Tempo decorrido entre a abertura do chamado e a implementação da solicitação.                                                                                  | 8 horas após abertura de chamado                                                                                                                  |
| NMS-07 | Construção de dashboards                | Solicitações de criação ou alteração de gráficos e disponibilização de painéis. Tempo decorrido entre a abertura do                                                                                                                                                            | 48 horas após abertura de chamado                                                                                                                 |

| Ref.   | Métrica                                               | Descrição                                                                                                                                                                                  | NMS de referência                                |
|--------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
|        |                                                       | chamado e a disponibilização do acesso ao painel.                                                                                                                                          |                                                  |
| NMS-08 | Construção de relatórios                              | Solicitações de criação de novos modelos de relatórios automatizados na ferramenta. Tempo decorrido entre a abertura do chamado e a disponibilização do acesso ao relatório.               | 5 dias corridos após abertura de chamado         |
| NMS-09 | Construção de formulários                             | Solicitações de criação de novos modelos de formulários automatizados na ferramenta. Tempo decorrido entre a abertura do chamado e a disponibilização do acesso ao formulário.             | 5 dias corridos após abertura de chamado         |
| NMS-10 | Atendimento a chamados para esclarecimento de dúvidas | Suporte a dúvidas e questões relacionadas à solução ou aos serviços contratados. Tempo decorrido entre a abertura do chamado e a resposta da solicitação.                                  | 48 horas após abertura de chamado                |
| NMS-11 | Atualização de segurança da solução                   | Implementação de correções e atualizações de segurança, incluído o tempo de homologação do pacote pela CONTRATADA. Tempo decorrido entre a liberação da atualização e a sua implementação. | 30 dias corridos após a liberação da atualização |
| NMS-12 | Configuração de integração                            | Configuração de integração mediante conector ou interface já contemplada na solução contratada. Tempo decorrido entre a solicitação e a conclusão da integração.                           | 10 dias                                          |
| NMS-13 | Troca de informações                                  | Resposta a solicitações de informação formuladas pelos analistas do CONTRATANTE aos analistas da CONTRATADA. Tempo decorrido entre a solicitação e o recebimento da informação.            | 1 hora                                           |

## 11.2. Níveis de severidade dos chamados

| Ref.   | Severidade                       | Descrição                                                    | 1ª resposta                                           | Solução remota                                                   |
|--------|----------------------------------|--------------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------|
| NMS-14 | Urgente / Crítica / Severidade 1 | A solução está totalmente parada ou inoperante.              | Até 2 (duas) horas após a abertura do chamado remoto. | Até 24 (vinte e quatro) horas após a abertura do chamado remoto. |
| NMS-15 | Alta / Severidade 2              | A solução está ativa, mas com inoperância da maioria de suas | Até 4 (quatro) horas após                             | Até 2 (dois) dias após a abertura do                             |

| Ref.   | Severidade            | Descrição                                                                         | 1ª resposta                                            | Solução remota                                         |
|--------|-----------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------|
|        |                       | funcionalidades, causando impacto negativo no ambiente de produção.               | a abertura do chamado remoto.                          | chamado remoto.                                        |
| NMS-16 | Normal / Severidade 3 | A solução está operativa, mas suas funcionalidades são executadas com restrições. | Até 8 (oito) horas após a abertura do chamado remoto.  | Até 4 (quatro) dias após a abertura do chamado remoto. |
| NMS-17 | Baixa / Severidade 4  | A solução está operativa e a falha não compromete suas funcionalidades.           | Até 12 (doze) horas após a abertura do chamado remoto. | Até 6 (seis) dias após a abertura do chamado remoto.   |

### 11.3. Demais indicadores da série única

Integram o conjunto de Níveis Mínimos de Serviço da contratação, em série numérica única com as tabelas acima, os seguintes indicadores:

NMS-18 – Cumprimento do cronograma de implantação: atendimento integral dos marcos do Plano de Implantação homologado pelo CONTRATANTE, apurado na emissão do Termo de Aceitação Definitivo.

NMS-19 – Entrega da documentação técnica e operacional da implantação, inclusive da documentação das parametrizações realizadas: até 10 (dez) dias úteis contados da entrada em produção.

NMS-20 – Realização das turmas de capacitação e entrega dos materiais de apoio previstos no item de transferência de conhecimento: conforme cronograma homologado, com índice mínimo de 95% (noventa e cinco por cento) das turmas realizadas nas datas pactuadas.

NMS-21 – Prazo de entrega dos serviços técnicos especializados, contado da emissão da Ordem de Serviço: 5 (cinco) dias úteis para entregas de complexidade baixa, 10 (dez) dias úteis para complexidade média e 20 (vinte) dias úteis para complexidade alta, salvo prazo diverso pactuado na própria Ordem de Serviço.

NMS-22 – Índice de aceite das entregas dos serviços técnicos especializados na primeira apresentação: mínimo de 90% (noventa por cento) das entregas apuradas no trimestre.

NMS-23 – Prazo para correção de entrega devolvida de forma motivada pelo CONTRATANTE: 5 (cinco) dias úteis contados da devolução.

NMS-24 – Entrega do Relatório de Serviços Prestados: até o 5º (quinto) dia útil do mês subsequente, sendo a sua apresentação condição para o pagamento.

NMS-25 – Atendimento a solicitação de exportação ou devolução de dados: até 10 (dez) dias úteis, em formato estruturado, aberto ou amplamente utilizado, acompanhado de dicionário de dados e leiaute.

A numeração dos indicadores é única e vinculante para o Estudo Técnico Preliminar, para o Termo de Referência, para os seus anexos e para a minuta contratual, vedada a reutilização da mesma referência para obrigações distintas.

