

CONTRATO DE FORNECIMENTO DE 4.083 LICENÇAS DA SOLUÇÃO DE IGA E 1000 USTS DE SERVIÇOS TÉCNICOS ESPECIALIZADOS, CONTEMPLANDO IMPLANTAÇÃO, TREINAMENTO E SUPORTE DE SOLUÇÃO DE GOVERNANÇA E ADMINISTRAÇÃO DE IDENTIDADE (IGA), QUE ENTRE SI FAZEM O BANCO DA AMAZÔNIA S.A. E A EMPRESA QOS TECNOLOGIA E SERVIÇOS LTDA.

Por este instrumento particular de Contrato, em que são Partes, de um lado o Banco da Amazônia S.A., sociedade de economia mista, vinculado ao Governo Federal, com sede em Belém (PA), na Avenida Presidente Vargas, nº 800, Bairro Campina, inscrito no CNPJ/MF sob o nº 04.902.979/0001-44, representado neste ato por seu Diretor Corporativo - DICOP, Sr. **DIEGO SANTOS LIMA**, brasileiro, casado, graduado em administração de empresas, portador do RG nº 075403072021-5 SSP/MA e do CPF/MF nº 011.772.821-78, residente e domiciliado na Região Metropolitana de Belém/PA, doravante denominado **CONTRATANTE**, e de outro lado a empresa **QOS TECNOLOGIA E SERVIÇOS LTDA**, com registro na Junta Comercial do Estado de Pernambuco sob o NIRE nº 26201347140, com sede na Cidade de Recife/PE, situada na Avenida Rio Branco, nº 243, Edifício São Paulo, Sala 401, CEP: 50.030-310, inscrita no CNPJ/MF nº 05.012.577/0001-37, representada neste ato por seu Sócio Administrador Sr. **WALTER FERNANDES PINTO NETO**, brasileira, casado, empresário, portador da CNH nº 01339104606 DETRAN/PE e do CPF/MF nº 025.596.954-64, doravante denominada **CONTRATADA**, por este instrumento e na melhor forma de direito, nos termos da decisão da Diretoria Executiva- DIREX do **CONTRATANTE**, datada de 07/07/2025, ajustam o presente Contrato, nos termos do **Edital do Pregão Eletrônico nº 90002/2025**, sujeitando, ainda, as Partes às disposições da Lei nº 13.303 de 30.06.2016, do Decreto nº 8.945/2026 e do Regulamento de Licitações e Contratos do Banco da Amazônia S.A e suas alterações.

1. CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Contrato tem como objeto a contratação de empresa para o fornecimento de **4.083 (quatro mil e oitenta e três) licenças da solução de IGA**, bem como sua **implantação, treinamento, serviço de suporte e operação da solução e 1000 (um mil) USTs de serviços técnicos especializados em governança de identidade**, contemplando os serviços de implantação, treinamento e suporte e operação da solução, conforme diretrizes, condições, quantidades e exigências estabelecidas no **Edital do Pregão Eletrônico nº 90002/2025 e seus anexos** e neste Contrato, pelo período de 36 (trinta e seis) meses renováveis até o prazo legal.

1.2. O presente Contrato decorre do processo de contratação aprovado no **Parecer GECOG-GT CONTRATAÇÕES Nº 2025/001** e realizado pelo **Edital do Pregão Eletrônico nº 90002/2025**.

2. CLÁUSULA SEGUNDA – ANEXOS

2.1. Fazem parte integrante do presente Contrato, como se nele estivessem transcritos, os seguintes Anexos:

Anexo I - Termo de Confidencialidade e Sigilo de Dados de informação

Anexo II - Termo de Política Anticorrupção

Anexo III - Termo de Referência

Anexo IV - Especificações Técnicas dos Serviços

Anexo V - Acordo de Níveis de Serviço

Anexo VI - Prova de Conceito

BANCO DA AMAZÔNIA
CONTRATO Nº 2025/154-01
Anexo VII - Proposta Comercial

2.2. Este Contrato e seus Anexos são considerados como um único termo e suas regras deverão ser interpretados de forma harmônica. Em caso de divergência insuperável entre as regras deste Contrato e os seus Anexos, prevalecerão às regras deste Contrato e, na sequência, na ordem dos Anexos.

3. CLÁUSULA TERCEIRA – PRAZOS

3.1. O prazo para início de execução do objeto desta contratação será na forma contida no **Anexo I – Termo de Referência** deste Contrato e o prazo de vigência deste instrumento contratual são de 36 (trinta e seis) meses, contados a partir da data da assinatura deste Contrato.

4. CLÁUSULA QUARTA – VALOR DO CONTRATO E RECURSOS ORÇAMENTÁRIOS

4.1. Como contrapartida à execução do objeto do presente Contrato, o **CONTRATANTE** deverá pagar à **CONTRATADA** o Valor Global Total de **R\$9.638.292,70** (nove milhões, seiscentos e trinta e oito mil, duzentos e noventa e dois reais e setenta centavos), sendo o valor do serviço de subscrição anual da solução de IGA (**item 01**) de **R\$6.936.608,70** (seis milhões, novecentos e trinta e seis mil, seiscentos e oito reais e setenta centavos), serão distribuídos durante a vigência do Contrato e **pagos anualmente**, o valor do serviço de implantação da solução de IGA (**item 03**), o valor do serviço de capacitação na solução IGA (**item 05**) e o valor de serviços técnicos especializados (**item 06**), perfazendo o valor total de **R\$1.392.140,80** (um milhão, trezentos e noventa e dois mil, cento e quarenta reais e oitenta centavos), serão pagos de **uma única vez** e o valor dos serviços de suporte e operação da solução (**item 04**) de **R\$1.309.543,20** (um milhão, trezentos e nove mil, quinhentos e quarenta e três reais e vinte centavos) serão pagos **mensalmente**, conforme **item 11** do **Termo de Referência – Anexo I** deste Contrato e as especificações do objeto e as demais condições ofertadas, de acordo com a proposta comercial apresentada pela **CONTRATADA**, datada de 07/05/2025, no Pregão Eletrônico nº 90002/2025, conforme abaixo:

Grupo 01					
Item	Descrição	Unidade de Medida	Quantidade	Preço Unitário (R\$)	Preço Total (R\$)
01	Serviço de subscrição anual da solução de IGA	Identidade	4083	1.698,90	6.936.608,70
03	Serviço de implantação da solução de IGA	-	01	1.201.118,00	1.201.118,00
04	Serviço de suporte e operação da solução	Mês	36	36.376,20	1.309.543,20
05	Serviço de capacitação na solução de IGA	Turma	01	30.002,80	30.002,80
06	Serviços técnicos especializados	UST	1000	161,02	161.020,00
VALOR GLOBAL					9.638.292,70

4.1.1. O valor contratado inclui todos os impostos e taxas vigentes na Legislação Brasileira para a execução do objeto desta contratação, e também, todos os custos



diretos e indiretos inerentes, tais como os a seguir indicados, porém sem se limitar aos mesmos: despesas com pessoal (inclusive obrigações sociais, viagens e diárias), despesas administrativas, administração, lucro e outras despesas necessárias a boa realização do objeto desta contratação, isentando o **CONTRATANTE** de quaisquer ônus adicionais.

4.1.2. Os recursos orçamentários para cobrir as despesas decorrentes da execução do objeto deste Contrato estão previstos no orçamento do **CONTRATANTE**, nas rubricas abaixo:

- I. 82.543-3 - Despesas de Segurança - Sxec. Serv. (Implant, Instal) - C/INSS PJ (R\$1.201.118,00);
- II. 82.545-0 – Despesas Segurança Informação – Gestão de Acessos Lógicos (R\$161.020,00);
- III. 82.546-8 - Despesas Segurança Informação - Subscrição de Solução/Software (R\$6.936.608,70);
- IV. 82.547-6 - Despesas Segurança Informação - Suporte Técnico Soluções (R\$1.309.543,20); e
- V. 82.548-4 - Despesas Segurança Informação - Treinam p/Implant - Instrut. Externos S/INSS (R\$30.002,80).

4.1.3. Considerando que o **CONTRATANTE** está submetido às Leis orçamentárias Federais (LDO-LOA), ficam as Partes cientes de que a execução do objeto adstrita a este Contrato estará condicionada às respectivas aprovações orçamentárias.

5. CLÁUSULA QUINTA - GARANTIA

5.1. Para garantia do fiel e perfeito cumprimento de todas as obrigações ora ajustadas, a **CONTRATADA** deve, dentro de 10 (dez) dias úteis, contados a partir da assinatura do Contrato, apresentar garantia ao **CONTRATANTE**, no valor equivalente a 5% (cinco por cento) do valor total desta contratação, que deve cobrir o período de execução do Contrato e estender-se até 03 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação ou renovação contratual e aditivos e apostilas para reajustes.

5.1.1. A **CONTRATADA** deve prestar garantia numa das seguintes modalidades:

a) **Fiança Bancária**, acompanhado dos seguintes documentos a seguir listados, para análise e aceitação por parte do **CONTRATANTE**:

- I - Estatuto Social e ata de posse da diretoria da Instituição Financeira;
- II - Quando Procuradores, encaminhar as procurações devidamente autenticadas, com poderes específicos para representar a Instituição Financeira;
- III - Balanços Patrimoniais e Demonstração de Resultado dos últimos dois anos, acompanhado das notas explicativas e respectivos pareceres do Conselho de Administração e Auditores Independentes;
- IV - Memória de cálculo do Índice de Adequação de Capital (Índice da Basileia) e Índice de Imobilização, comprovando que a instituição financeira está enquadrada no limite estabelecido pelo Banco Central, para comparação e validação com os dados disponíveis no "site" do Banco Central do Brasil (www.bcb.gov.br).

b) **Caução em dinheiro** deve ser efetuada junto a uma Agência do **CONTRATANTE**, em que o depósito tenha como beneficiário o **CONTRATANTE**, sendo a cópia do recibo será entregue ao Gestor do Contrato.

c) **Seguro Garantia** feito junto à entidade com situação regular no mercado de seguros do Brasil, nos termos estipulados neste Contrato, para análise e aceitação por parte do **CONTRATANTE**.



CONTRATO Nº 2025/154-01

5.1.2.A garantia, qualquer que seja a modalidade escolhida, deve assegurar o pagamento de:

- a) Prejuízos advindos do não cumprimento ou do cumprimento irregular do objeto do presente Contrato;
- b) Prejuízos diretos causados ao **CONTRATANTE** decorrentes de culpa ou dolo durante a execução do Contrato;
- c) Multas moratórias e compensatórias aplicadas pelo **CONTRATANTE** à **CONTRATADA**; e
- d) Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber.

5.2. A inobservância do prazo fixado nesta Cláusula para apresentação da garantia acarreta a aplicação de multa de 0,1% (um centésimo por cento) sobre o valor total do Contrato, por dia de atraso, limitada a 2,5% (dois vírgula cinco por cento) sobre o valor total do Contrato.

5.2.1.O atraso superior a 25 (vinte e cinco) dias para a apresentação da garantia autoriza o **CONTRATANTE** a:

- a) Promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas obrigações; ou
- b) Reter o valor da garantia dos pagamentos eventualmente devidos à **CONTRATADA** até que a garantia seja apresentada.

5.3. A garantia deve ser considerada extinta:

- a) Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do **CONTRATANTE**, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as Cláusulas do Contrato; ou
- b) Após 03 (três) meses do término da vigência do presente Contrato.

6. CLÁUSULA SEXTA – EXECUÇÃO DO CONTRATO

6.1. O objeto deverá ser fornecido rigorosamente conforme estabelecido neste Contrato e no **Termo de Referência - Anexo III** deste Contrato, e no **Edital do Pregão Eletrônico nº 90002/2025** e seus Anexos e nas especificações neles contidas, sendo que a inobservância de qualquer condição poderá acarretar a não aceitação dos mesmos, sem qualquer ônus para o **CONTRATANTE**.

6.1.1.A **CONTRATADA** deverá fornecer os serviços, especificados no objeto deste Contrato, cumprindo todas as obrigações e responsabilidades a si indicadas no **Termo de Referência - Anexo III** deste Contrato.

6.1.2. O **CONTRATANTE** deverá acompanhar e assegurar as condições necessárias para o fornecimento dos bens, cumprindo rigorosamente todas as obrigações e responsabilidades a si indicadas no **Termo de Referência - Anexo III** deste Contrato.

6.2. A **CONTRATADA** é responsável pelos danos causados direta ou indiretamente ao **CONTRATANTE** ou a terceiros em razão da execução do Contrato, não excluindo ou reduzindo essa responsabilidade a Fiscalização ou o acompanhamento pelo **CONTRATANTE**.

6.3. A Gestão e Fiscalização do presente Contrato deve ser realizada pela área técnica do **CONTRATANTE**. A Gestão do Contrato abrange o encaminhamento de providências, devidamente instruídas e motivadas, identificadas em razão da Fiscalização da execução do Contrato, suas alterações, aplicação de sanções, rescisão contratual e outras medidas que importem disposição sobre o Contrato.



6.4. A Fiscalização da execução do presente Contrato será realizada por Agentes de Fiscalização, que devem ser designados pelo Gestor do Contrato, permitindo-se designar mais de 01 (um) empregado e atribuir-lhes funções distintas, como a Fiscalização administrativa e técnica, consistindo na verificação do cumprimento das obrigações contratuais por parte da **CONTRATADA**, com a alocação dos recursos, pessoal qualificado, técnicas e materiais necessários.

6.5. O Gestor do Contrato pode suspender a sua execução em casos excepcionais e motivados tecnicamente pelo Fiscal Técnico do Contrato, devendo comunicá-la ao Preposto da **CONTRATADA**, indicando:

- a) O prazo da suspensão, que pode ser prorrogado, se as razões que a motivaram não estão sujeitas ao controle ou à vontade do Gestor do Contrato;
- b) Se deve ou não haver desmobilização, total ou parcial, e quais as atividades devem ser mantidas pela **CONTRATADA**;
- c) O montante que deve ser pago à **CONTRATADA** a título de indenização em relação a eventuais danos já identificados e o procedimento e metodologia para apurar valor de indenização de novos danos que podem ser gerados à **CONTRATADA**.

6.6. Constatada qualquer irregularidade na licitação ou na execução contratual, o Gestor do Contrato deve, se possível, sanear a situação, evitando-se a suspensão da execução do Contrato ou outra medida como decretação de nulidade ou rescisão contratual.

6.6.1. Na hipótese prevista neste subitem, a **CONTRATADA** deve submeter ao **CONTRATANTE**, por escrito, todas as medidas que lhe parecerem oportunas, com vistas a reduzir ou eliminar as dificuldades encontradas, bem como os custos envolvidos. O **CONTRATANTE** compromete-se a manifestar-se, por escrito, no prazo máximo de 10 (dez) dias consecutivos, quanto à sua aprovação, recusa ou às disposições por ela aceitas, com seus custos correlatos.

6.7. As Partes Contratantes não são responsáveis pela inexecução, execução tardia ou parcial de suas obrigações, quando a falta resultar, comprovadamente, de fato necessário, cujo efeito não era possível evitar ou impedir. Essa exoneração de responsabilidade deve produzir efeitos nos termos do Parágrafo Único do Artigo 393 do Código Civil Brasileiro.

6.8. No caso de uma das partes se achar impossibilitada de cumprir algumas de suas obrigações, por motivo de caso fortuito ou força maior, deve informar expressa e formalmente esse fato à outra Parte, no máximo até 10 (dez) dias consecutivos contados da data em que ela tenha tomado conhecimento do evento.

6.8.1. A comunicação de que trata este subitem deve conter a caracterização do evento e as justificativas do impedimento que alegar, fornecendo à outra parte, com a maior brevidade, todos os elementos comprobatórios e de informação, atestados periciais e certificados, bem como comunicando todos os elementos novos sobre a evolução dos fatos ou eventos verificados e invocados, particularmente sobre as medidas tomadas ou preconizadas para reduzir as consequências desses fatos ou eventos, e sobre as possibilidades de retomar, no todo ou em parte, o cumprimento de suas obrigações contratuais.

6.8.2. O prazo para execução das obrigações das Partes, nos termos desta Cláusula, deve ser acrescido de tantos dias quanto durarem as consequências impeditivas da execução das respectivas obrigações da parte afetada pelo evento.

6.9. A não utilização pelas partes de quaisquer dos direitos assegurados neste Contrato, ou na Lei em geral, ou no Regulamento, ou a não aplicação de quaisquer sanções, não



CONTRATO Nº 2025/154-01

invalida o restante do Contrato, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação ou de ações futuras.

6.10. Qualquer comunicação pertinente ao Contrato, a ser realizada entre as partes contratantes, inclusive para manifestar-se, oferecer defesa ou receber ciência de decisão sancionatória ou sobre rescisão contratual, deve ocorrer por escrito, preferencialmente nos seguintes e-mails:

E-mail **CONTRATANTE** – ita.rodriques@basa.com.br

E-mail **CONTRATADA** - comercial@qostecnologia.com.br

6.10.1. As Partes são obrigadas a verificar os e-mails referidos neste subitem a cada 24 (vinte e quatro) horas e, se houver alteração de e-mail ou qualquer defeito técnico, devem comunicar à outra Parte no prazo de 24 (vinte e quatro) horas.

6.10.2. Os prazos indicados nas comunicações iniciam em 02 (dois) dias úteis a contar da data de envio do e-mail.

6.11. A execução do presente Contrato e das parcelas do presente Contrato estão condicionadas à expedição, por parte do Gestor de Contrato do **CONTRATANTE**, das respectivas ordens de fornecimento do bem e da prestação dos serviços.

7. CLÁUSULA SÉTIMA – RECEBIMENTO

7.1. O **CONTRATANTE**, por meio do Agente de Fiscalização Técnica, deve receber o objeto do presente Contrato na forma do **Termo de Referência – Anexo III** deste Contrato.

7.2. Acaso verifique o descumprimento de obrigações por parte da **CONTRATADA**, o Agente de Fiscalização técnica ou administrativo deve comunicar ao preposto desta, indicando, expressamente, o que deve ser corrigido e o prazo máximo para a correção. O tempo para a correção deve ser computado no prazo de execução do Contrato, para efeito de configuração da mora e suas cominações.

7.2.1. Realizada a correção pela **CONTRATADA**, abrem-se novamente os prazos para os recebimentos estabelecidos nesta Cláusula.

8. CLÁUSULA OITAVA – CONDIÇÕES DE FATURAMENTO E PAGAMENTO

8.1. Pelos serviços de suporte técnico, o **CONTRATANTE** pagará mensalmente à **CONTRATADA**, da seguinte forma:

8.1.1 Para a efetivação do pagamento, o **CONTRATANTE** deverá receber a nota fiscal e/ou fatura, e seus valores, que deverá ser entregue em duas vias, no local de prestação de serviço. Deverá ser realizado pelo **CONTRATANTE**, através crédito em **Conta Corrente nº 48403-2, Agência 0007- 8, Banco do Brasil (001)** da **CONTRATADA**, nos dias 05 (cinco), 15 (quinze) ou 25 (vinte e cinco), desde que a **CONTRATADA** efetive a entrega das Notas Fiscais e Faturas discriminativas com 10 (dez) dias de antecedência da data prevista para pagamento, e após a conferência e confirmação da execução do serviço, devidamente comprovado através do Termo Circunstanciado elaborado pelo fiscal.

8.1.2 O pagamento dos valores referentes ao suporte e manutenção do hardware associados à solução serão efetuados após a apresentação da nota fiscal/fatura ao **CONTRATANTE**.

8.1.3 Caso a **CONTRATADA** opte pelo recebimento do pagamento em conta corrente mantida em outra instituição financeira será cobrado o valor da tarifa TED correspondente ao da tabela de tarifas e serviços do Banco, sendo que esse



valor será de responsabilidade da **CONTRATADA** e deduzido do valor do crédito a ser enviado.

- 8.1.4 O pagamento será automaticamente transferido para o dia útil subsequente, caso não haja expediente no **CONTRATANTE** nas datas previstas para tal. O atraso na entrega da Nota Fiscal/Fatura implicará a transferência automática do pagamento para o próximo mês, sem qualquer acréscimo financeiro ao **CONTRATANTE**.
- 8.1.5 No caso de atraso no pagamento por culpa exclusiva do **CONTRATANTE**, o valor devido será acrescido de encargos financeiros de 0,5% (cinco décimos por cento) ao mês, calculados "pro-rata die" até o dia do efetivo pagamento.
- 8.1.6 Para efeito de pagamento, a **CONTRATADA** deverá apresentar, juntamente com as notas fiscais/faturas, a documentação abaixo relacionada, caso não estejam disponíveis no Cadastro Único de Fornecedores (SICAF):
- I - Certidão Conjunta Negativa de **Débitos relativos a Tributos Federais** e à Dívida Ativa da União;
 - II - Certidão Negativa de Débitos das **Fazendas Estadual e Municipal** de seu domicílio ou sede;
 - III - Certidão de Regularidade do **FGTS – CRF**;
 - IV - Certidão Negativa de Dívidas Trabalhistas – **CNDT**; e
 - V - Declaração do **Simples Nacional**, caso seja optante.
- 8.1.7 A não apresentação dos documentos referidos no item anterior poderá implicar em rescisão do Contrato.
- 8.1.8 A Nota Fiscal/Fatura deverá conter o endereço, o CNPJ, o número do Contrato, o número do banco, da agência e da conta corrente da empresa e a descrição clara do objeto da contratação.
- 8.1.9 A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pelo **CONTRATANTE**, o qual atestará a execução dos serviços contratados e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela **CONTRATADA**, todas as condições pactuadas.
- 8.1.10 Em caso de necessidade de ajuste na Nota Fiscal/Fatura será estabelecido prazo para a **CONTRATADA** fazer a substituição do documento em questão.
- 8.1.11 A Nota Fiscal deve ser emitida em nome do **CONTRATANTE**, emitida sem rasuras, com as informações a seguir e o item sobressalente entregue no endereço abaixo:

Banco da Amazônia S.A.		Endereço para emissão da nota fiscal			
Seq.	Estado	Endereço	Município	UF	CEP
01	Pará	Avenida Presidente Vargas, nº 800	Belém	PA	66.017-901

- 8.1.12 - No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão estes restituídos à **CONTRATADA** para as correções solicitadas, não respondendo o **CONTRATANTE** por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.
- 8.1.13 Não serão efetuados quaisquer pagamentos, enquanto perdurar pendência de liquidação de obrigações, em virtude de penalidades impostas à **CONTRATADA** ou inadimplência total ou parcial referente à contratação.



8.2 Caso haja interesse de ambas as partes, o prazo de pagamento, considerada a data do efetivo desembolso, poderá ser reduzido desde que seja concedido o desconto estabelecido pelo Departamento Econômico-Financeiro, sendo que a taxa de deságio deverá ser no mínimo equivalente ao CDI (Certificado de Depósito Interbancário), acrescida da taxa de juros de 12% (doze por cento) ao ano.

8.2.1 As faturas que apresentarem erros devem ser devolvidas à **CONTRATADA** pela Unidade de Gestão de Contrato do **CONTRATANTE** para a correção ou substituição. O **CONTRATANTE**, por meio da Unidade de Gestão de Contrato, deve efetuar a devida comunicação à **CONTRATADA** dentro do prazo fixado para o pagamento. Depois de apresentada a Nota Fiscal/Fatura, com as devidas correções, o prazo previsto no subitem acima deve começar a correr novamente do seu início, sem que nenhuma atualização ou encargo possa ser imputada ao **CONTRATANTE**.

8.3 Havendo controvérsia sobre a execução do objeto, quanto à dimensão, à qualidade e à quantidade, o montante correspondente à parcela incontroversa deverá ser pago no prazo previsto no subitem acima e o relativo à parcela controvertida deve ser retido.

8.4 É vedado o pagamento antecipado.

8.5 É permitido ao **CONTRATANTE** descontar dos créditos da **CONTRATADA** qualquer valor relativo à multa, ressarcimentos e indenizações, sempre observado o contraditório e a ampla defesa.

8.6 Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo **CONTRATANTE**, o valor devido deve ser acrescido de atualização financeira, desde a data do vencimento até a data do efetivo pagamento, à taxa nominal de 6% a.a. (seis por cento ao ano), acrescido dos encargos, calculados da seguinte forma:

$$EM = I \times VP \times N$$

Onde:

EM = Encargos moratórios devidos;

I=Índice de atualização financeira, calculado como: $(6 / 100 / 365) = 0,00016438$;

VP = Valor da parcela em atraso;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

9 CLÁUSULA NONA – SUBCONTRATAÇÃO

9.1. A **CONTRATADA** não poderá subcontratar os serviços objeto deste Contrato.

10 CLÁUSULA DÉCIMA – ALTERAÇÕES INCIDENTES SOBRE O OBJETO DO CONTRATO

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

10.1.1. A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do Artigo 81 da Lei n. 13.303/2016, devendo observar o seguinte:

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

b) Deve ser mantida a diferença, em percentual, entre o valor global do Contrato e o valor orçado pelo **CONTRATANTE**, salvo se o Fiscal Técnico do Contrato apontar justificativa técnica ou econômica, que deve ser ratificada pelo Gestor do Contrato;



10.1.2. A alteração qualitativa não se sujeita aos limites previstos nos § 1º e 2º do Artigo 81 da Lei n. 13.303/2016, devendo observar o seguinte:

- a) Os encargos decorrentes da continuidade do Contrato devem ser inferiores aos da rescisão contratual e aos da realização de um novo procedimento licitatório;
- b) As consequências da rescisão contratual, seguida de nova licitação e contratação, devem importar prejuízo relevante ao interesse coletivo;
- c) As mudanças devem ser necessárias ao alcance do objetivo original do Contrato, à otimização do cronograma de execução e à antecipação dos benefícios sociais e econômicos decorrentes;
- d) A capacidade técnica e econômico-financeira da **CONTRATADA** deve ser compatível com a qualidade e a dimensão do objeto contratual aditado;
- e) A motivação da mudança contratual deve ter decorrido de fatores supervenientes não previstos e que não configurem burla ao processo licitatório;
- f) A alteração não deve ocasionar a transfiguração do objeto originalmente contratado em outro de natureza ou propósito diverso.

10.2. As alterações incidentes sobre o objeto devem ser:

- a) Instruídas com memória de cálculo e justificativas de competência do Fiscal Técnico e do Fiscal Administrativo do **CONTRATANTE**, que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites;
- b) As justificativas devem ser ratificadas pelo Gestor do Contrato do **CONTRATANTE**; e
- c) Submetidas à área jurídica e, quando for o caso, à área financeira do **CONTRATANTE**;

10.3. As alterações contratuais incidentes sobre o objeto e as decorrentes de revisão contratual devem ser formalizadas por termo aditivo firmado pela mesma autoridade que firmou o contrato, devendo o extrato do termo aditivo ser publicado no sítio eletrônico do **CONTRATANTE**.

10.4. Não caracterizam alteração do contrato e podem ser registrados por simples apostila, dispensando a celebração de termo aditivo:

- a) A variação do valor contratual para fazer face ao reajuste de preços;
- b) As atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no Contrato;
- c) A correção de erro material havido no instrumento de Contrato;
- d) As alterações na razão ou na denominação social da **CONTRATADA**;
- e) As alterações na Legislação tributária que produza efeitos nos valores contratados.

11. CLÁUSULA DÉCIMA PRIMEIRA – EQUILÍBRIO ECONÔMICO-FINANCEIRO DO CONTRATO

11.1. O equilíbrio econômico-financeiro do Contrato deve ocorrer por meio de:

- a) Reajuste: instrumento para manter o equilíbrio econômico-financeiro do Contrato diante de variação de preços e custos que sejam normais e previsíveis, relacionadas com o fluxo normal da economia e com o processo inflacionário, devido ao completar 01 (um) ano a contar da data da proposta;



b) Revisão: instrumento para manter o equilíbrio econômico-financeiro do Contrato diante de variação de preços e custos decorrentes de fatos imprevisíveis ou previsíveis, porém com consequências incalculáveis, e desde que se configure álea econômica extraordinária e extracontratual, sem a necessidade de periodicidade mínima.

11.2. O reajuste deve ser concedido de ofício pelo **CONTRATANTE** e deve observar o índice ICTI.

11.3. A revisão deve ser precedida de solicitação da **CONTRATADA**, acompanhada de comprovação:

a) Dos fatos imprevisíveis ou previsíveis, porém com consequências incalculáveis;

b) Da alteração de preços ou custos, por meio de notas fiscais, faturas, tabela de preços, orçamentos, notícias divulgadas pela imprensa e por publicações especializadas e outros documentos pertinentes, preferencialmente com referência à época da elaboração da proposta e do pedido de revisão; e

c) De demonstração analítica, por meio de planilha de custos e formação de preços, sobre os impactos da alteração de preços ou custos no total do Contrato.

11.3.1. A revisão que não for solicitada durante a vigência do Contrato considera-se preclusa com a prorrogação ou renovação contratual ou com o encerramento do Contrato.

11.3.2. Caso, a qualquer tempo, a **CONTRATADA** seja favorecida com benefícios fiscais isenções e/ou reduções de natureza tributárias em virtude do cumprimento do Contrato, as vantagens auferidas serão transferidas ao **CONTRATANTE**, reduzindo-se o preço.

11.3.3. Caso, por motivos não imputáveis à **CONTRATADA**, sejam majorados os gravames e demais tributos ou se novos tributos forem exigidos da **CONTRATADA**, cuja vigência ocorra após a data da apresentação da Proposta, O **CONTRATANTE** absorverá os ônus adicionais, reembolsando a **CONTRATADA** dos valores efetivamente pagos e comprovados, desde que não sejam de responsabilidade legal direta e exclusiva da **CONTRATADA**.

11.4. Os pedidos de revisão serão decididos em decisão fundamentada no prazo máximo de 60 (sessenta) dias contados da formalização do requerimento.

11.4.1. O **CONTRATANTE** poderá realizar diligências junto à **CONTRATADA** para que esta complemente ou esclareça alguma informação indispensável à apreciação dos pedidos. Nesta hipótese, o prazo estabelecido neste subitem ficará suspenso enquanto pendente a resposta pela **CONTRATADA**.

12. CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

12.1. O inadimplemento contratual de ambas as partes autoriza a rescisão, que deve ser formalizada por distrato e antecedida de comunicação à outra Parte Contratante sobre a intenção de rescisão, apontando-se as razões que lhe são determinantes, dando-se o prazo de 05 (cinco) dias úteis para eventual manifestação.

12.2. A Parte que pretende a rescisão deve avaliar e responder motivadamente a manifestação referida no subitem precedente no prazo de 10 (dez) dias úteis, comunicando a outra parte, na forma prevista neste Contrato, considerando-se o Contrato rescindido com a referida comunicação.