### 11.4. Descontos pelo não cumprimento dos NMS

11.4.1 Ao final do mês será computado o percentual de atendimento aos Níveis Mínimos de Serviço.



11.4.2. Caso o nível de atendimento seja inferior a 95%, será aplicado desconto de 15% na nota fiscal/fatura dos serviços; entre 95% e 96,99%, desconto de 5%; entre 97% e 97,99%, desconto de 3%.

11.4.3. Os descontos na fatura dos serviços de suporte e operação serão limitados a 30% do seu valor; ultrapassado esse limite, aplicam-se as sanções administrativas previstas no Termo de Referência.

11.4.4. Os chamados somente poderão ser fechados após autorização do CONTRATANTE; o fechamento não autorizado sujeita a CONTRATADA a multa de 0,5% do valor mensal do serviço por chamado, cumulativamente.

11.4.5. A frequência de aferição é mensal, devendo a CONTRATADA elaborar Relatório de Serviços Prestados (RSP) até o 5º dia útil do mês subsequente, contendo os níveis de serviço acordados e alcançados, resultados, disponibilidade e desempenho de chamados. A entrega do relatório é condição para o pagamento.

O descumprimento dos indicadores NMS-18 a NMS-20 sujeita a CONTRATADA a desconto de 0,5% (cinco décimos por cento) do valor do respectivo item por dia útil de atraso, limitado a 10% (dez por cento) do valor do item.

O descumprimento do indicador NMS-21 sujeita a CONTRATADA a desconto de 2% (dois por cento) do valor da entrega por dia útil de atraso, limitado a 20% (vinte por cento) do valor da entrega. O descumprimento do NMS-22, apurado trimestralmente, sujeita a CONTRATADA a desconto de 5% (cinco por cento) sobre o valor das entregas aceitas no trimestre.

Os descontos por descumprimento de Nível Mínimo de Serviço constituem adequação do pagamento ao serviço efetivamente prestado, na linha do Acórdão nº 717/2010-Plenário do Tribunal de Contas da União, e não se confundem com as sanções administrativas previstas neste instrumento, vedada a dupla incidência pelo mesmo fato.

**ANEXO VI****ROTEIRO DO TESTE DE PROVA DE CONCEITO****1. DO TESTE DE PROVA DE CONCEITO**

- 1.1. Da(s) licitante(s) classificada(s) em primeiro lugar será realizada prova de conceito do software licitado, em até 15 (quinze) dias, que deverá seguir o mesmo padrão do especificado no Edital e na Proposta.
- 1.2. A solicitação da apresentação da prova de conceito será encaminhada via “chat” no sistema eletrônico de licitação e deverá ser realizada de forma on-line, via aplicativo Microsoft Teams, no prazo fixado pelo pregoeiro. A data da realização do procedimento será informada a todos os interessados através do próprio sistema, via chat.
- 1.3. Não será aceita a proposta da licitante que tiver a prova de conceito rejeitada, que não a apresentar, ou que apresentá-la fora do prazo estabelecido.
- 1.4. Para a presente contratação entende-se o termo software como sendo um exemplar completo, que segue as especificações técnicas constantes do Termo de Referência do Edital, com o fim de ser analisada quanto à sua conformidade com o especificado.
- 1.5. As despesas necessárias à realização da Prova de Conceito correrão por conta da licitante. A prova será realizada integralmente de forma remota, não havendo despesas de deslocamento ou de locomoção de representantes.
- 1.6. Análise de conformidade com as especificações técnicas do edital;
- 1.7. Após a análise, a Comissão Técnica emitirá parecer indicando “aprovada sem ressalvas”, “aprovada com ressalvas” ou “reprovada”. A hipótese de aprovação com ressalvas restringe-se exclusivamente aos procedimentos classificados como desejáveis no roteiro, sendo concedido novo prazo de 3 (três) dias úteis para correção, mediante ajustes ou apresentação de nova prova de conceito.
- 1.8. Após as correções ou apresentação de nova prova de conceito, a Comissão Técnica emitirá novo parecer onde constará aprovada ou reprovada.
- 1.9. Caso reprovada, a licitante será desclassificada, sendo convocada a licitante seguinte. Os resultados das avaliações serão divulgados por meio de mensagem no sistema. As licitantes deverão colocar à disposição do Banco da Amazônia todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.
- 1.10. A licitante mais bem classificada na etapa de lances do pregão deverá realizar “prova de conceito”, para comprovar a aderência da solução oferecida as características técnicas previstas neste Termo de Referência. As provas de conceito serão realizadas no prazo fixado pelo pregoeiro.
- 1.11. O Teste de Prova de Conceito será realizado com base em relatório específico denominado Roteiro de Teste de Prova de Conceito, objetivo e detalhado contendo as funcionalidades e características funcionais que possam ser demonstradas, na forma dos requisitos abaixo:
- 1.12. Os demais licitantes participarão exclusivamente na condição de ouvintes, sendo-lhes terminantemente vedada qualquer manifestação, intervenção, interrupção ou questionamento aos técnicos da Administração ou à empresa proponente durante a execução dos testes.