12.3. Aplica-se a teoria do adimplemento substancial, devendo as partes contratantes ponderar, no que couber, antes de decisão pela rescisão:

- a) Impactos econômicos e financeiros decorrentes do atraso na fruição dos benefícios do empreendimento;
- b) Riscos sociais, ambientais e à segurança da população local decorrentes do atraso na fruição dos benefícios do empreendimento;
- c) Motivação social e ambiental do empreendimento;
- d) Custo da deterioração ou da perda das parcelas executadas;
- e) Despesa necessária à preservação das instalações e dos objetos já executados;
- f) Despesa inerente à desmobilização e ao posterior retorno às atividades;
- g) Possibilidade de saneamento dos descumprimentos contratuais;
- h) Custo total e estágio de execução física e financeira do Contrato;
- i) Empregos diretos e indiretos perdidos em razão da paralisação do Contrato;
- j) Custo para realização de nova licitação ou celebração de novo Contrato;
- k) custo de oportunidade do capital durante o período de paralisação.

12.4. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pela **CONTRATADA** pode dar ensejo à rescisão contratual, sem prejuízo das demais sanções.

12.4.1. Na hipótese deste subitem, o **CONTRATANTE** pode conceder prazo para que a **CONTRATADA** regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade da **CONTRATADA** de corrigir a situação.

13. CLÁUSULA DÉCIMA TERCEIRA – SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa nos termos da Legislação vigente, a **CONTRATADA** que:

- 13.1.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação.
- 13.1.2 Ensejar o retardamento da execução do objeto.
- 13.1.3 Falhar ou fraudar na execução do contrato.
- 13.1.4 Comportar-se de modo inidôneo; e
- 13.1.5 Fraude fiscal.

13.1. Pela inexecução total ou parcial do objeto deste contrato, o **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções:

13.1.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.

13.1.2. Multa de:

- 1. 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério do **CONTRATANTE**, no caso de execução com atraso, poderá ocorrer a não-



- aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão da avença.
2. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima ou de inexecução parcial da obrigação assumida.
 3. 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida.
 4. 0,2% a 3,2% por dia sobre o valor do Contrato, conforme detalhamento constante das tabelas 1 e 2 abaixo.
 5. Até 1% (um por cento) por dia útil de atraso na implantação dos serviços. A referida multa terá como base o valor global referente ao serviço descumprido;
 6. Até 10% (dez por cento) sobre o valor global do Contrato, a critério da autoridade competente do **CONTRATANTE**, em razão de qualquer descumprimento das demais obrigações contratuais, não previstas nos itens acima.
- 13.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com o **CONTRATANTE**, por prazo não superior a 02 (dois) anos, apurados em razão da natureza e gravidade da infração cometida.
 - 13.2. O total das multas aplicadas não poderá exceder o montante de 30% (trinta por cento) do valor global do Contrato.
 - 13.3. O valor da multa poderá ser descontado da nota fiscal ou de crédito existente no **CONTRATANTE** em relação à **CONTRATADA**. Caso o valor da multa seja superior ao crédito existente, a diferença será cobrada na forma da lei.
 - 13.4. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.
 - 13.5. A aplicação de qualquer das penalidades previstas somente poderá ser aplicada após procedimento administrativo, e desde que assegurados o contraditório e a ampla defesa, facultada a **CONTRATADA** a defesa prévia, no prazo de 10 (dez) dias úteis, observando-se o procedimento previsto na Legislação Vigente.
 - 13.6. Contra a decisão de aplicação de penalidade, a **CONTRATADA** poderá interpor o recurso cabível, na forma e no prazo previstos no Regulamento de Formalização, Execução e Fiscalização de Contratos Administrativos.
 - 13.7. A imposição de penalidades não impede a extinção do Contrato pelo **CONTRATANTE**, nos termos da Legislação aplicável.
 - 13.8. As sanções de advertência e de impedimento de licitar e contratar com o **CONTRATANTE** poderão ser aplicadas à **CONTRATADA** juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.
 - 13.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado ao **CONTRATANTE**, observado o princípio da proporcionalidade.
 - 13.10. As penalidades serão obrigatoriamente registradas no SICAF.
 - 13.10.1. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:



GRAU	CORRESPONDÊNCIA
01	0,2% (dois décimos por cento) Por dia sobre o valor do Contrato
02	0,4% (quatro décimos por cento) Por dia sobre o valor do Contrato
03	0,8% (oito décimos por cento) Por dia sobre o valor do Contrato
04	1,6% (um inteiro e seis décimos por cento) Por dia sobre o valor do Contrato
05	3,2% (três inteiros e dois décimos por cento) Por dia sobre o valor do Contrato

INFRAÇÃO		
ITEM	DESCRIÇÃO	GRAU
01	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência;	05
02	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por Unidade de atendimento;	04
03	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
04	Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
05	Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo Órgão fiscalizador, por item e por ocorrência;	03
06	Deixar de indicar e manter durante a execução do contrato os prepostos previstos no Edital/contrato;	01

14. CLÁUSULA DÉCIMA QUARTA – RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANCO DA AMAZÔNIA

14.1. Com fundamento no artigo 5º da Lei n. 12.846/2013, constituem atos lesivos ao **CONTRATANTE** as seguintes práticas:

- a) Fraudar o presente Contrato;
- b) Criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o Contrato;
- c) Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações deste Contrato, sem autorização em lei, no ato convocatório da licitação pública ou neste instrumento contratual; ou
- d) Manipular ou fraudar o equilíbrio econômico-financeiro deste Contrato; e
- e) Realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei n. 12.846/2013, Decreto n. 8.420/2015, revogado pelo Decreto nº 11.129/2022, Lei n. 13.303/15, ou de quaisquer outras leis ou regulamentos aplicáveis, ainda que não relacionadas no presente Contrato.

14.2. A prática, pela **CONTRATADA**, de atos lesivos ao **CONTRATANTE**, a sujeitará, garantida a ampla defesa e o contraditório, às seguintes sanções administrativas:



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

b) Publicação extraordinária da decisão condenatória.

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

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

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

a) Em jornal de grande circulação na área da prática da infração e de atuação Em jornal de grande circulação na área da prática da infração e de atuação da **CONTRATADA** ou, na sua falta, em publicação de circulação nacional;

b) Em edital afixado no estabelecimento ou no local de exercício da atividade do **CONTRATANTE**, em localidade que permita a visibilidade pelo público, pelo prazo mínimo de 30 (trinta) dias; e

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

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

14.3. A prática de atos lesivos ao **CONTRATANTE** será apurada e apenada em Processo Administrativo de Responsabilização (PAR), instaurado pelo Gestor do Contrato e conduzido por comissão composta por 02 (dois) servidores designados.

14.3.1. Na apuração do ato lesivo e na dosimetria da sanção eventualmente aplicada, o **CONTRATANTE** deve levar em consideração os critérios estabelecidos no Artigo 7º e seus incisos da Lei n. 12.846/2013.

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

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

14.3.4. O processamento do PAR não interferirá na instauração e seguimento de processo administrativo específicos para apuração da ocorrência de danos e prejuízos ao **CONTRATANTE** resultantes de ato lesivo cometido pela **CONTRATADA**, com ou sem a participação de Agente Público.

14.3.5. O PAR e o sancionamento administrativo obedecerão às regras e parâmetros dispostos em legislação específica, notadamente, na Lei n. 12.846/2013 e no Decreto n. 8.420/ 2015, inclusive suas eventuais alterações, sem prejuízo ainda da aplicação do ato de que trata o artigo 21 do Decreto no. 8.420/2015, revogado pelo Decreto nº 11.129/2022.



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

14.5. As disposições deste item se aplicam quando a **CONTRATADA** se enquadrar na definição legal do Parágrafo Único do artigo 1º da Lei n. 12.846/2013.

14.6. Não obstante o disposto nesta Cláusula, a **CONTRATADA** está sujeita a quaisquer outras responsabilizações de natureza cível, administrativa e, ou criminal, previstas neste Contrato e, ou na Legislação aplicável, no caso de quaisquer violações.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICIDADE E CONFIDENCIALIDADE

15.1. Quaisquer informações relativas ao presente Contrato, somente podem ser dadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, após autorização, por escrito, do **CONTRATANTE**. Para os efeitos desta Cláusula, deve ser formulada a solicitação, por escrito, ao **CONTRATANTE**, informando todos os pormenores da intenção da **CONTRATADA**, reservando-se, ao **CONTRATANTE**, o direito de aceitar ou não o pedido, no todo ou em parte. O **Termo de confidencialidade e sigilo para o tratamento de dados e informações** conforme **ANEXO I** deste Contrato asseguram os termos aqui propostos.

16. CLÁUSULA DÉCIMA SEXTA – POLÍTICA DE RELACIONAMENTO E ANTICORRUPÇÃO

16.1. A **CONTRATADA** assume o compromisso de deferência a práticas de integridade em todo o encadeamento contratual, com expressa observância aos princípios contidos no Código de Condutas e Integridade do **CONTRATANTE**, cuja íntegra esta disponibilizada no site do Banco da Amazônia S.A. (www.bancoamazonia.com.br), bem como assinar o **Termo de Confidencialidade e Sigilo - ANEXO I** e o **Termo de Política Anticorrupção - Anexo II**, ambos Anexos deste Contrato.

16.2. O **CONTRATANTE** reserva-se no direito de realizar auditoria na **CONTRATADA** para verificar sua conformidade com as Leis e o seu Programa Anticorrupção, sendo a **CONTRATADA** responsável por manter em sua guarda todos os arquivos e registros evidenciando tal conformidade, assim como disponibilizá-los ao **CONTRATANTE** dentro de 05 (cinco) dias úteis a contar de sua solicitação.

17. CLÁUSULA DÉCIMA SÉTIMA – TRATAMENTO DE DADOS

17.1 A **CONTRATADA**, por si e por seus colaboradores, obriga-se a atuar no presente Contrato em conformidade com a Legislação vigente sobre proteção de Dados consoante às 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, o tratamento de dados pessoais, além de atender às demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos Dados Pessoais do **CONTRATANTE**, o que inclui os Dados dos clientes desta.

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



- 17.2.1 Diretrizes de tratamento. Considerando que competirá ao **CONTRATANTE** as decisões referentes ao tratamento dos Dados Pessoais (sendo, portanto, controladora) e que a **CONTRATADA** realizará o tratamento dos Dados Pessoais em nome do **CONTRATANTE** sendo, portanto, Operadora), a **CONTRATADA** seguirá estritamente as instruções recebidas do **CONTRATANTE** em relação ao tratamento dos Dados Pessoais atinentes às finalidades do Contrato, devendo observar rigorosamente o cumprimento das normas aplicáveis.
- 17.2.2 A **CONTRATADA** deverá corrigir, completar, excluir e/ou bloquear os Dados, caso seja solicitado pelo **CONTRATANTE**.
- 17.2.3 Solicitações de Titulares. A **CONTRATADA** deverá notificar imediatamente o **CONTRATANTE** sobre quaisquer reclamações e solicitações dos Titulares de Dados Pessoais que ocorram em virtude deste Contrato, atentando ao prazo máximo de 24h.
- 17.2.4 Confidencialidade e Sigilo. Os termos de confidencialidade e sigilo para o tratamento de dados e informações estão descritos no **Anexo I - TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES** deste Contrato, sendo sua formalização, parte integrante e indispensável desta cláusula.
- 17.2.5 A **CONTRATADA** deverá garantir a formalização de termo de Confidencialidade e Sigilo com todos os empregados envolvidos na prestação do serviço, conforme modelo disponibilizado no **ADENDO III - TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE DO EMPREGADO TERCEIRIZADO**, do **Edital de Pregão Eletrônico nº 90002/2025**.
- 17.2.6 Registro de atividades. A **CONTRATADA** deverá manter registro das operações de tratamento de dados pessoais que realizar e a identificação de quem as realizou.
- 17.2.7 Governança e segurança. A **CONTRATADA** deverá garantir a implementação de 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 os ambientes físicos ou lógicos utilizados no tratamento de Dados são estruturados de forma a atender aos requisitos de segurança, padrões de boas práticas, governança e princípios gerais previstos em Lei, além das demais normas regulamentares aplicáveis.
- 17.2.8 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 ao **CONTRATANTE** relatórios sobre esses controles sempre que solicitado. Os relatórios deverão incluir, no mínimo: (i) o status dos sistemas de processamento de Dados Pessoais; (ii) as medidas de segurança; (iii) o tempo de inatividade registrado das medidas técnicas de segurança; (iv) as inconformidades relacionadas as medidas organizacionais; (v) quaisquer eventuais violações de dados e/ou incidentes de segurança; (vi) as ameaças percebidas à segurança e aos Dados Pessoais; e (vii) as melhorias exigidas e/ou recomendadas.
- 17.2.9 Monitoramento de conformidade. O **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.



- 17.2.10 Notificação. A **CONTRATADA** deverá notificar o **CONTRATANTE** em até 24h (vinte e quatro) horas: (i) qualquer descumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (ii) qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (iii) qualquer violação de segurança na **CONTRATADA** ou nos seus contratados; (iv) qualquer exposições ou ameaças em relação à conformidade da proteção de Dados Pessoais; (v) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente.
- 17.2.11 Colaboração. A **CONTRATADA** compromete-se a auxiliar o **CONTRATANTE**: (i) 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; (ii) e no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais.
- 17.2.12 Propriedade dos Dados. O presente Contrato não transfere a propriedade ou controle dos dados do **CONTRATANTE** ou dos clientes desta para a **CONTRATADA** ("Dados"). Os Dados gerados, obtidos ou coletados a partir da prestação dos Serviços ora contratados são e continuarão sendo de propriedade do **CONTRATANTE**, inclusive sobre qualquer novo elemento de Dados, produto ou subproduto que seja criado a partir do tratamento de Dados estabelecido por este Contrato.
- 17.2.13 Tratamento de dados no exterior. Todo e qualquer tratamento de dados fora do Brasil, depende de autorização prévia e por escrito pelo **CONTRATANTE** à **CONTRATADA**.
- 17.2.14 Atuação restrita e vedação de compartilhamento sem autorização. A **CONTRATADA** não poderá usar, compartilhar ou comercializar quaisquer eventuais elementos de Dados, produtos ou subprodutos que se origem ou sejam criados a partir do tratamento de Dados estabelecido por este Contrato sem autorização expressa do **CONTRATANTE**.
- 17.2.15 Adequação legislativa. Caso exista modificação dos textos legais ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços à **CONTRATANTE** ou na execução das atividades ligadas a este Contrato, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a **CONTRATADA** concorda em notificar formalmente este fato ao **CONTRATANTE**, que terá o direito de resolver o presente Contrato sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.
- 17.2.16 Se qualquer Legislação nacional ou internacional aplicável ao tratamento de Dados Pessoais no âmbito do Contrato vier a exigir adequação de processos e/ou instrumentos contratuais por forma ou meio determinado, as Partes desde já acordam em celebrar termo aditivo escrito neste sentido.
- 17.2.17 Solicitação de Dados ou Registros. Sempre que Dados ou Registros forem solicitados pelo **CONTRATANTE**, a **CONTRATADA** 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 o **CONTRATANTE** antes de fornecê-los, se possível.
- 17.2.18 Devolução dos Dados. A **CONTRATADA** se compromete a devolver todos os Dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que (i) o **CONTRATANTE** solicitar; (ii) o Contrato for rescindido; ou (iii) com o término do presente Contrato. Em adição, a **CONTRATADA** não deve guardar, armazenar ou



reter os Dados por tempo superior ao prazo legal ou necessário para a execução do presente Contrato.