- 1.13. Cada procedimento do roteiro é classificado como obrigatório ou desejável e possui critério objetivo de aprovação, aferido de forma binária, vedada a avaliação por juízo de conveniência. A reprovação em procedimento classificado como obrigatório enseja a reprovação da prova de conceito; a reprovação em procedimento classificado como desejável não enseja desclassificação.
- 1.14. Da sessão será lavrada ata circunstanciada, com o registro do resultado de cada procedimento, da respectiva motivação técnica e das manifestações apresentadas pelos demais licitantes na condição de ouvintes, a qual será juntada aos autos e disponibilizada no sistema eletrônico.

| ID | Grupo / Tema              | Procedimento de teste a ser demonstrado pela licitante                                                                                                                                                                                                                                                                                     | Atende? |
|----|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 1  | Gestão e acesso           | Realizar login utilizando autenticação de múltiplos fatores (MFA/2FA) e exibir os registros de auditoria que identificam usuário, endereço IP, data e hora da tentativa de acesso. (Obrigatório. Critério objetivo de aprovação: login concluído com segundo fator e exibição, na própria solução, do registro contendo os quatro campos.) |         |
| 2  | Interface                 | Acessar a solução por navegador web padrão e demonstrar a apresentação em dispositivo móvel, com interface integralmente em português do Brasil. (Obrigatório. Critério objetivo de aprovação: acesso concluído em navegador e em dispositivo móvel, com todos os menus apresentados em português do Brasil.)                              |         |
| 3  | Painéis                   | Criar um painel gerencial com ao menos um gráfico e demonstrar a funcionalidade de detalhamento (drill-down), sem uso de programação. (Obrigatório. Critério objetivo de aprovação: painel criado durante a sessão e gráfico detalhado por, no mínimo, um nível, sem edição de código.)                                                    |         |
| 4  | Automação                 | Criar um fluxo de trabalho por interface gráfica, com ao menos uma regra de decisão, sem programação. (Obrigatório. Critério objetivo de aprovação: fluxo criado e executado durante a sessão, com a regra de decisão produzindo encaminhamentos distintos conforme a resposta informada.)                                                 |         |
| 5  | Inventário (ROPA)         | Registrar um processo de tratamento no inventário, associando finalidade, base legal e dados tratados, e gerar o respectivo registro. (Obrigatório. Critério objetivo de aprovação: registro gravado e relatório emitido contendo os três elementos.)                                                                                      |         |
| 6  | Relatórios de privacidade | Gerar um Relatório de Impacto à Proteção de Dados a partir dos dados inventariados. (Obrigatório. Critério objetivo de aprovação: relatório emitido pela solução, em arquivo, referenciando a operação de tratamento registrada no procedimento anterior.)                                                                                 |         |
| 7  | Incidentes                | Registrar um incidente de segurança simulado, preenchendo atores envolvidos, natureza da violação e anexando uma evidência. (Obrigatório. Critério objetivo de aprovação: incidente gravado com os três elementos e evidência anexada recuperável na própria solução.)                                                                     |         |
| 8  | Incidentes / ANPD         | Gerar, a partir do incidente registrado, o formulário de comunicação de incidente à ANPD. (Obrigatório. Critério objetivo de aprovação: formulário gerado pela solução e preenchido com os dados do incidente registrado no procedimento anterior.)                                                                                        |         |

| ID | Grupo / Tema                        | Procedimento de teste a ser demonstrado pela licitante                                                                                                                                                                                                                                                                                                 | Atende? |
|----|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 9  | Terceiros                           | Enviar um questionário de avaliação a um fornecedor e demonstrar o portal em que ele apresentará as respostas. (Obrigatório. Critério objetivo de aprovação: questionário enviado e portal acessado com o questionário disponível para resposta.)                                                                                                      |         |
| 10 | Riscos à privacidade                | Cadastrar um risco de privacidade, classificá-lo por impacto e probabilidade e registrar um plano de ação associado. (Obrigatório. Critério objetivo de aprovação: risco gravado com classificação e plano de ação vinculado, contendo prazo e responsável.)                                                                                           |         |
| 11 | Cookies                             | Executar ou exibir o resultado de uma varredura em uma URL, identificando e classificando os cookies encontrados, e demonstrar a configuração de um banner com suporte a múltiplos idiomas. (Obrigatório. Critério objetivo de aprovação: relação de cookies apresentada com a respectiva classificação e banner exibido em, no mínimo, dois idiomas.) |         |
| 12 | Titulares                           | Acessar o Portal do Titular e abrir uma solicitação de direito, demonstrando o recebimento no painel administrativo. (Obrigatório. Critério objetivo de aprovação: solicitação registrada com protocolo e visível no painel administrativo com prazo em contagem.)                                                                                     |         |
| 13 | Descoberta – bases estruturadas     | Configurar uma conexão com uma fonte de dados estruturada e executar a varredura para catalogação dos dados. (Obrigatório. Critério objetivo de aprovação: conexão estabelecida e catálogo apresentado com os objetos identificados na fonte.)                                                                                                         |         |
| 14 | Descoberta – bases não estruturadas | Configurar uma conexão com um repositório de arquivos e executar a varredura, com apoio de reconhecimento óptico de caracteres. (Obrigatório. Critério objetivo de aprovação: varredura concluída e apresentação de, no mínimo, um dado pessoal identificado em arquivo digitalizado ou de imagem.)                                                    |         |
| 15 | Classificação de dados              | Exibir dados descobertos automaticamente classificados com etiquetas, com base em regras configuráveis. (Obrigatório. Critério objetivo de aprovação: registros apresentados com etiqueta atribuída automaticamente, conforme regra exibida durante a sessão.)                                                                                         |         |
| 16 | Busca assistida                     | Realizar uma busca de dado pessoal e verificar o retorno das fontes em que o dado reside. (Obrigatório. Critério objetivo de aprovação: retorno da consulta indicando a fonte e o objeto em que o dado foi localizado.)                                                                                                                                |         |
| 17 | Integração titular x descoberta     | Demonstrar que, a partir de uma solicitação de titular, a solução se integra ao componente de descoberta para localizar os dados pessoais do solicitante nas fontes cadastradas. (Obrigatório. Critério objetivo de aprovação: solicitação vinculada ao resultado da descoberta, com apresentação das fontes localizadas.)                             |         |
| 18 | Planos de ação e conformidade       | Demonstrar o acompanhamento centralizado de planos de ação, com prazos, responsáveis e status, e a emissão de relatório do grau de atendimento aos requisitos legais aplicáveis. (Obrigatório. Critério objetivo de aprovação: painel de planos de ação apresentado com os três campos e relatório de conformidade emitido pela solução.)              |         |