- 17.2.19 Caso os Dados da **CONTRATADA** estejam contidos em um banco de Dados, além de restituir este banco de Dados de inteira propriedade do **CONTRATANTE** em qualquer hipótese de extinção deste instrumento, 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.

18. CLÁUSULA DÉCIMA OITAVA – DAS OBRIGAÇÕES

18.1 OBRIGAÇÕES DO CONTRATANTE

- 18.2. O **CONTRATANTE** deverá indicar o responsável pela Gestão e Fiscalização do Contrato.
- 18.3. O **CONTRATANTE** deverá disponibilizar todas as informações necessárias à **CONTRATADA**, com o intuito de fornecer subsídios, para prestação dos serviços contratados.
- 18.4. O **CONTRATANTE** deverá efetuar o pagamento devido pela prestação dos serviços, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas neste Contrato e no **Edital de pregão Eletrônico nº 9002/2025** e seus Anexos.
- 18.5. O **CONTRATANTE** deverá permitir, sempre que necessário, acesso dos profissionais da **CONTRATADA** às dependências, equipamentos, softwares e sistemas de informação do **CONTRATANTE**, relacionados ao objeto do Contrato ou necessários à execução dos serviços.
- 18.6. O **CONTRATANTE** deverá fiscalizar o cumprimento dos requisitos de qualificação profissional exigidos neste Contrato e Anexos, solicitando à **CONTRATADA**, sempre que necessário, substituição de profissional, treinamentos e certificações necessárias.
- 18.7. O **CONTRATANTE** deverá comunicar, formalmente, a **CONTRATADA** qualquer falha verificada no cumprimento do Contrato.
- 18.7.1. Fornecer cópia dos normativos internos vigentes do **CONTRATANTE** que estiverem relacionados à prestação dos serviços.

18.8. OBRIGAÇÕES DA CONTRATADA

- 18.8.1. Alocar todos os recursos necessários para obter uma fiel execução dos serviços previstos no objeto da contratação, de forma plena e satisfatória, iniciando e prestando os serviços no prazo estipulado, na forma e nas condições pactuadas, em estrita conformidade com as especificações, prazos e condições estabelecidas nos termos contratuais e na sua proposta.
- 18.8.2. Planejar, desenvolver, implantar, executar e manter o serviço objeto do Contrato dentro dos acordos de níveis mínimos de serviço estabelecidos.
- 18.8.3. Qualquer problema que venha a comprometer o bom andamento dos serviços ou o alcance dos níveis mínimos de serviço acordados, deve ser imediatamente comunicado ao **CONTRATANTE**, que colaborará com a **CONTRATADA** na busca da melhor solução.
- 18.8.4. Notificar o **CONTRATANTE**, imediatamente e por escrito, qualquer anormalidade que verificar na execução dos serviços.



- 18.8.5. Responder pelos danos comprovadamente causados ao **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, inclusive de seus empregados, quando da execução do objeto contratado. A Fiscalização ou o acompanhamento do **CONTRATANTE** não excluirá ou reduzirá essa responsabilidade da **CONTRATADA**.
- 18.8.6. Observar boas práticas relativas à segurança da informação, especialmente as indicadas nos normativos internos do **CONTRATANTE**, sobretudo na Política de Segurança da Informação e Cibernética, em todas as atividades executadas durante o ciclo de desenvolvimento das aplicações.
- 18.8.7. Emitir, por ocasião da assinatura deste Contrato, o **Anexo I – Termo De Confidencialidade E Sigilo deste Contrato**, pelo qual se compromete a 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.
- 18.8.8. Fornecer, antes do início da prestação do serviço, o **Adendo III – Termo De Confidencialidade e Sigilo do Profissional do Edital de Pregão Eletrônico nº 90002/2025**, a ser assinado por cada profissional que venha a prestar os seus serviços, pelo qual se comprometem a manter o sigilo e a confidencialidade de todos os dados e informações de que venha a ter conhecimento no exercício de suas atribuições.
- 18.8.9. Em caso de não cumprimento das condições estabelecidas nos Termos mencionados nos **itens 18.8.7 e 18.8.8**, desta Cláusula e/ou em caso de quebra da guarda e sigilo, aludidos, ou de utilização dos dados fornecidos pelo **CONTRATANTE**, para outros fins de qualquer natureza ou espécie, que não os expressamente autorizados e para uso exclusivo dos serviços prestados a este, a **CONTRATADA** responderá de forma incondicional, civil, criminal e administrativamente pelo fato, sem prejuízo do direito do **CONTRATANTE** de promover a rescisão contratual, com a aplicação das penalidades previstas neste ajuste.
- 18.8.10. Possuir em sua equipe profissionais especialistas certificados nas soluções ofertadas para prestação do serviço, comprovada por meio de certificações emitidas pelo fabricante do software.
- 18.8.11. Devolver e eliminar de suas bases de dados, após a realização dos serviços, toda e qualquer informação ou documentos porventura encaminhados pelo **CONTRATANTE** para auxiliar na realização dos serviços.
- 18.8.12. Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação para contratar com a Administração Pública, apresentando sempre que exigido os comprovantes de regularidade.
- 18.8.13. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o **CONTRATANTE**.
- 18.8.14. Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à prestação dos serviços, originariamente ou vinculados por prevenção, conexão ou contingência.
- 18.8.15. Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus



empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do Contrato a ser firmado.

- 18.8.16. Assumir inteira responsabilidade técnica e administrativa pelo respectivo objeto contratado, não podendo, em qualquer hipótese, transferir a outras empresas a responsabilidade por problemas ocorridos na execução do serviço.
- 18.8.17. 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 Banco 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.
- 18.8.18. Assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do **CONTRATANTE** através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado.
- 18.8.19. Indicar formalmente um profissional para a função de preposto da **CONTRATADA** apto a representá-la junto ao **CONTRATANTE**, que deverá responder pela fiel execução do Contrato.
- 18.8.20. Prestar todos os esclarecimentos que lhe forem solicitados pelo **CONTRATANTE**.
- 18.8.21. Aceitar, por parte do **CONTRATANTE**, em todos os aspectos, a fiscalização no cumprimento do objeto contratado.
- 18.8.22. Além das obrigações usualmente aplicadas à **CONTRATADA**, permitir ao Banco Central do Brasil acesso a termos firmados, documentos e informações atinentes aos serviços prestados, bem como às suas dependências, nos termos do § 1º do artigo 33 da Resolução CMN nº 4.557/2017.

19. CLÁUSULA DÉCIMA NONA – FORO

19.1. As Partes contratantes elegem o Foro da Cidade de Belém, Capital do Estado do Pará, para a solução de qualquer questão oriunda do presente Contrato, com exclusão de qualquer outro.

19.2. 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 o presente Contrato para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

Belém-PA,

BANCO DA AMAZÔNIA S.A.



DocuSigned by:
Diego Santos Lima
2E9901FEDD4F4482
DIEGO SANTOS LIMA
Diretor Corporativo – DICOP

QOS TECNOLOGIA E SERVIÇOS LTDA

DocuSigned by:
Walter Fernandes Pinto Neto
2E9901FEDD4F4482
WALTER FERNANDES PINTO NETO
Sócio Administrador

ANEXO I**TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES**

Este Termo de Compromisso é celebrado entre:

BANCO DA AMAZÔNIA, Endereço Avenida Presidente Vargas, 800, Belém, Pará, inscrito no CNPJ/MF 04.902.979/0001-44, neste ato representado por seu Diretor Corporativo - DICOP, Sr. **DIEGO SANTOS LIMA**, brasileiro, casado, graduado em administração de empresas, portador do RG nº 075403072021-5 SSP/MA e do CPF/MF nº 011.772.821-78, residente e domiciliado na Região Metropolitana de Belém/PA, abaixo assinado ("**CONTRATANTE**"), e a empresa **QOS TECNOLOGIA E SERVIÇOS LTDA**, com registro na Junta Comercial do Estado de Pernambuco sob o NIRE nº 26201347140, com sede na Cidade de Recife/PE, situada na Avenida Rio Branco, nº 243, Edifício São Paulo, Sala 401, CEP: 50.030-310, inscrita no CNPJ/MF nº 05.012.577/0001-37, representada neste ato por seu Sócio Administrador Sr. **WALTER FERNANDES PINTO NETO**, brasileira, casado, empresário, portador da CNH nº 01339104606 DETRAN/PE e do CPF/MF nº 025.596.954-64, abaixo assinado ("**CONTRATADA**"), **CONTRATANTE** e **CONTRATADA** em conjunto denominadas como Partes:

CONSIDERANDO QUE as Partes, por meio do Contrato nº 2025/154-01 estão estabelecendo uma relação jurídica para o fornecimento de **4.083 (quatro mil e oitenta e três) licenças da solução de IGA**, bem como sua **implantação, treinamento, serviço de suporte e operação da solução e 1000 (um mil) USTs de serviços técnicos especializados em governança de identidade**, contemplando os serviços de implantação, treinamento e suporte e operação da solução, conforme diretrizes, condições, quantidades e exigências estabelecidas no **Edital do Pregão Eletrônico nº 90002/2025 e seus anexos e** neste Contrato, pelo período de 36 (trinta e seis) meses renováveis até o prazo legal, sendo que para serem executados, necessariamente incluem o acesso, o conhecimento e o tratamento de dados e informações corporativas da **CONTRATANTE** pela **CONTRATADA**, além do uso de equipamentos, de recursos computacionais e outros que envolvam a possibilidade de divulgação de informações restritas, de exclusivo interesse da **CONTRATANTE**, sob a posse, guarda e domínio da **CONTRATADA**;

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

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

RESOLVEM as Partes celebrar o presente Termo de Compromisso e Sigilo de Dados e Informações ("Termo"), o qual se regerá pelas considerações acima, bem como, **pelas considerações que forem pertinentes constantes na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).**

1. OBJETO

Este Termo tem por objeto exclusivo proteger as Informações Confidenciais que venham a ser fornecidas ou reveladas pelo **CONTRATANTE** à **CONTRATADA**, bem como disciplinar a forma pela qual elas devem ser utilizadas pela **CONTRATADA**.

1.1. Todas as informações ou dados revelados ou fornecidos, direta ou indiretamente, pela **CONTRATANTE** ou por terceiros em nome desta à **CONTRATADA**, ou obtida por esta de forma lícita, independentemente de divulgação explícita, em quaisquer meios de armazenamento ou transmissão e independente do formato, rotulação ou forma de envio, devem ser tratadas como Informações Confidenciais.



1.2.A **CONTRATADA** reconhece que as Informações Confidenciais são de propriedade exclusiva do **CONTRATANTE** ou são advindas de terceiros e estão sob sua responsabilidade.

1.3.As Informações Confidenciais poderão estar contidas e serem transmitidas por quaisquer meios, incluindo, entre outros, as formas escritas, gráfica, verbal, mecânica, eletrônica, digital, magnética ou criptográfica.

2. RESTRIÇÕES QUANTO À UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1.A **CONTRATADA** reconhece a importância de se manter as Informações Confidenciais em segurança e sob sigilo, mesmo após o término de vigência do presente Termo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem prévia autorização do **CONTRATANTE**, a qualquer terceiro estranho a este Termo.

2.2.Sem prejuízo das demais obrigações previstas neste Termo, a **CONTRATADA** obriga-se a:

- (i) Tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que lhe forem fornecidos pelo **CONTRATANTE** e preservar o seu sigilo, de acordo com a Legislação vigente;
- (ii) Preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo ou comercializar a terceiros;
- (iii) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;
- (iv) Não copiar ou reproduzir, por qualquer meio ou modo: (a) informações classificadas em qualquer grau de sigilo; (b) informações relativas aos materiais de acesso restrito do **CONTRATANTE** salvo autorização da autoridade competente.
- (v) Não utilizar, reter, duplicar modificar, adulterar, subtrair ou adicionar qualquer elemento das Informações Confidenciais que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo **CONTRATANTE** para finalidades específicas;
- (vi) Não modificar ou adulterar as Informações Confidenciais fornecidas pelo **CONTRATANTE**, bem como a não subtrair ou adicionar qualquer elemento a essas Informações Confidenciais;
- (vii) Armazenar e transmitir as Informações Confidenciais digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia;
- (viii) Devolver ao **CONTRATANTE**, ou a exclusivo critério dessa destruir, todas as Informações Confidenciais que estejam em seu poder em até 48h (quarenta e oito horas), contados da data da solicitação; e
- (ix) Informar imediatamente o **CONTRATANTE** qualquer violação a este Termo.

3. PROTEÇÃO DE DADOS PESSOAIS

**CONTRATO Nº 2025/154-01**

3.1.A **CONTRATADA** obriga-se a, sempre que aplicável, atuar em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física identificada ou identificável ("Dados Pessoais") e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais"), bem como seguir as instruções informadas pelo **CONTRATANTE** quanto ao tratamento dos Dados Pessoais que teve acesso em função do presente Termo.

3.2.A **CONTRATADA** compromete-se a auxiliar o **CONTRATANTE**: i) com a suas obrigações judiciais ou administrativas, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e ii) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas;

3.3.Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da relação estabelecida com o **CONTRATANTE** ou na execução das atividades ligadas a este Termo, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade da relação negocial conforme as disposições acordadas, a **CONTRATADA** concorda em notificar formalmente este fato o **CONTRATANTE**, que terá o direito de resolver a relação negocial sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

4. DISPOSIÇÕES GERAIS

4.1. A **CONTRATADA** declara estar ciente de que o manuseio inadequado das Informações Confidenciais, sua divulgação ou revelação não autorizada a quaisquer terceiros representarão, por si só, prejuízo ao patrimônio, à imagem e reputação do **CONTRATANTE**, e implicará em sua responsabilização civil ou criminal, de acordo com a violação verificada, obrigando-se ao ressarcimento das perdas e danos decorrente.

4.2. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a **CONTRATADA**, além de sanções penais cabíveis, ao pagamento o **CONTRATANTE** e a terceiros pelas perdas e danos, diretos e indiretos, decorrentes do evento de descumprimento, facultada ainda o **CONTRATANTE** a rescisão do presente Termo e demais acordos que estiverem vigentes com a **CONTRATADA**.

4.3. Este Termo não impõe obrigações à **CONTRATADA** com relação às Informações Confidenciais que (i) já sejam lícita e comprovadamente de conhecimento da **CONTRATADA** anteriormente à da sua divulgação pelo **CONTRATANTE**; (ii) sejam ou venham a se tornar de conhecimento público, sem qualquer intervenção da **CONTRATADA** e (iii) sejam divulgadas à **CONTRATADA** por qualquer terceiro que as detenham em legítima posse, sem que isto constitua violação de dever de confidencialidade previamente assumido com o **CONTRATANTE**.

4.4. Se a **CONTRATADA** vier a ser obrigada a divulgar, no todo ou em parte, as Informações Confidenciais por qualquer ordem judicial ou autoridade governamental competente, a **CONTRATADA** poderá fazê-lo desde que notifique imediatamente o **CONTRATANTE**, para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4.5. Se a **CONTRATADA**, na hipótese aqui tratada, tiver que revelar as Informações Confidenciais, divulgará tão somente a informação que foi legalmente exigível e envidará seus melhores esforços para obter tratamento de segredo para quaisquer Informações Confidenciais que revelar, nos precisos dispositivos deste Termo e da Lei.