- 1.15. Apenas os membros da Comissão de Avaliação e os técnicos designados pela Administração poderão solicitar informações ou esclarecimentos adicionais à equipe do licitante proponente durante a realização da POC.
- 1.16. Eventuais observações ou desconformidades técnicas notadas pelos demais licitantes deverão ser registradas em sede de recurso administrativo, conforme prazos legais.

## ANEXO VII

**CARTA DE APRESENTAÇÃO DE PROPOSTA**

Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação n. .... / ..... Objeto: .....

Prezados senhores,

A ..... inscrita no CNPJ sob o n. ...., sediada  
(endereço  
completo)....., com o telefone para contato n. (.....) ..... e e-mail  
....., por intermédio do seu representante legal o(a) Sr.(a)  
.....,  
.....(cargo)....., portador(a) da Carteira de Identidade n. .... e do CPF n.  
....., residente e domiciliado(a) no .....(endereço completo)....., tendo  
examinado as condições do Edital e dos Anexos que o integram, apresenta a proposta comercial  
relativa à licitação em epígrafe, assumindo inteira responsabilidade por quaisquer erros ou  
omissões que tiverem sido cometidos quando da preparação da mesma:

1. Propõe-se o Valor Total de R\$ .....(.....), para o fornecimento dos  
serviços  
objeto desta licitação.

| ITEM | DESCRIÇÃO                                                                                                                                                                           | UNIDADE | QTD. | Valor Unitário | Valor Anual | Valor Global |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|----------------|-------------|--------------|
| 1    | Subscrição corporativa de solução tecnológica para apoio à governança, gestão, monitoramento e conformidade em privacidade e proteção de dados pessoais.                            | Mês     | 60   |                |             |              |
| 2    | Subscrição corporativa de solução para identificação, mapeamento, inventário, classificação e monitoramento de dados pessoais e sensíveis em bases estruturadas e não estruturadas. | Mês     | 60   |                |             |              |
| 3    | Serviços de implantação da solução                                                                                                                                                  | Serviço | 1    |                |             |              |
| 4    | Transferência de conhecimento (capacitação de administradores e usuários, materiais de apoio, manuais, documentação das parametrizações e repasse formal das configurações)         | Serviço | 1    |                |             |              |

| ITEM | DESCRIÇÃO                                                                                             | UNIDADE | QTD. | Valor Unitário | Valor Anual | Valor Global |
|------|-------------------------------------------------------------------------------------------------------|---------|------|----------------|-------------|--------------|
| 5    | Serviços continuados de suporte técnico, manutenção, operação assistida e sustentação (24x7)          | Mês     | 60   |                |             |              |
| 6    | Serviços técnicos especializados em Privacidade e Proteção de Dados, sob demanda (itens de catálogo)* | Entrega | 290  |                |             |              |
| 7    | Saldo de horas técnicas especializadas, sob demanda, para demandas supervenientes não catalogadas     | Hora    | 320  |                |             |              |

Deverão ser descritos os valores do item 6-Serviços técnicos especializados em Privacidade e Proteção de Dados (itens de catálogo).

| Cód.  | Serviço                                                                                    | Qtd./ano | Qtd./60 meses | Valor Unitário | Valor Ano | Valor Global |
|-------|--------------------------------------------------------------------------------------------|----------|---------------|----------------|-----------|--------------|
| CS-01 | Elaboração ou revisão de instrumento normativo de privacidade                              | 4        | 20            |                |           |              |
| CS-02 | Diagnóstico do programa de privacidade e plano de evolução                                 | 1        | 5             |                |           |              |
| CS-03 | Análise e registro de operação de tratamento no inventário (ROPA)                          | 10       | 50            |                |           |              |
| CS-04 | Revisão integral do inventário de macroprocesso                                            | 2        | 10            |                |           |              |
| CS-05 | Elaboração de Relatório de Impacto à Proteção de Dados                                     | 4        | 20            |                |           |              |
| CS-06 | Avaliação de riscos de privacidade e plano de tratamento                                   | 3        | 15            |                |           |              |
| CS-07 | Avaliação de privacidade desde a concepção                                                 | 6        | 30            |                |           |              |
| CS-08 | Apoio técnico à análise, contenção, documentação e comunicação de incidente de privacidade | 6        | 30            |                |           |              |
| CS-09 | Apoio técnico ao atendimento de solicitação de titular de alta complexidade                | 10       | 50            |                |           |              |
| CS-10 | Avaliação de privacidade de operador, suboperador ou terceiro                              | 4        | 20            |                |           |              |
| CS-11 | Análise de impacto de ato normativo superveniente e plano de adequação                     | 3        | 15            |                |           |              |
| CS-12 | Integração da solução com sistema ou fonte de dados não prevista na implantação            | 2        | 10            |                |           |              |
| CS-13 | Capacitação técnica complementar sobre a solução ou sobre processos de privacidade         | 3        | 15            |                |           |              |
|       |                                                                                            | 58       | 290           |                |           |              |



No valor total proposto estão englobados todos os custos e despesas previstos no Edital n ...../....., tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucro, uniformes, alimentação, transporte, plano de assistência médico-hospitalar e odontológica e outros necessários ao cumprimento integral do objeto.

Junta-se detalhamento da proposta.

Que, em relação às prerrogativas da Lei Complementar n. 123/2016, o proponente:

( ) Enquadra-se como microempresa, empresa de pequeno porte ou equivalente legal, nos termos previsto no Decreto n. 8.538/2015, conforme certidão expedida pela Junta Comercial ou Cartório de Registro em anexo. Ainda, que:

( ) É optante do Simples Nacional, submetendo-se à alíquota de %, apurada com base no faturamento acumulado dos últimos 12 meses. ( ) Não é optante do Simples Nacional.

( ) Não se enquadra na condição de microempresa, empresa de pequeno porte ou equivalente legal.

Essa proposta é válida por 90 (noventa) dias, contados da data prevista para abertura dos envelopes.

Até que o contrato seja assinado, esta proposta constituirá um compromisso da, observadas as condições do Edital. Caso esta proposta não venha a ser aceita para contratação, O Banco da Amazônia fica desobrigada de qualquer responsabilidade referente à presente proposta.

Os pagamentos serão efetuados em conformidade com as condições estabelecidas na Minuta do Contrato.

Devem ser utilizados, para quaisquer pagamentos, os dados bancários a seguir: BANCO:

.....

AGÊNCIA: .....

CONTA CORRENTE: .....

PRAÇA DE PAGAMENTO: .....

Por fim, declara conhecer e aceitar as condições constantes do Edital n. .... e de seus Anexos.

.....  
(Local e Data)

.....  
(representante legal)

**ANEXO VIII****Catálogo de Serviços Técnicos Especializados Privacidade e Proteção de Dados Pessoais****1. Finalidade e estrutura**

Este catálogo define os serviços técnicos especializados em privacidade e proteção de dados pessoais passíveis de acionamento sob demanda durante a vigência contratual. Para cada serviço são definidos o macrotema, o escopo, os entregáveis, os critérios de aceite, o perfil profissional exigido, a faixa de complexidade, o prazo de entrega e o quantitativo anual estimado.

Os serviços são remunerados por entrega aceita, e não por tempo empregado. A remuneração por entrega decorre de os produtos de cada serviço serem previamente identificáveis e verificáveis, em observância à Súmula TCU nº 269, ao art. 26, item 2, do Regulamento de Licitações e Contratos do Banco da Amazônia e ao art. 3º, inciso III, da Resolução CGPAR nº 45/2022.

O quantitativo estimado constitui limite máximo, não gera direito subjetivo à execução integral e não impõe consumo mínimo. Demandas supervenientes que não se enquadrem em nenhum dos serviços catalogados são atendidas pelo saldo de horas técnicas especializadas, de acionamento subsidiário e excepcional, tratado na seção 5.

**2. Quadro-resumo do catálogo de serviços**

| Cód.  | Macrotema                             | Serviço                                                                                    | Compl ex. | Qtd./ano | Qtd./60 meses |
|-------|---------------------------------------|--------------------------------------------------------------------------------------------|-----------|----------|---------------|
| CS-01 | Governança de Privacidade             | Elaboração ou revisão de instrumento normativo de privacidade                              | Média     | 4        | 20            |
| CS-02 | Evolução da maturidade em privacidade | Diagnóstico do programa de privacidade e plano de evolução                                 | Alta      | 1        | 5             |
| CS-03 | Inventário e Mapeamento de Dados      | Análise e registro de operação de tratamento no inventário (ROPA)                          | Baixa     | 10       | 50            |
| CS-04 | Inventário e Mapeamento de Dados      | Revisão integral do inventário de macroprocesso                                            | Alta      | 2        | 10            |
| CS-05 | RIPD / DPIA                           | Elaboração de Relatório de Impacto à Proteção de Dados                                     | Alta      | 4        | 20            |
| CS-06 | Gestão de Riscos de Privacidade       | Avaliação de riscos de privacidade e plano de tratamento                                   | Média     | 3        | 15            |
| CS-07 | Privacy by Design                     | Avaliação de privacidade desde a concepção                                                 | Média     | 6        | 30            |
| CS-08 | Gestão de Incidentes                  | Apoio técnico à análise, contenção, documentação e comunicação de incidente de privacidade | Média     | 6        | 30            |
| CS-09 | Atendimento aos Titulares             | Apoio técnico ao atendimento de solicitação de titular de alta complexidade                | Baixa     | 10       | 50            |
| CS-10 | Gestão de Terceiros                   | Avaliação de privacidade de operador, suboperador ou terceiro                              | Média     | 4        | 20            |
| CS-11 | Adequação normativa                   | Análise de impacto de ato normativo superveniente e plano de adequação                     | Média     | 3        | 15            |
| CS-12 | Apoio técnico especializado           | Integração da solução com sistema ou fonte de dados não prevista na implantação            | Alta      | 2        | 10            |

|       |                                |                                                                                    |       |    |     |
|-------|--------------------------------|------------------------------------------------------------------------------------|-------|----|-----|
| CS-13 | Treinamentos e Conscientização | Capacitação técnica complementar sobre a solução ou sobre processos de privacidade | Média | 3  | 15  |
|       | TOTAL                          |                                                                                    |       | 58 | 290 |

Agrupamento por faixa de complexidade, para fins de composição da proposta e de medição:

| Faixa | Serviços                                        | Entregas/ano | Entregas em 60 meses |
|-------|-------------------------------------------------|--------------|----------------------|
| Baixa | CS-03, CS-09                                    | 20           | 100                  |
| Média | CS-01, CS-06, CS-07, CS-08, CS-10, CS-11, CS-13 | 29           | 145                  |
| Alta  | CS-02, CS-04, CS-05, CS-12                      | 9            | 45                   |
| Total | —                                               | 58           | 290                  |