4.6.A **CONTRATADA** concorda que não deve se opor à cooperação ou empenho de esforços com o **CONTRATANTE** para auxiliar na adoção das medidas judiciais



competentes, sendo certo que nada poderá ser exigido ou solicitado a **CONTRATADA** que não esteja dentro dos estritos limites legais.

4.7. O presente Termo permanecerá em vigor por prazo indeterminado, independentemente da formalização de qualquer negócio entre as Partes.

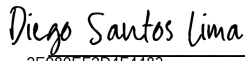
4.8. Quaisquer alterações a este Termo somente terão validade e eficácia se forem devidamente formalizadas através de termo aditivo firmado entre as Partes.

4.9. O presente Termo será interpretado pela Legislação da República Federativa do Brasil e as Partes desde já elegem o Foro da Cidade de Belém, Estado do Pará, para dirimir qualquer controvérsia oriunda deste instrumento, salvo disposição específica pela legislação aplicável.

E por estarem 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.

DocuSigned by:

2E980EF2D4F4483... **DIEGO SANTOS LIMA**
Diretor Corporativo – DICOP

QOS TECNOLOGIA E SERVIÇOS LTDA

DocuSigned by:

2B667A01777F7948... **WALTER FERNANDES PINTO NETO**
Sócio Administrador

ANEXO II

TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO

Por este instrumento particular, a **CONTRATADA** compromete-se a cumprir integralmente as disposições da Política Anticorrupção, Política de Responsabilidade



Socioambiental e da Política de Relacionamento com Fornecedores do **CONTRATANTE** da qual tomou conhecimento neste ato por meio da leitura da cópia que lhe foi disponibilizada.

E, para fiel cumprimento desse compromisso, a **CONTRATADA** declara e garante que nem ela, diretamente ou por intermédio de qualquer subsidiária ou afiliada, e nenhum de seus diretores, empregados ou qualquer pessoa agindo em seu nome ou benefício, realizou ou realizará qualquer ato que possa consistir em violação às proibições descritas (i) na Lei n. 12.846/2013, doravante denominada “Lei Anticorrupção Brasileira”, (ii) na Lei Contra Práticas de Corrupção Estrangeiras de 1977 dos Estados Unidos da América (*United States Foreign Corrupt Practices Act of 1977*, 15 U.S.C. §78-dd-1, et seq., conforme alterado), doravante denominada FCPA, (iii) e nas convenções e pactos internacionais dos quais o Brasil seja signatário, em especial a Convenção da OCDE sobre Combate à Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, a Convenção das Nações Unidas contra a Corrupção e a Convenção Interamericana contra a Corrupção – OEA, todas referidas como “Normas Anticorrupção”, incluindo pagamento, oferta, promessa ou autorização de pagamento de dinheiro, objeto de valor ou mesmo de valor insignificante mas que seja capaz de influenciar a tomada de decisão, direta ou indiretamente, a:

- a) Qualquer empregado, oficial de governo ou representante de, ou qualquer pessoa agindo oficialmente para ou em nome de uma entidade de governo, uma de suas subdivisões políticas ou uma de suas jurisdições locais, um órgão, conselho, comissão, tribunal ou agência, seja civil ou militar, de qualquer dos indicados no item anterior, independente de sua constituição, uma associação, organização, empresa ou empreendimento controlado ou de propriedade de um governo, ou um partido político (os itens A a D doravante denominados conjuntamente autoridade governamental);
- b) Oficial legislativo, administrativo ou judicial, independentemente de se tratar de cargo eletivo ou comissionado;
- c) Oficial de, ou indivíduo que ocupe um cargo em, um partido político;
- d) Candidato ou candidata a cargo político;
- e) Um indivíduo que ocupe qualquer outro cargo oficial, cerimonial, comissionado ou herdado em um governo ou qualquer um de seus órgãos; ou
- f) Um oficial ou empregado(a) de uma organização supranacional (por exemplo, Banco Mundial, Nações Unidas, Fundo Monetário Internacional, OCDE) (doravante denominado oficial de governo);
- g) Ou a qualquer pessoa enquanto se saiba, ou se tenha motivos para crer que qualquer porção de tal troca é feita com o propósito de:
 - g.1) Influenciar qualquer ato ou decisão de tal oficial de governo em seu ofício, incluindo deixar de realizar ato oficial, com o propósito de assistir o **CONTRATANTE** ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro;
 - g.2) Assegurar vantagem imprópria;
 - g.3) Induzir tal oficial de governo a usar de sua influência para afetar ou influenciar qualquer ato ou decisão de uma autoridade governamental com o propósito de assistir o **CONTRATANTE** ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro; ou
 - g.4) Fornecer um ganho ou benefício pessoal ilícito, seja financeiro ou de outro valor, a tal oficial de governo.

A **CONTRATADA**, inclusive seus diretores, empregados e todas as pessoas agindo em seu nome ou benefício, com relação a todas as questões afetando o **CONTRATANTE** ou seus negócios, se obrigam a:

- a) Permanecer em inteira conformidade com as Leis Anticorrupção, e qualquer legislação antissuborno, anticorrupção e de conflito de interesses aplicável, ou qualquer outra

**CONTRATO Nº 2025/154-01**

legislação, regra ou regulamento de propósito e efeito similares, abstendo-se de qualquer conduta que possa ser proibida a pessoas sujeitas às Leis Anticorrupção;

b) Tomar todas as precauções necessárias visando prevenir ou impedir qualquer incompatibilidade ou conflito com outros serviços ou com interesses do **CONTRATANTE**, o que inclui o dever de comunicar as relações de parentesco existentes entre os colaboradores da **CONTRATADA** e do **CONTRATANTE**; e

c) Observar, no que for aplicável, o Programa de *Compliance* do **CONTRATANTE**, sobre o qual declara ter pleno conhecimento.

Entendendo que é papel de cada organização fomentar padrões éticos e de transparência em suas relações comerciais, o **CONTRATANTE** incentiva a **CONTRATADA**, caso ainda não possua, a elaborar e implementar programa de integridade próprio, observando os critérios estabelecidos no Decreto n. 8.420/2015, revogado pelo Decreto nº 11.129/202.

Caso a **CONTRATADA** ou qualquer de seus colaboradores venha a tomar conhecimento de atitudes ilícitas ou suspeitas, especialmente se referentes à violação das Leis Anticorrupção, deve informar prontamente ao **CONTRATANTE**, por meio do Canal de Denúncias canal.denuncia@basa.com.br e no telefone **08007441000**.

Fica esclarecido que, para os fins do Contrato, a **CONTRATADA** é responsável, perante o **CONTRATANTE** e terceiros, pelos atos ou omissões de seus colaboradores.

Por fim, a **CONTRATADA** declara estar ciente de que a fiel observância deste instrumento é fundamental para a condução das atividades inerentes ao Contrato maneira ética e responsável constituindo falta grave, passível de imposição de penalidade, qualquer infração, no disposto deste instrumento.

Belém-PA, data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

DocuSigned by:

2E980EF2D4F4483... **DIEGO SANTOS LIMA**
Diretor Corporativo – DICOP

QOS TECNOLOGIA E SERVIÇOS LTDA

DocuSigned by:

2B66AD11AF4946... **WALTER FERNANDES PINTO NETO**
Sócio Administrador

ANEXO III**TERMO DE REFERÊNCIA****1. OBJETO**

- 1.1** O presente termo tem por objeto a contratação de empresa para o fornecimento de **Solução de Governança e Administração de Identidade**, conhecida no mercado como IGA (Identity Governance and Administration), contemplando os serviços de implantação, treinamento e suporte e operação da solução, conforme diretrizes,



condições, quantidades e exigências estabelecidas neste Termo de Referência e seus anexos, pelo período de 36 (trinta e seis) meses renováveis até o prazo legal.

- 1.2** As empresas participantes, doravante denominadas LICITANTES, deverão ser capazes de executar todo o conjunto de serviços, objeto da presente Licitação.
- 1.3** Não será aceita a participação de consórcios e sublocação/subcontratação de serviços em parte ou de modo global para a execução do objeto deste certame.
- 1.4** Esta contratação será realizada via sistema de registro de preço (SRP), amparado no Decreto nº 11.462/2023 e 13.303/2016.
- 1.5** Da Ata de Registro de Preços

- 1.5.1** A contratação será realizada via Sistema de Registro de Preços visando a economicidade da contratação, uma vez que a quantidade de identidades a serem governadas pelo Banco da Amazônia (BASA) trata-se de uma estimativa. Devido à ausência de base histórica de solução de IGA e divergências de dados internos de contas de usuários, poderá haver necessidade de incremento do número de licenças inicialmente contratadas. Ainda, a solução de CIEM somente será contratada quando o BASA implantar os serviços de IaaS (Infraestrutura como Serviço) em nuvem pública.
- 1.5.2** A efetivação do registro de preços é necessária, visto que propiciará ao BASA firmar antecipadamente a ata por via das quais procederá, oportuna e convenientemente, sem obrigatoriedade de consumo total.
- 1.5.3** O quantitativo previsto neste termo de referência e seus anexos prevê a aquisição máxima a ser realizada pelo BASA, porém, inicialmente, serão adquiridas quantidades menores, garantindo a economicidade da contratação e em conformidade com as melhores práticas recomendadas pelo Tribunal de Contas da União (TCU).
- 1.5.4** Nesse sentido, prevê-se a contratação imediata de 4.083 licenças da solução de IGA, bem como sua implantação, treinamento, serviço de suporte e operação da solução e 1000 USTs de serviços técnicos especializados em governança de identidade.

2. JUSTIFICATIVA DA CONTRATAÇÃO

- 2.1** O Banco da Amazônia passa por um momento de avaliação e adequação às novas práticas, conceitos e tecnologias adotados no mercado. Para ter sucesso nessas iniciativas, é necessário que a empresa possua maturidade no processo de gestão de acessos lógicos. Um dos primeiros passos para atingir este requisito é detectar falhas nos controles relacionados ao processo e, assim, amadurecer suas práticas e processos internos.
- 2.2** Isto posto, cabe destacar que o Banco da Amazônia utiliza, atualmente, o sistema AMAZONSEGU como ferramenta de autorização e controle de acesso de seus funcionários e colaboradores. Tal sistema foi desenvolvido para a empresa e utiliza uma filosofia já defasada e que não atende as melhores práticas e requisitos normativos. Nesse contexto, durante o 2º semestre de 2020, a auditoria independente apontou fragilidades no processo de controle de acesso, com destaque para a ausência de mapeamento de funções conflitante e falhas no processo de revisão periódica dos perfis de acesso.



- 2.3** Conforme identificado pela auditoria e confirmado pela Gerência Executiva de Segurança Corporativa (GESEC), o processo executado no Banco não é suficiente para conter os riscos referentes à segregação de funções e concessão de acessos inadequados. Por conseguinte, os estudos técnicos preliminares indicaram como solução do problema a implantação de uma ferramenta de Governança e Administração de Identidade (IGA – Identity Governance and Administration).
- 2.4** O Gartner define IGA como uma solução para gerenciar o ciclo de vida da identidade digital e controlar o acesso do usuário em ambientes locais e na nuvem. Para conseguir isso, as ferramentas IGA agregam e correlacionam dados díspares de identidade e direitos de acesso que são distribuídos por todo o cenário de TI para aprimorar o controle sobre o acesso humano e de máquinas. O objetivo da IGA é gerenciar a complexa gama de direitos de acesso (para funções e associações de grupos, por exemplo) e repositórios de identidade dentro das organizações, tanto no local quanto na nuvem.
- 2.5** Ainda segundo o Gartner, para ser categorizado como uma “suíte IGA”, todos os recursos padrão e obrigatórios devem estar presentes. Ferramentas que fornecem recursos essenciais e cinco ou mais recursos padrão podem ser chamadas de “soluções IGA leves”, que não atendem a necessidade do BASA.
- 2.6** Nessa perspectiva, a contratação de uma solução de IGA é fundamental para que o BASA esteja em conformidade com as boas práticas de segurança e garanta que o processo de controle de acesso é suficientemente moderno e adequado para receber os novos sistemas bancários que serão implantados no projeto corporativo em curso.
- 2.7** Com essa contratação, visa-se a proteção contra acessos não autorizados, a conformidade com os requisitos legais e de auditoria, a redução de riscos de quebras de confidencialidade e integridades das informações, a redução de fraudes e perdas oriundas da materialização dos riscos do processo de controle de acesso, a melhoria da eficiência operacional, com a redução de custo com mão de obra de service desk e maior agilidade pro usuário final nos processos de troca, desbloqueio e reset de senhas.
- 2.8** Esses fatores demonstram a importância de uma solução de gestão de identidade para proteger os ativos da empresa e garantir a integridade das operações, contribuindo diretamente para o sucesso e a sustentabilidade da organização.
- 2.9** A contratação de uma solução de IGA é um investimento estratégico que oferece benefícios significativos em termos de segurança, eficiência, conformidade, e experiência do usuário. Além disso, ao proteger os ativos do BASA e garantir a integridade das operações, essa solução contribui diretamente para o sucesso e a sustentabilidade da organização.

3. DESCRIÇÃO DO SERVIÇO

- 3.1** O conjunto de serviços objeto da presente licitação é composto pelos itens descritos na tabela a seguir:



Grupo 1			
Item	Descrição	Unidade de Medida	Quantidade
01	Serviço de subscrição anual da solução de IGA	Identidade	5000
02	Serviço de subscrição anual do módulo de CIEM	Identidade	200
03	Serviço de implantação da solução de IGA	Serviço	01
04	Serviço de suporte e operação da solução	Mês	36
05	Serviço de capacitação na solução de IGA	Turma	01
06	Serviços técnicos especializados em governança de identidade	UST	5000

3.2 Justificativa para o não parcelamento do objeto:

3.2.1.1 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 sobre maneira mais complexa, além de impossibilitar uma execução satisfatória. Logo, os itens devem ser licitados em um lote único e serem entregues por uma única empresa CONTRATADA, visando tornar mais eficaz o controle das entregas, a prestação de serviços e a gestão do contrato.

3.3 Para fins de execução do contrato, a licitante vencedora deverá atender aos seguintes requisitos técnicos, incluindo outras previsões constantes neste Termo de Referência.

3.4 Item 1 e 2 - Serviço de subscrição anual da solução de IGA e do módulo de CIEM

3.4.1 As especificações técnicas detalhadas das soluções são apresentadas no Anexo I-A - Requisitos Técnicos Da Solução De Governança E Administração De Identidade, do presente Termo de Referência, no qual devem ser respeitadas as capacidades mínimas requeridas e que, no momento de contingência ou indisponibilidade de um equipamento ou software, os produtos alocados suportem, sem degradação ou perda de performance, todos os requisitos técnicos exigidos.

3.4.2 Todos os requisitos da contratação devem ser entregues licenciados e palavras como: “deve”, “permite”, “suporta”, “efetua”, “proporciona”, “possui” e etc. significam que a funcionalidade deve ser entregue operacional, sem ônus adicional à CONTRATANTE.

3.4.3 Todas as capacidades são especificadas em seu requisito mínimo, podendo ser entregue capacidade superior. Todos os requisitos devem garantir a compatibilidade às versões especificadas e superiores.

3.4.4 As soluções deverão ser fornecidas em sua última versão estável, atualizada pelo respectivo fabricante e não constar, no momento da apresentação da



proposta, em listas de End-of-Life, End-of-sale ou End-of-Support do fabricante ou, ainda, em qualquer relatório referente à existência de data futura de fim de fornecimento, garantia ou assistência técnica. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Para aferição, a CONTRATADA deverá apresentar documentação referente ao Roadmap da solução, com informações relativas ao ciclo de vida (End-of-Life, End-of-sale e End-of-Support).

3.4.5 Não serão aceitas soluções de segurança customizadas para o BASA. Serão aceitas somente aquelas soluções que fizerem parte do portfólio de soluções oferecidas pelos fabricantes para o mercado corporativo.

3.4.6 A solução deverá ser fornecida na modalidade SaaS (Software as a Service) baseada em cloud.

3.4.7 A CONTRATADA deverá fornecer suporte direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto, conforme previsto neste Termo de Referência e seus anexos.

3.4.8 O serviço de assistência técnica do fabricante deve prover, durante o prazo contratado:

3.4.8.1 Correções de falhas reportadas pelo BASA que prejudiquem o ambiente de produção;

3.4.8.2 Acesso à base de conhecimento e fóruns no site do fabricante pelo BASA;

3.4.8.3 Serviço de abertura de ticket para endereçamento de eventuais problemas no software.

3.4.9 O software licenciado deve estar coberto por contrato de atualização de versão pelo prazo do contrato a contar da data da liberação da licença.

3.4.10 Caso o software fornecido seja descontinuado pelo fabricante, ele deve ser substituído por software equivalente pela CONTRATADA.

3.5 Item 3 - Serviço de Implantação da solução de IGA

3.5.1 O serviço de implantação da solução de IGA compreende o planejamento da implantação, instalação e configuração da solução, além da integração da solução com os seguintes sistemas:

3.5.1.1 Sistema de Gestão de Pessoas (Oracle PeopleSoft);

3.5.1.2 Active Directory;

3.5.1.3 Microsoft Office365;

3.5.1.4 Solução de PAM (Beyondtrust);

3.5.2 A etapa de implantação deverá ter duração máxima de 150 (cento e cinquenta) dias, contados a partir da reunião de kick-off e terá seu término com a emissão do TAD (Termo de Aceitação Definitivo).



- 3.5.3** Em até 5 (cinco) dias úteis após a assinatura do contrato, deverá ser realizada, de forma remota, a reunião de kick-off do projeto que será agendada conforme disponibilidade de agenda da equipe do Banco.
- 3.5.4** Na reunião de kick-off, a CONTRATADA deverá apresentar a documentação comprobatória da qualificação técnica dos profissionais que atuarão na implantação da solução.
- 3.5.5** Dentre os profissionais alocados na implantação, a CONTRATADA deverá indicar, no mínimo:
- 3.5.5.1** 1 (um) Gerente de Projetos: líder e responsável pela entrega dos serviços e pela implantação e integração da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital.
 - 3.5.5.2** 1 (um) Consultor especializado em Governança de Identidades: responsável por apoiar as atividades de caráter técnico, bem como pela instalação, configuração, testes, ativação e documentação as-built do projeto.
 - 3.5.5.3** 1 (um) Analista de Negócios: responsável por executar as atividades de caráter de negócio, como levantamentos, análise de processos, etapas, e pela documentação do projeto, traduzindo as questões técnicas para a visão de negócios.
 - 3.5.5.4** 1 (um) Especialistas em Operação e Suporte da Solução: deverá ser o mesmo profissional que executará o Serviço de Suporte e Operação das soluções (item 4). Dessa forma, busca-se uma mudança fluida da fase de implantação para a fase de operação, com o menor impacto possível para o BASA.
- 3.5.6** Todos os profissionais alocados na implantação deverão atender os requisitos de capacidade técnica definidos no item 4 – Qualificação Técnica dos profissionais da CONTRATADA deste Termo de Referência.
- 3.5.7** Todas as atividades relacionadas à implantação ocorrerão sob a responsabilidade e expensas da CONTRATADA, sem nenhum ônus adicional para o Banco, cabendo a este somente o apoio técnico e a avaliação dos resultados, nos termos previstos no Edital.
- 3.5.8** Por instalação, configuração, integração e ativação entende-se todos os procedimentos relacionados à implantação e configuração (lógica), parametrização e testes de quaisquer componentes da solução ofertada, além de outras integrações com o ambiente do Banco necessárias, de modo a garantir o pleno funcionamento da solução.
- 3.5.9** A CONTRATADA deve criar e manter atualizada a documentação das atividades, dos processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, atas de reuniões, de modo a compor uma documentação final da implantação a ser entregue ao Banco no final do processo;
- 3.5.10** A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de apoio a customização e implementação da solução, objeto do Edital. Caso o diagnóstico aponte para problemas não relacionados aos serviços de apoio a customização e



implementação da solução, o Banco deverá executar os referidos procedimentos, desde que devidamente comprovados pela CONTRATADA, e a critério do Banco.

- 3.5.11** A CONTRATADA deve, às suas expensas, alocar toda a equipe que irá instalar, configurar, integrar e executar os serviços de implantação descritos no Edital que deverá atuar de forma presencial ou remota, em horários agendados com a equipe do BASA cumprindo as políticas e diretrizes de segurança do Banco.
- 3.5.12** As atividades de instalação e configuração inicial da solução, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição do BASA.
- 3.5.13** A CONTRATADA deverá apresentar ao BASA, em reunião própria, um plano de implantação que balizará o acompanhamento de todo o projeto de implantação, em formato Microsoft Project, detalhando todas as fases, atividades, ações, recursos envolvidos (humanos e materiais), prazos, interdependências entre fases, atividades e ações, linha crítica temporal da implantação e quais serão os produtos gerados para cada fase, atividade e ação.
- 3.5.14** O plano de implantação deverá ser entregue em até 5 (cinco) dias úteis a contar da data de realização da reunião de kick-off.
- 3.5.15** A CONTRATADA deve submeter o Plano de Implantação à homologação por parte do Banco, reservando-se este o direito de requerer os ajustes necessários, observadas as melhores práticas amplamente aceitas no mercado e a realidade de seu ambiente;
- 3.5.16** A CONTRATADA deve implementar, no Plano de Implantação, todos os ajustes que venham a ser solicitados pelo Banco e apresentar a nova versão;
- 3.5.17** A entrega da versão final do plano deverá ser realizada em até 5 (cinco) dias úteis a contar da data da solicitação dos ajustes por parte do Banco.
- 3.5.18** O serviço de implantação da solução deverá abranger, no mínimo, todas as atividades abaixo elencadas.
 - 3.5.18.1** Instalação:
 - 3.5.18.1.1.** Ativação das licenças que compõe a solução;
 - 3.5.18.1.2.** Instalação de todos os módulos licenciados e conectores no ambiente virtualizado do BASA;
 - 3.5.18.1.3.** Configuração dos conectores;
 - 3.5.18.1.4.** Integração com a Base Autoritativa: Oracle PeopleSoft;
 - 3.5.18.1.5.** Implementação do Ciclo de Vida das Identidades dos colaboradores do BASA, incluindo:
 - 3.5.18.1.5.1.** Configuração do padrão visual da plataforma (Look'n Feel BASA);



- 3.5.18.1.5.2.** Configuração da Autenticação SSO com MFA provido pelo BASA;
- 3.5.18.1.5.3.** Ciclo de Vida Funcionários – Admissão;
- 3.5.18.1.5.4.** Ciclo de Vida Funcionários – Movimentação;
- 3.5.18.1.5.5.** Ciclo de Vida Funcionários – Desligamento;
- 3.5.18.1.5.6.** Ciclo de Vida Funcionários - Férias / Afastamentos;
- 3.5.18.1.5.7.** Ciclo de Vida Funcionários - Regra de Exceção de Férias;
- 3.5.18.1.5.8.** Ciclo de Vida Funcionários – Readmissão;
- 3.5.18.1.5.9.** Ciclo de Vida Terceiros – Admissão;
- 3.5.18.1.5.10.** Ciclo de Vida Terceiros – Movimentação;
- 3.5.18.1.5.11.** Ciclo de Vida Terceiros - Expiração de Usuários;
- 3.5.18.1.5.12.** Ciclo de Vida Terceiros – Desligamento;
- 3.5.18.1.5.13.** Ciclo de Vida Terceiros - Férias / Afastamentos;
- 3.5.18.1.5.14.** Ciclo de Vida Terceiros - Exceção de Férias ;
- 3.5.18.1.5.15.** Processo de aprovação até 3 passos;
- 3.5.18.1.5.16.** Configuração de Regra de definição de OU no Active Directory;
- 3.5.18.1.5.17.** Regra de Movimentações;
- 3.5.18.1.5.18.** Regra de Criação de Login para funcionário;
- 3.5.18.1.5.19.** Regra de Criação de Login para terceiro;
- 3.5.18.1.5.20.** Regra de Criação de E-mail para funcionário;
- 3.5.18.1.5.21.** Regra de Criação de E-mail para terceiro;
- 3.5.18.1.5.22.** Regra de Criação de Caixa de E-mail;
- 3.5.18.1.5.23.** Regra de Readmissão/Internalização;
- 3.5.18.1.5.24.** Configuração do Processo de Recertificação de Usuários Ativos;
- 3.5.18.1.5.25.** Configuração do Processo de Certificação de Usuários;
- 3.5.18.1.5.26.** Configuração do Processo de Recertificação de Composição de Perfis;
- 3.5.18.1.5.27.** Configuração do Processo de Recertificação de SoD;
- 3.5.18.1.5.28.** Configuração do Regra de redirecionamento de aprovações e recertificações de usuários indisponíveis;
- 3.5.18.1.5.29.** Configurações de Notificações dos Processos;



3.5.18.1.6. Implantação do Fluxos de Gestão de Identidades e Acessos, incluindo: Solicitação de Acessos, Aprovação do Acesso, Configuração do Autosserviço de Reset e Desbloqueio;

3.5.18.1.7. Integração da solução com o Active Directory para permitir a gestão das contas por meio do IGA, incluindo o gerenciamento de senhas;

3.5.18.1.8. Integração da solução com a ferramenta de ITSM do BASA, para abertura de incidentes;

3.5.18.1.9. Integração da solução de IGA com a solução de PAM;

3.5.18.1.10. Integração da solução de IGA com o Red Hat Single Sign-On (RHSSO);

3.5.18.1.11. Configuração de relatórios para Governança;

3.5.18.1.12. Configuração de Relatórios de Auditoria;

3.5.18.1.13. Cadastramento dos usuários da equipe do BASA gestão de contrato para gestão da solução;

3.5.18.1.14. Configuração dos perfis de acesso dos usuários administradores;

3.5.18.1.15. Configuração de envio de logs para o SIEM do BASA.

3.5.18.2 Homologação

3.5.18.2.1 Após o recebimento do comunicado de conclusão, o Banco realizará encontro de homologação para decidir sobre o aceite de finalização da macro fase. Este encontro contará com a presença mínima dos seguintes profissionais:

3.5.18.2.1.1. Gerente de Projeto (CONTRATADA);

3.5.18.2.1.2. Representante da equipe técnica (CONTRATADA);

3.5.18.2.1.3. Representante da equipe técnica (BANCO);

3.5.18.2.2 Em caso de não ser aceita a conclusão, o CONTRATADO ficará obrigado a adotar medidas imediatas visando corrigir quaisquer situações que possam estar impedindo a devida finalização da macro fase.

3.5.18.3 Período de funcionamento experimental (PFE).

3.5.18.3.1 Após a homologação da solução, será iniciado o período de funcionamento experimental (PFE) no qual a solução será colocada em operação no ambiente de produção com aprofundamento da verificação das características funcionais, sistêmicas e de operação.

3.5.18.3.2 O PFE terá duração de até 15 (quinze) dias.

3.5.18.3.3 Durante o PFE, deverão ser eliminadas todas as pendências de qualquer natureza (instalação, configuração, migração, ativação, funcionamento e outras) que porventura existirem. Logo após, iniciará o Período Sem Falhas (PSF), descrito a seguir.



3.5.18.3.4 O Período Sem Falhas (PSF) é parte do PFE no qual a solução contratada não deverá apresentar falhas de qualquer natureza ou quaisquer outras condições em desacordo com as exigências técnicas do Edital.

3.5.18.3.5 Toda vez que for detectada uma nova falha ou condição em desacordo com as exigências técnicas do Edital, o PFE será reiniciado.

3.5.18.3.6 O Banco definirá o encerramento desta etapa através de comunicação formal ao CONTRATADO, permitindo o avanço dos trabalhos para a etapa seguinte. Concluída esta fase, o Banco emitirá o TERMO DE ACEITAÇÃO DEFINITIVO DA SOLUÇÃO (TAD).

3.5.18.3.7 O Termo de Aceitação Definitiva será emitido após a efetiva implantação de todos os componentes do serviço de apoio à customização e implementação da solução contratada, integrados ao ambiente tecnológico do Banco.

3.5.18.3.8 O TAD não isenta o CONTRATADO das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas pelos serviços. A emissão do TAD não terá caráter de atestado de capacidade técnica.

3.5.18.3.9 Somente após a emissão do TAD deverá ser iniciado o período do Serviço de Suporte e Operação da solução.

3.5.18.3.10 Durante o PFE, deverá ser fornecido o documento de as-built do projeto de implantação, contendo, no mínimo, as seguintes informações:

3.5.18.3.10.1. Descrição dos serviços implantados;

3.5.18.3.10.2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

3.5.18.3.10.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

3.5.18.3.10.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

3.5.18.3.10.5. Definição de responsabilidades;

3.5.18.3.10.6. Decisões de projeto;

3.5.18.3.10.7. Recomendações;

3.5.18.3.10.8. Apresentação da solução e operação;

3.5.18.3.10.9. Scripts de operação, incluindo desligamento e ligamento, switch over, acionamento do equipamento de contingência, quando necessário;

3.5.18.3.10.10. Procedimentos para abertura e atendimento a chamados;

3.5.18.3.10.11. Procedimentos de recuperação de equipamentos;

3.5.18.3.10.12. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

3.5.18.3.10.13. Rotinas periódicas configuradas;



3.5.18.3.10.14. Documentação dos processos de trabalho associados ao item, em esquema de fluxograma, com definição de responsáveis por cada atividade, prazos de execução, rotinas de atualização e revisão periódica de regras;

3.5.18.3.10.15. Regras implantadas;

3.5.18.3.10.16. Definição de padrões porventura existentes na solução (ex. padrão de nome de regras);

3.5.19 A CONTRATADA deverá manter atualizada toda a documentação gerada e entregue ao CONTRATANTE durante a vigência do contrato.

3.5.20 A CONTRATADA deverá, quando necessário, realizar manutenção e atualização de todos entregáveis já executados.

3.5.21 A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados à implantação dos serviços. Caso o diagnóstico aponte para problemas não relacionados à implantação dos serviços, o BASA deverá executar os referidos procedimentos, desde que devidamente comprovados pela Contratada, e a critério do Banco.

3.6 Item 4 - Serviço de Suporte e Operação das soluções

3.6.1 O serviço de suporte técnico e operação visa apoiar a equipe técnica do BASA a manter e melhorar o gerenciamento da solução, incluindo a customização da solução quando necessário.

3.6.2 A fase de Suporte e Operação da solução será iniciada após a emissão do Termo de Aceitação Definitivo (TAD).

3.6.3 O serviço deverá ser prestado por, no mínimo, 1 (um) Especialista em Operação e Suporte da Solução da CONTRATADA, conforme qualificação técnica definida no item 4.1.3.

3.6.4 O profissional deverá atuar de forma dedicada ao BASA, visando assegurar o cumprimento dos SLAs e pleno conhecimento do ambiente da CONTRATADA.