### 3. Faixas de complexidade

| Faixa | Critério objetivo de enquadramento                                                                                                    | Esforço de referência      | Prazo de entrega |
|-------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------|------------------|
| Baixa | Entrega que recai sobre uma única operação de tratamento, solicitação ou fornecedor, com um único produto.                            | Até 8 horas                | 5 dias úteis     |
| Média | Entrega que envolve mais de uma unidade organizacional ou até 3 produtos.                                                             | Acima de 8 e até 24 horas  | 10 dias úteis    |
| Alta  | Entrega que envolve múltiplas unidades ou sistemas, produto submetido a instância de governança ou revisão integral de macroprocesso. | Acima de 24 e até 60 horas | 20 dias úteis    |

### 4. Descrição dos serviços

#### CS-01 — Elaboração ou revisão de instrumento normativo de privacidade

*Macrotema: Governança de Privacidade · Faixa de complexidade: Média · Prazo: 10 dias úteis · Quantitativo estimado: 4 por ano (20 em 60 meses)*

**Escopo.** Elaboração ou revisão de política, norma, procedimento ou fluxo institucional relativo à privacidade e à proteção de dados pessoais, a partir de diagnóstico do texto vigente, da legislação e da regulamentação aplicáveis e das práticas já adotadas pelo Banco.

**Entregáveis.** Minuta do instrumento normativo; quadro comparativo entre a versão vigente e a proposta, com a motivação de cada alteração; registro e versionamento do documento na solução, com associação aos controles e às áreas responsáveis.

**Crítérios de aceite.** A minuta contempla todos os pontos indicados na Ordem de Serviço; cita expressamente os dispositivos legais e regulatórios aplicáveis; é compatível com os normativos internos vigentes; e está registrada e versionada na solução.

**Perfil profissional.** Profissional com formação superior e experiência comprovada em privacidade e proteção de dados ou em governança corporativa.

#### CS-02 — Diagnóstico do programa de privacidade e plano de evolução

*Macrotema: Evolução da maturidade em privacidade · Faixa de complexidade: Alta · Prazo: 20 dias úteis · Quantitativo estimado: 1 por ano (5 em 60 meses)*



Escopo. Avaliação do grau de atendimento do programa institucional de privacidade aos requisitos legais e regulatórios aplicáveis, a partir das evidências mantidas na solução, com identificação de lacunas e proposição de plano de evolução.

Entregáveis. Relatório de diagnóstico, com o grau de atendimento por requisito e as lacunas identificadas; plano de evolução com ações, prazos, responsáveis e prioridades; registro das ações na solução.

Critérios de aceite. O diagnóstico cobre todos os requisitos definidos na Ordem de Serviço; cada lacuna está associada a evidência verificável na solução; e o plano de evolução contém ação, prazo e responsável para cada lacuna.

Perfil profissional. Profissional com formação superior e experiência comprovada em programas de privacidade e proteção de dados.

### **CS-03 — Análise e registro de operação de tratamento no inventário (ROPA)**

*Macrotema: Inventário e Mapeamento de Dados · Faixa de complexidade: Baixa · Prazo: 5 dias úteis · Quantitativo estimado: 10 por ano (50 em 60 meses)*

Escopo. Levantamento junto à área gestora, análise e registro de uma operação de tratamento de dados pessoais no inventário mantido na solução, com identificação de finalidade, base legal, categorias de dados e de titulares, ciclo de vida, compartilhamentos, operadores envolvidos e riscos associados.

Entregáveis. Operação registrada no inventário da solução, com todos os campos preenchidos; relação dos riscos identificados; indicação das evidências coletadas.

Critérios de aceite. A operação está registrada e recuperável na solução; a base legal indicada está fundamentada; e a ficha não apresenta campos obrigatórios em branco.

Perfil profissional. Profissional com formação superior e experiência comprovada em mapeamento de operações de tratamento.

### **CS-04 — Revisão integral do inventário de macroprocesso**

*Macrotema: Inventário e Mapeamento de Dados · Faixa de complexidade: Alta · Prazo: 20 dias úteis · Quantitativo estimado: 2 por ano (10 em 60 meses)*

Escopo. Revisão de todas as operações de tratamento vinculadas a um macroprocesso do Banco, com validação junto às áreas gestoras, atualização dos registros e identificação de operações não inventariadas.

Entregáveis. Inventário do macroprocesso revisado e atualizado na solução; relatório de lacunas, com as operações não inventariadas identificadas; plano de correção com prazos e responsáveis.

Critérios de aceite. Todas as operações do macroprocesso indicadas na Ordem de Serviço foram revisadas; as alterações estão registradas na solução com trilha de auditoria; e o relatório de lacunas indica a área responsável por cada pendência.

Perfil profissional. Profissional com formação superior e experiência comprovada em mapeamento e governança de dados.

### **CS-05 — Elaboração de Relatório de Impacto à Proteção de Dados**

*Macrotema: RIPD / DPIA · Faixa de complexidade: Alta · Prazo: 20 dias úteis · Quantitativo estimado: 4 por ano (20 em 60 meses)*

Escopo. Elaboração de relatório de impacto à proteção de dados pessoais relativo a operação, produto, serviço ou sistema indicado pelo Banco, contemplando descrição das operações, necessidade e proporcionalidade, riscos aos titulares, salvaguardas e conclusão.

Entregáveis. RIPD emitido na solução, com identificação dos riscos, avaliação de necessidade e proporcionalidade, medidas mitigadoras e conclusão; plano de ação das medidas pendentes.



Critérios de aceite. O relatório atende à estrutura definida no art. 38 da Lei nº 13.709/2018 e às orientações da ANPD; está vinculado às operações de tratamento correspondentes no inventário; e cada risco possui medida mitigadora associada.

Perfil profissional. Profissional com formação superior e experiência comprovada em avaliação de impacto à proteção de dados.

#### **CS-06 — Avaliação de riscos de privacidade e plano de tratamento**

*Macrotema: Gestão de Riscos de Privacidade · Faixa de complexidade: Média · Prazo: 10 dias úteis · Quantitativo estimado: 3 por ano (15 em 60 meses)*

Escopo. Identificação, análise e avaliação de riscos de privacidade associados a operação, área ou processo indicado pelo Banco, com definição de controles e plano de tratamento. Inclui, quando aplicável, a avaliação de legítimo interesse.

Entregáveis. Avaliação de riscos registrada na solução, com probabilidade, impacto e nível inerente; plano de tratamento com controles, prazos e responsáveis; avaliação de legítimo interesse, quando aplicável.

Critérios de aceite. Os riscos estão registrados na solução e associados às operações de tratamento correspondentes; cada risco de nível alto ou crítico possui controle e responsável definidos.

Perfil profissional. Profissional com formação superior e experiência comprovada em gestão de riscos de privacidade.

#### **CS-07 — Avaliação de privacidade desde a concepção**

*Macrotema: Privacy by Design · Faixa de complexidade: Média · Prazo: 10 dias úteis · Quantitativo estimado: 6 por ano (30 em 60 meses)*

Escopo. Avaliação de privacidade desde a concepção de novo produto, serviço, processo ou sistema, inclusive os que envolvam tratamentos automatizados, com identificação dos requisitos de privacidade a serem observados antes da entrada em produção.

Entregáveis. Parecer técnico de privacidade por concepção, com os requisitos aplicáveis e as recomendações; registro da avaliação e do respectivo fluxo de aprovação na solução.

Critérios de aceite. O parecer identifica as operações de tratamento previstas, as bases legais aplicáveis e os requisitos de privacidade; cada recomendação possui responsável e prazo; e a avaliação está registrada na solução.

Perfil profissional. Profissional com formação superior e experiência comprovada em privacidade desde a concepção.

#### **CS-08 — Apoio técnico à análise, contenção, documentação e comunicação de incidente de privacidade**

*Macrotema: Gestão de Incidentes · Faixa de complexidade: Média · Prazo: Acionamento imediato; entrega em 5 dias úteis contados da conclusão da contenção · Quantitativo estimado: 6 por ano (30 em 60 meses)*

Escopo. Apoio técnico especializado ao Banco na análise de incidente de privacidade, incluindo caracterização do evento, delimitação do escopo, identificação dos dados e titulares afetados, avaliação do risco aos titulares e elaboração das comunicações devidas.

Entregáveis. Incidente registrado na solução com todos os campos preenchidos; relatório de análise com escopo, causa, dados e titulares afetados e avaliação de risco; minutas da comunicação à ANPD e aos titulares; plano de ação das medidas corretivas.

Critérios de aceite. O relatório permite ao Banco decidir sobre a comunicação, com fundamentação da avaliação de risco; as minutas atendem ao formato exigido pela ANPD; e as medidas corretivas estão registradas na solução com prazo e responsável.



Perfil profissional. Profissional com formação superior e experiência comprovada em resposta a incidentes de privacidade ou de segurança da informação.

### **CS-09 — Apoio técnico ao atendimento de solicitação de titular de alta complexidade**

*Macrotema: Atendimento aos Titulares · Faixa de complexidade: Baixa · Prazo: 5 dias úteis · Quantitativo estimado: 10 por ano (50 em 60 meses)*

Escopo. Apoio técnico ao atendimento de solicitação de titular que envolva múltiplas fontes de dados, dados de terceiros, decisões automatizadas, controvérsia sobre a base legal aplicável ou risco de negativa fundamentada.

Entregáveis. Resposta técnica fundamentada, com indicação da base legal e dos limites do atendimento; evidências da localização e do tratamento dos dados do titular nas fontes cadastradas; registro do atendimento na solução.

Critérios de aceite. A resposta está fundamentada em dispositivo legal expresso; as evidências permitem reconstituir a busca realizada; e o atendimento está registrado na solução dentro do prazo legal.

Perfil profissional. Profissional com formação superior e experiência comprovada em atendimento a direitos de titulares.

### **CS-10 — Avaliação de privacidade de operador, suboperador ou terceiro**

*Macrotema: Gestão de Terceiros · Faixa de complexidade: Média · Prazo: 10 dias úteis · Quantitativo estimado: 4 por ano (20 em 60 meses)*

Escopo. Avaliação de conformidade em privacidade de operador, suboperador ou terceiro que trate dados pessoais por conta do Banco, a partir de questionário, evidências documentais e análise das cláusulas contratuais de proteção de dados.

Entregáveis. Relatório de avaliação com riscos identificados, percentual de adequação e plano de ação; recomendações de cláusulas contratuais; registro da avaliação na solução.

Critérios de aceite. A avaliação cobre os itens definidos na Ordem de Serviço; cada risco possui classificação e recomendação; e o resultado está registrado na solução e associado ao fornecedor.

Perfil profissional. Profissional com formação superior e experiência comprovada em gestão de riscos de terceiros em privacidade.