3.6.5 A prestação dos serviços deve ser baseada em modelo de remuneração em função dos resultados apresentados, em que os pagamentos são realizados após mensuração, avaliação e validação de métricas quantitativas e qualitativas, contendo metas e indicadores de desempenho, com Nível Mínimo de Serviço (NMS), conforme Anexo I-B, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. Assim, os níveis de serviço devem ser registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar a remuneração devida.

3.6.6 O serviço de Suporte Técnico e Operação terá pagamento mensal, pois possui natureza de execução continuada.

3.6.7 O modelo de prestação do serviço deve contemplar as atividades a serem demandadas pelo BASA, tais como abertura de chamados técnicos para



resolução de problemas e de consulta de informações, e aquelas a serem desenvolvidas periodicamente pela empresa, tais como inclusão de sistemas gerenciados, configuração de conectores, criação de identidade sem base autoritativa (terceiros), configuração de regras, criação de políticas e demais parametrizações, realização de buscas, emissão de relatórios, monitoramento da solução e apresentação tempestiva de relatórios, conforme periodicidade e níveis de serviço definidos.

- 3.6.8** A contratada deverá prestar os serviços abaixo no modelo 8x5 (8 horas por 5 dias na semana):
- 3.6.8.1** Atendimento dos chamados abertos no ITSM do BASA pelos usuários internos referentes à serviço de IGA.
 - 3.6.8.2** Atendimentos a dúvidas técnicas quanto ao uso do ambiente;
 - 3.6.8.3** Resolução de eventuais problemas identificados, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes;
 - 3.6.8.4** Implantação e configuração dos conectores, incluindo mapeamento, instalação e documentação do conector nativo.
 - 3.6.8.5** Criação e ativação de conectores para bases de autenticação e/ou autorização, incluindo mapeamento, desenvolvimento, implantação e documentação do novo conector criado para atender à solicitação do BASA.
 - 3.6.8.6** Criação e manutenção de regras;
 - 3.6.8.7** Criação e manutenção de políticas de SoD através da importação de políticas e matriz de perfis providos pelo BASA (no formato XLSX), na solução de IGA para gestão de acesso às aplicações integradas;
 - 3.6.8.8** Análise de alertas;
 - 3.6.8.9** Parametrização da solução, de acordo com as regras e políticas disponíveis e adequadas às necessidades do BASA.
 - 3.6.8.10** Criação de identidades sem base autoritativa (ex: terceiros);
 - 3.6.8.11** Realização de buscas;
 - 3.6.8.12** Elaboração e emissão de relatórios;
 - 3.6.8.13** Criação e acompanhamento de campanhas de revisão de acesso.
 - 3.6.8.14** Apoio dos gestores dos sistemas em relação as campanhas de revisão de acesso.
 - 3.6.8.15** Proposição de melhorias nos processos relacionados ao ciclo de vida implementado, incluindo análise, implantação e documentação das melhorias propostas nos processos do ciclo de vidas implementados.
 - 3.6.8.16** Proposição de melhorias de novas política de conformidade.
 - 3.6.8.17** Implantação e configuração do módulo de CIEM, se contratado.
 - 3.6.8.18** Realização de transferência de conhecimento, acerca das execuções realizadas e conhecimentos sobre o uso da solução e procedimentos realizados.
 - 3.6.8.19** Identificação de melhorias e respectivo tratamento (melhoria de parametrização).
 - 3.6.8.20** Implementação de políticas de segregação de funções previamente mapeadas.



CONTRATO Nº 2025/154-01

- 3.6.8.21** Interação com a equipe técnica do BASA responsável pela configuração de ferramentas que eventualmente se integrarão com a solução ofertada, como, por exemplo, firewalls, proxies, Microsoft Active Directory, dentre outros.
- 3.6.8.22** Instalação, reinstalação e desinstalação de quaisquer componentes da solução.
- 3.6.8.23** Sugestões de parametrizações baseadas em boas práticas e na experiência em outros projetos;
- 3.6.8.24** Elaboração de relatórios executivos, gerenciais e operacionais;
- 3.6.8.25** Qualquer tipo de configuração de funcionalidades já suportadas pela solução, a partir da solicitação formal do BASA.
- 3.6.8.26** Quaisquer outras intervenções nos componentes da solução de forma a assegurar o bom funcionamento deles, de acordo com as necessidades do BASA.
- 3.6.8.27** Instalação de patches e correções de vulnerabilidades dos componentes no ambiente do BASA.
- 3.6.9** A contratada deverá prestar os serviços abaixo no modelo 24x7x365 (24 horas por dia, 7 dias na semana por 365 dias do ano):
 - 3.6.9.1** Apoio na administração, gerenciamento e monitoramento da saúde da solução de modo a evitar interrupções e impactos para as operações do BASA;
 - 3.6.9.2** Apoio na sustentação da solução;
 - 3.6.9.3** Apoio na resolução de problemas;
 - 3.6.9.4** Troubleshooting na solução;
 - 3.6.9.5** Instalação de patches e correções de vulnerabilidades dos componentes no ambiente do BASA, quando houver necessidade de janela de GMUD (gestão de mudanças).
- 3.6.10** A CONTRATADA deverá apresentar um conjunto de regras pré-estabelecidas para ativação. Estas regras somente serão implementadas após a aprovação do Banco;
- 3.6.11** A CONTRATADA será responsável pela execução de todas as atividades de administração, manutenção, configuração, suporte e administração da solução;
- 3.6.12** A CONTRATADA deverá utilizar a solução de ITSM do BASA para atendimentos dos chamados relacionados a operação da solução. Não haverá limite mensal para a quantidade de chamados abertos.
- 3.6.13** O acesso do time de operação da CONTRATADA ao ITSM do BASA deverá ocorrer por meio de VPN a ser fornecida pelo BASA.
- 3.6.14** O time de especialista 8x5 da CONTRATADA responsável pela operação terá acesso ao ambiente colaborativo do Office365 do BASA para comunicação com os usuários do BASA, se necessário. As licenças do Office365 serão fornecidas pelo BASA.
- 3.6.15** A CONTRATADA deverá manter atualizados os appliances virtuais dos conectores e demais componentes implantados na infraestrutura do BASA, bem como instalar patches, correções e versões ou releases mais recentes dos softwares.



- 3.6.16** A CONTRATADA deverá executar procedimentos para resolução de problemas relacionados à configuração, atualização, funcionamento e uso dos componentes necessários ao funcionamento dos módulos da solução.
- 3.6.17** A CONTRATADA deverá monitorar, analisar e controlar o desempenho de cada componente da solução fornecida, executando procedimentos para resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos componentes da solução, substituindo-os sem custo adicional ao Banco, caso necessário.
- 3.6.18** A CONTRATADA deverá executar procedimentos para fazer o ajuste fino (tunning) de toda a solução ofertada, adequando-a ao ambiente do Banco e realizando as customizações de configuração necessárias.
- 3.6.19** A CONTRATADA deverá realizar a gerência de segurança da solução fornecida, sendo responsável pela proteção das informações, restringindo o acesso à rede e impedindo o uso incorreto por parte de seus usuários, de forma intencional ou não.
- 3.6.20** A CONTRATADA deverá realizar as operações de administração da solução fornecida para solicitação de criação de contas de acesso para os analistas do BASA, solicitação de registros de auditoria da ferramenta ou outras configurações solicitadas pelo BASA. As solicitações devem ser registradas e realizadas por meio dos canais de suporte do CONTRATADO.
- 3.6.21** A CONTRATADA deverá configurar os perfis de acesso diferenciados, necessários para que os analistas do Banco utilizem todos os serviços contratados. A CONTRATADA deverá fornecer possibilidade de perfis que permitam acesso a qualquer informação armazenada na solução fornecida.
- 3.6.22** A CONTRATADA deve fornecer, sob demanda do Banco, relatório contendo a lista de usuários cadastrados na ferramenta, o perfil de acesso, situação da conta e última data de acesso.
- 3.6.23** A CONTRATADA deverá definir em comum acordo com o Banco o método mais eficiente para a implementação de políticas de IGA, de forma a não prejudicar o trabalho dos colaboradores do Banco. O procedimento proposto só será aceito após avaliado pelo Banco;
- 3.6.24** A CONTRATADA deverá realizar a configuração das regras na solução fornecida, de forma proativa ou sempre que solicitada pelo Banco, permitindo a detecção de ameaças ao ambiente do Banco.
- 3.6.25** A CONTRATADA deverá determinar a causa e prover solução para os chamados abertos junto ao(s) responsável(is) pela prestação dos serviços de suporte técnico e manutenção (se o próprio Contratado ou sua(s) filial(ais) ou representante(s) ou credenciada(s)).
- 3.6.26** O BASA poderá solicitar, a qualquer momento, a implementação de novas regras na solução fornecida, baseadas na necessidade do negócio. A CONTRATADA deverá avaliar os requisitos técnicos necessários e operacionalizar as regras na



solução. As solicitações devem ser registradas e realizadas por meio da solução de ITSM do BASA.

- 3.6.27** A CONTRATADA deverá realizar a configuração dos painéis e relatórios de monitoramento na solução fornecida, de forma proativa ou sempre que solicitada pelo Banco;
- 3.6.28** A CONTRATADA deverá configurar um conjunto básico de painéis, contendo indicadores definidos de acordo com suas bases de conhecimento próprias, customizadas para o ambiente do BASA.
- 3.6.29** O BASA poderá solicitar, a qualquer momento, a implementação de painéis ou relatórios para apresentar indicadores próprios definidos baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar os painéis na solução. As solicitações devem ser registradas e realizadas por meio dos canais de suporte do CONTRATADO;
- 3.6.30** O BASA poderá solicitar acesso a quaisquer dos painéis ou relatórios configurados na ferramenta, de acordo com o nível de acesso que o Banco definirá para cada um de seus analistas autorizados a acessar a ferramenta fornecida;
- 3.6.31** O BASA poderá solicitar perfil de acesso aos seus analistas que possibilitem a construção de painéis e relatórios customizados, visualização e a filtragem dos eventos e alertas na ferramenta ofertada;
- 3.6.32** A CONTRATADA deverá disponibilizar um canal para abertura dos chamados referentes aos serviços a serem realizados pelo time de 24x7 (item 3.6.9). O canal deverá estar disponível, em regime 24x7x365 (24 horas por dia, 7 dias na semana, 365 dias no ano), com atendimento em língua portuguesa, ou por meio de portal de serviços na internet.
 - 3.6.32.1** No momento de abertura de chamados, deve ser fornecido ao BASA um número único de identificação da demanda, com classificação conforme definição do BASA. Assim, deve ser encaminhada uma notificação, contendo as informações de registro do chamado, para endereço eletrônico de e-mail do BASA.
 - 3.6.32.2** O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe do BASA.
 - 3.6.32.3** Em casos de chamados abertos via telefone, o sistema deverá disponibilizar um número local onde o BASA possui sua sede (Belém-PA), evitando custos desnecessários, onde o número deverá ser disponibilizado pela CONTRATADA no formato (091)+(número local) ou 0800, devendo o sistema identificar o número utilizado pré-cadastrado e liberado para abertura de chamados que serão automaticamente abertos e enviados para uma fila de atendimentos apropriada, devendo registrar o horário do momento da ligação como horário de abertura do chamado em questão.
 - 3.6.32.4** Não haverá limite mensal para a quantidade de chamados abertos.
 - 3.6.32.5** A equipe de gestão de contrato do BASA deverá ter acesso ao sistema de controle de chamados da CONTRATADA para fins de acompanhamento e



auditoria de chamados, sendo possível a extração de relatórios compreendendo o período integral do contrato.

- 3.6.33** A CONTRATADA deve realizar os devidos escalonamentos de acordo com a prioridade e nível de atendimento dos chamados, reportados pelo BASA ou pelo sistema de monitoramento da CONTRATADA.
- 3.6.34** Em qualquer mudança na situação de chamados, deve ser encaminhada uma notificação ao BASA, contendo as informações de registro do chamado, para endereço eletrônico de e-mail, inclusive quando houver mudança de status interrompendo a contagem de NMS.
- 3.6.35** O BASA analisará a correteza da resolução do atendimento para então aprovar ou recusar o fechamento dele. Para efeitos de apuração do tempo gasto pela CONTRATADA para a apuração do NMS, serão desconsiderados os períodos em que o BASA estiver responsável por executar ações necessárias para a análise e atendimento da solicitação. Os chamados abertos somente podem ser concluídos e fechados após autorização do BASA.
- 3.6.36** Para que um chamado seja considerado concluído, os serviços executados devem ser adequadamente documentados, evidenciados e arquivados no sistema de controle de chamados. A documentação entregue deve ser simplificada para esclarecer os procedimentos executados e permitir que servidores do BASA possam repetir as ações tomadas posteriormente.
- 3.6.37** Caso seja necessária a elaboração de uma documentação detalhada dos procedimentos executados, incluindo justificativas técnicas, esclarecimentos e gráficos, o BASA pode solicitar sua elaboração por meio de registro de uma solicitação.
- 3.6.38** Considerar-se-á como tempo de resolução, o período líquido compreendido entre o momento de início e a finalização do atendimento, descontado o tempo em que ele ficou pendente de execução por outras equipes do BASA.
- 3.6.39** Toda e qualquer alteração na configuração da solução deverá ocorrer mediante autorização do BASA.
- 3.6.40** O BASA, no momento da implantação da solução, indicará as pessoas que poderão autorizar as referidas alterações.
- 3.6.41** As alterações das configurações deverão ocorrer em horários determinados pelo BASA.
- 3.6.42** A CONTRATADA deverá garantir que o fabricante da solução efetue, em laboratório próprio, os testes necessários antes de implementar qualquer alteração no ambiente cloud, visando evitando impactos negativos nas operações do BASA.
- 3.6.43** A qualquer momento durante o contrato, o BASA poderá solicitar que a CONTRATADA atualize a Documentação técnica de as-built da solução,



incluindo parâmetros de instalação, configuração, arquitetura e topologias implementadas;

3.7 Item 5 - Serviço de Capacitação

3.7.1 A capacitação deverá ser realizada durante a vigência contratual, conforme solicitação do BASA por meio de Ordem de Serviço (OS).

3.7.2 A capacitação deverá ser realizada no horário compreendido entre 08:00 e 18:00 horas, de segunda a sexta-feira, em turno integral ou parcial, conforme carga horária diária e horário definidos pelo BASA.

3.7.3 A capacitação deverá ter carga horária mínima de 8 (oito) horas para uma turma de até 10 alunos, deverá utilizar material autorizado pelo fabricante da solução e poderá ser realizada de forma remota. Se realizada de forma remota, as aulas deverão ocorrer através da ferramenta Microsoft Teams e será gravada pelo BASA.

3.7.4 Instrutor:

3.7.4.1 O instrutor deverá possuir certificação que lhe confira as competências necessárias para ministrar o treinamento. A certificação exigida deve estar válida durante o período de prestação do serviço da capacitação técnica. A entrega da documentação que comprova o atendimento da exigência deverá ser realizada em meio digital e com antecedência mínima de 10 (dez) dias úteis do início da realização da respectiva capacitação. A capacitação técnica só será realizada após a CONTRATADA apresentar a devida comprovação.

3.7.4.2 É vedada a alteração de instrutor sem prévia comunicação e concordância do BASA, estando um eventual substituto sujeito ao mesmo processo de verificação descrito anteriormente.

3.7.4.3 A capacitação técnica deverá ser ministrada em língua portuguesa ou em língua inglesa (mediante autorização pelo BASA).