### **CS-11 — Análise de impacto de ato normativo superveniente e plano de adequação**

*Macrotema: Adequação normativa · Faixa de complexidade: Média · Prazo: 10 dias úteis · Quantitativo estimado: 3 por ano (15 em 60 meses)*

Escopo. Análise de ato normativo, regulamento, resolução, guia orientativo ou decisão superveniente com impacto sobre o programa de privacidade do Banco, com identificação das obrigações novas ou alteradas e das providências necessárias.

Entregáveis. Nota técnica de impacto, com as obrigações identificadas e os processos, sistemas e instrumentos normativos afetados; plano de adequação com ações, prazos e responsáveis; registro na solução.

Critérios de aceite. A nota técnica indica expressamente os dispositivos analisados e os processos afetados; o plano de adequação contém ação, prazo e responsável para cada obrigação identificada.

Perfil profissional. Profissional com formação superior e experiência comprovada em conformidade regulatória em privacidade.

### **CS-12 — Integração da solução com sistema ou fonte de dados não prevista na implantação**

*Macrotema: Apoio técnico especializado · Faixa de complexidade: Alta · Prazo: 20 dias úteis · Quantitativo estimado: 2 por ano (10 em 60 meses)*



Escopo. Especificação, configuração, teste, homologação e documentação de integração entre a solução e sistema ou fonte de dados do Banco não contemplada no escopo da implantação, observados os requisitos de segurança e governança de dados.

Entregáveis. Integração configurada, testada e homologada; documentação técnica da integração, incluindo mapeamento de campos, credenciais utilizadas, tratamento de erros e procedimento de reprocessamento; registro dos testes.

Critérios de aceite. A integração opera em ambiente de produção pelo período de estabilização definido na Ordem de Serviço; a documentação permite a sua reconstituição pela equipe do Banco; e os testes estão evidenciados.

Perfil profissional. Profissional com formação superior e experiência comprovada em integração de sistemas.

### **CS-13 — Capacitação técnica complementar sobre a solução ou sobre processos de privacidade**

*Macrotema: Treinamentos e Conscientização · Faixa de complexidade: Média · Prazo: Conforme cronograma pactuado na Ordem de Serviço · Quantitativo estimado: 3 por ano (15 em 60 meses)*

Escopo. Realização de turma de capacitação técnica complementar, presencial ou remota, sobre funcionalidades da solução ou sobre processos institucionais de privacidade, com conteúdo ajustado ao público-alvo indicado pelo Banco.

Entregáveis. Turma realizada, com carga horária mínima de 8 (oito) horas; material didático; lista de presença; avaliação de aproveitamento; gravação da sessão, quando remota.

Critérios de aceite. A turma foi realizada na data e com a carga horária pactuadas; o material foi entregue ao Banco sem restrição de uso interno; e a avaliação de aproveitamento foi aplicada.

Perfil profissional. Profissional com formação superior, experiência comprovada na matéria e experiência em capacitação.

## **5. Saldo de horas técnicas especializadas**

O saldo de horas técnicas destina-se exclusivamente ao atendimento de demandas supervenientes relacionadas à privacidade e à proteção de dados pessoais que não se enquadrem em nenhum dos serviços catalogados. Corresponde a 64 (sessenta e quatro) horas por ano de vigência, totalizando 320 (trezentas e vinte) horas, quantitativo equivalente ao da reserva técnica anteriormente prevista.

Regras de acionamento e comprovação:

Solicitação formal da área demandante, com descrição do resultado pretendido.

Manifestação técnica do gestor do contrato atestando a inexistência de serviço catalogado equivalente e a ausência de sobreposição com os serviços de implantação, de transferência de conhecimento e de suporte e sustentação.

Apresentação, pela contratada, de proposta técnica com escopo, produtos, cronograma, perfis profissionais e estimativa de horas.

Autorização prévia mediante Ordem de Serviço, que fixará o teto de horas e os critérios de aceite.

Registro diário das horas efetivamente utilizadas, por profissional e por atividade.

Apresentação de relatório de execução com evidências dos produtos.

Aceite formal do contratante, que poderá glosar horas não comprovadas ou não aderentes ao escopo autorizado.

Faturamento exclusivamente das horas autorizadas, executadas, comprovadas e aceitas.

Vedações. O saldo de horas não poderá ser utilizado para a execução de serviços catalogados, para atividades compreendidas nos serviços de implantação, de transferência de conhecimento ou de suporte e sustentação, nem para o atendimento de obrigações já remuneradas na subscrição.

Controle. O gestor do contrato manterá controle do saldo remanescente, com registro de cada autorização, execução e aceite, disponibilizado à fiscalização e à auditoria interna e externa.

**6. Níveis mínimos de serviço aplicáveis**

| Indicador | Objeto                                                                             | Valor de referência                                                |
|-----------|------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| NMS-21    | Prazo de entrega dos serviços técnicos especializados, contado da Ordem de Serviço | 5 dias úteis (baixa), 10 dias úteis (média) e 20 dias úteis (alta) |
| NMS-22    | Índice de aceite das entregas na primeira apresentação                             | Mínimo de 90% das entregas apuradas no trimestre                   |
| NMS-23    | Prazo para correção de entrega devolvida de forma motivada                         | 5 dias úteis contados da devolução                                 |

O descumprimento do NMS-21 sujeita a contratada a desconto de 2% do valor da entrega por dia útil de atraso, limitado a 20% do valor da entrega. O descumprimento do NMS-22, apurado trimestralmente, sujeita a contratada a desconto de 5% sobre o valor das entregas aceitas no trimestre. Os descontos constituem adequação do pagamento ao serviço efetivamente prestado e não se confundem com as sanções administrativas.