3.7.5 Disciplinas

3.7.5.1 Para a solução de IGA, a capacitação técnica provida deverá abordar todos os componentes da solução licenciados pelo BASA, abrangendo, no mínimo, os seguintes tópicos:

3.7.5.1.1. Conceitos de IGA e análise em segurança, funcionamento da solução e características do produto.

3.7.5.1.2. Descrição das funcionalidades e navegação em cada módulo da ferramenta e seus modos de funcionamento.

3.7.5.1.3. Configuração de conectores.

3.7.5.1.4. Regras: Definição, desenvolvimento, otimização e customização de regras.

3.7.5.1.5. Dashboards: Descrição das funcionalidades, navegação, criação e customização de dashboards. Análise, busca de dados e definição de incidentes utilizando dashboards.



- 3.7.5.1.6.** Relatórios: Criação, customização, geração e agendamento de relatórios. Funções de filtragem de eventos e construção de métricas para relatórios.
- 3.7.5.1.7.** Campanhas de revisão de acesso: Criação, customização, geração e agendamento.
- 3.7.5.1.8.** Codificação de conectores e integrações com IA.
- 3.7.5.1.9.** Criação de workflow de integração.
- 3.7.5.1.10.** Catálogo de direitos: Descrição das funcionalidades, navegação.
- 3.7.5.1.11.** Configuração de fluxo de autosserviço.
- 3.7.5.1.12.** Criação de formulários web personalizáveis.
- 3.7.5.1.13.** Criação e edição de fluxo de autosserviço
- 3.7.5.1.14.** Customização de atributos das identidades
- 3.7.5.1.15.** Configuração de fluxos de trabalho
- 3.7.5.1.16.** Análise de dados: Descrição das funcionalidades da ferramenta para análise baseada em IA. Definição de buscas e monitoramento de eventos suspeitos, uso de gráficos e filtros avançados para pesquisas de ameaças.
- 3.7.5.1.17.** Funções administrativas básicas: visão geral das configurações da ferramenta e de perfis de acesso, visão geral de monitoramento da ferramenta e solução de problemas, configurações de segurança.

3.7.6 Material didático

- 3.7.6.1** A CONTRATADA deverá fornecer o material didático de acompanhamento detalhado, original do fabricante, preferencialmente em português, contendo todos os assuntos abordados na capacitação. Entende-se como material didático, apostilas, slides de apresentações, manuais, livros textos, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em português (Brasil) do material original do fabricante, será aceito apenas material em inglês.
- 3.7.6.2** O BASA se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes, para realizar capacitações internas de seus empregados.

3.7.7 Avaliação da Capacitação

- 3.7.7.1** Ao término do treinamento, deverá ser realizada uma Avaliação de Reação tendo em vista a medição e avaliação da qualidade da capacitação. O BASA aplicará a Avaliação de Reação, em formato de formulário eletrônico, em todos os treinandos, com o objetivo de avaliar a satisfação com a capacitação.
- 3.7.7.2** Caso a CONTRATADA, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão do BASA, ela poderá utilizar o seu próprio formulário, porém ele não será utilizado para aprovação da capacitação por parte do BASA.
- 3.7.7.3** Quatro fatores serão objeto de avaliação pelo formulário, a dizer: Instrutoria, Material Didático, Conteúdo Programático, Ambiente da Capacitação e Autoavaliação:



CONTRATO Nº 2025/154-01

- 3.7.7.3.1.** Instrutoria - Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto à sua habilidade didático-pedagógica e de interação com a turma.
- 3.7.7.3.2.** Material Didático - Avalia a percepção dos participantes sobre a adequação e clareza do material didático utilizado na capacitação.
- 3.7.7.3.3.** Conteúdo Programático - Avalia a percepção dos treinandos quanto ao equilíbrio entre teoria e prática, nível de profundidade, exemplos de exercícios, aderência e aplicabilidade.
- 3.7.7.3.4.** Autoavaliação - Avalia a percepção dos participantes quanto a aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado.
- 3.7.7.4** Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio da utilização de quatro conceitos, quais sejam: Fraco, Regular, Bom e Excelente.
- 3.7.7.5** Para fins de avaliação dos fatores, na fase de tabulação dos resultados, a cada conceito atribuído a um item, corresponderá um peso. Após o cálculo da média ponderada alcançada por grupo de itens, será obtida a média geral dos fatores correspondentes.
- 3.7.7.6** Na avaliação geral de cada fator, para fins de atribuição do conceito final da ação, serão utilizados os seguintes intervalos numéricos:

CONCEITO	PESO	INTERVALO
Fraco	1	0 a 1,59
Regular	2	1,60 a 2,59
Bom	3	2,60 a 3,59
Excelente	4	3,60 a 4,00

- 3.7.7.7** Para fins de avaliação geral da turma, será considerada a média obtida nos fatores que compõem a avaliação de reação.

3.7.8 Garantia da Capacitação

- 3.7.8.1** O resultado da capacitação será considerado INSATISFATÓRIO quando pelo menos uma das situações abaixo ocorrer:
- 3.7.8.2** Média final da turma igual ou inferior ao conceito regular, excluindo-se o fator Autoavaliação;
- 3.7.8.3** Média do fator Instrutoria igual ou inferior ao conceito regular;
- 3.7.8.4** Média de, pelo menos, dois fatores igual ou inferior ao conceito regular, excluindo-se o fator Autoavaliação.
- 3.7.8.5** A CONTRATADA será obrigada a realizar, sem ônus para o BASA, nova capacitação para todas as turmas em que ficar configurado como resultado INSATISFATÓRIO. A critério do BASA, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados. A nova capacitação deverá acontecer segundo um novo calendário a ser definido pelo BASA.
- 3.7.8.6** No caso de uma turma obter o resultado da avaliação INSATISFATÓRIO, o cronograma aprovado será automaticamente suspenso até que os problemas



identificados sejam considerados sanados pelo BASA. No caso de haver impacto nas turmas já planejadas, um novo cronograma deverá ser validado por ela.

3.7.9 Certificados e Lista de Presença

3.7.9.1 A CONTRATADA deverá disponibilizar para os participantes que obtiverem no mínimo 75% de frequência, os certificados de conclusão de curso, em papel ou meio eletrônico, ao final de cada turma. Aqueles que apresentarem percentuais inferiores não deverão recebê-lo.

3.7.9.2 A CONTRATADA deverá enviar ao BASA a lista de presença gerada pela ferramenta de videoconferência.

3.7.10 Anualmente e mediante solicitação do BASA, a CONTRATADA deverá fornecer, as suas expensas, uma capacitação de atualização para a equipe gestora do contrato, com carga horária mínima de 2 (duas) horas. A capacitação de atualização deverá ser ministrada para uma turma de até 10 alunos e não deverá gerar custos extras para o BASA.

3.8 Item 6 - Serviços técnicos especializados em governança de identidade

3.8.1 Para a execução dos Serviços técnicos especializados em governança de identidade, item 6, o modelo adotado nesta contratação é baseado produção, focado em demanda por escopo. Neste, o BASA definirá previamente todas as tarefas a serem executadas, os resultados esperados, os padrões de qualidade exigidos, os procedimentos e qualificações para execução em conformidade com os adotados pela organização, cabendo à empresa contratada cumprir as atividades solicitadas dentro do esforço e prazo estimado. O conceito promove um orçamento mais próximo da realidade dos serviços com a qualidade desejada.

3.8.2 O uso de UST (Unidade de Serviço Técnico) é busca atender não só as necessidades técnico-operacionais do BASA, como melhorar os procedimentos internos de execução em consonância com as melhores práticas para gerência de serviços de segurança da informação. Assegura-se um padrão mínimo de qualidade, permitindo o conhecimento do processo e facilitando sua fiscalização durante a vigência.

3.8.3 Logo, a prestação dos serviços técnicos especializados está condicionada à solicitação prévia do BASA por meio de ordem de serviço e a remuneração, em razão da natureza das atividades, será feita por meio de Unidade de Serviços Técnicos - UST.

3.8.4 Os Serviços foram catalogados com a respectiva remuneração no item 3.8.20.

3.8.5 A unidade de referência adotada é inicialmente equivalente à hora técnica (1 UST = 1 hora técnica), necessária para a realização de uma atividade de complexidade mínima.

3.8.6 Os acionamentos para a prestação dos Serviços técnicos especializados em segurança da informação serão feitos por Ordem de Serviço (OS), a ser entregue à CONTRATADA.



- 3.8.7** A Ordem de Serviço (OS) a ser elaborada pelo BASA deverá detalhar a demanda, o período de execução, a estimativa de UST e a previsão de conclusão da demanda.
- 3.8.8** A CONTRATADA terá o prazo de até 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinatura da Ordem de Serviço (OS).
- 3.8.9** A CONTRATADA não poderá iniciar qualquer tipo de atividade sem o recebimento da Ordem de Serviço (OS), devidamente assinada e entregue pelo Gestor do Contrato.
- 3.8.10** A CONTRATADA não poderá executar os serviços acima da quantidade demandada na Ordem de Serviço (OS).
- 3.8.11** Caso seja necessário reforço na quantidade demandada inicialmente, deverá ser emitida nova Ordem de Serviço (OS), observado os procedimentos desta Cláusula.
- 3.8.12** A CONTRATADA deve observar atentamente o prazo previsto para a conclusão dos serviços.
- 3.8.13** Após definido o tamanho do serviço em UST, o esforço empregado na execução da demanda é responsabilidade da CONTRATADA, ou seja, qualquer fator (por exemplo: atraso) que não tenha sido causado pela mudança do escopo do que foi demandado, não acarretará ônus financeiro para o BASA.
- 3.8.14** Caso o prazo não consiga ser cumprido, a CONTRATADA deve encaminhar justificativa com antecedência de 5 (cinco) dias úteis para avaliação do BANCO DA AMAZÔNIA. Não serão aceitas justificativas à posteriori, o que resultará nas sanções.
- 3.8.15** O encaminhamento de justificativa para atrasos, não implica a não aplicação de penalidade conforme estipulado nos níveis de serviços, salvo nos casos em que o atraso seja de responsabilidade do BANCO DA AMAZÔNIA.
- 3.8.16** A CONTRATADA quando concluir o atendimento deverá enviar em até 2 (dois) dias o relatório descrevendo como a solicitação foi atendida.
- 3.8.17** A prestação dos serviços poderá ocorrer tanto durante o horário comercial quanto fora deste, à critério exclusivo da CONTRATANTE.
- 3.8.18** O pagamento da ordem de serviço será efetivado somente após entrega do serviço e emissão do recebimento definitivo, condicionado à avaliação de cada uma das entregas.
- 3.8.19** O BASA não fica obrigado a adquirir qualquer quantidade mínima de USTs para contratação de algum serviço, e estes serão demandados de acordo com sua conveniência, podendo utilizar até 5.000 (cinco mil) UST durante a vigência do contrato.
- 3.8.19.1** Os Serviços foram catalogados com a respectiva remuneração, conforme tabela abaixo:



ITEM	Serviço	Descrição	Entregável	Faixa/ unidade de execução	Valor a ser remunerado (UST)
1	Mapeamento de matriz SoD	Elaboração de matriz de segregação de funções e acessos críticos de um sistema, incluindo: Identificação dos acessos/perfis que executam as operações dentro do processo; Avaliação dos acessos e das operações por criticidade, identificando, avaliando e classificando de acordo com o risco para os negócios do BASA; Mapeamento dos perfis que carecem de segregação mandatória em função de regulamentações externas; Identificação de conflitos de segregação de função e acessos críticos do processo; Avaliação do nível dos riscos atuais; Criação, revisão e atualização das regras de Segregação de Funções (SoD – Segregation of Duties) e Acessos Críticos (SAT – Sensitive Access Transaction) na matriz de riscos do BASA; sugestões de controles compensatórios.	• Matriz de Segregação de Funções (SoD – Segregation of Duties) do sistema validada pelo owner • Matriz de Acessos Críticos (SAT – Sensitive Access Transaction) do sistema validada pelo owner. • Regras SoD do sistema; • Sugestões de controles compensatórios.	Por hora trabalhada	1
2	Normas e Políticas	Apoiar a definição de Políticas e normas de gestão de identidade e controle de acesso;	Texto da norma conforme modelo do BASA	Por hora trabalhada	1

4. QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS DA CONTRATADA

4.1. Os Serviços deverão ser prestados por profissionais com qualificação técnica adequada às características e complexidade dos serviços, conforme as exigências a seguir:

4.1.1 Gerente de Projetos:

- 4.1.1.1** Certificação mínimo exigida: PMP – Project Management Professional do PMI – Project Management Institute ou MBA – Master of Business Administration em Gerência de Projetos.



4.1.1.2 Experiência mínima exigida: participação, como coordenador, em, pelo menos, 1 (um) projeto de implantação de solução de governança e administração de identidades para 1700 (mil e setecentos) usuários ou mais.

4.1.2 Consultor especializado em Governança de Identidades:

4.1.2.1 Certificação mínima exigida: certificação do fabricante da solução ofertada.

4.1.2.2 Experiência mínima exigida: experiência em 2 (dois) ou mais projetos de implantação de soluções para governança e administração de identidades compatível com a solução a ser implantada no BASA e experiência comprovada de, no mínimo, 2 (dois) anos na tecnologia da solução ofertada.

4.1.3 Analista de Negócios:

4.1.3.1 Certificação mínima exigida: formação superior completa em Tecnologia da Informação ou em outra área de conhecimento, desde que detenha especialização completa na área de TI. A formação deverá ser comprovada por meio de diploma de instituição de ensino superior reconhecida pelo MEC.

4.1.3.2 Experiência mínima exigida: deverá possuir experiência mínima de 2 (dois) anos em função equivalente com atividades relacionadas a desenho de processos e uso de frameworks e ferramentas de BPM (Business Process Management).

4.1.4 Especialista em Operação e Suporte da Solução:

4.1.4.1 Formação mínima exigida: formação superior completa em Tecnologia da Informação ou em outra área de conhecimento, desde que detenha especialização completa na área de TI. A formação deverá ser comprovada por meio de diploma de instituição de ensino superior reconhecida pelo MEC.

4.1.4.2 Certificação mínima exigida: certificação do fabricante da solução ofertada.

4.1.4.3 Experiência mínima exigida: deverá possuir experiência mínima de 4 (quatro) anos em tecnologia da informação e experiência mínima de 2 (dois) anos específicos na administração da solução de governança e administração de identidades ofertada ao BASA.

4.2 Para comprovação das certificações de cada profissional, deverá ser apresentada, antes do início da prestação de cada item de serviço, cópia do certificado de treinamento ou comprovação da certificação em questão pelos meios disponibilizados pela instituição certificadora e cópia da carteira de trabalho ou contrato de prestação de serviços ou declaração do empregador.

5. SEGURANÇA DA INFORMAÇÃO

5.1 Os serviços prestados de forma remota deverão ser realizados por meio de VPNs (Virtual Private Networks), garantindo confidencialidade, autenticação e integridade do tráfego de rede do BASA.

5.2 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).

5.3 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.

5.4 A contratada deverá:

- 5.4.1** 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;
- 5.4.2** 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;
- 5.4.3** 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;
- 5.4.4** 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;
- 5.4.5** 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;
- 5.4.6** manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do BASA;
- 5.4.7** garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do Banco da Amazônia;
- 5.4.8** A contratada deverá possuir Política de Segurança da Informação com no máximo 1 (um) ano desde a última atualização;
- 5.4.9** assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo e devidamente comprovados, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;
- 5.4.10** 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, desde que devidamente comprovados;

5.4.11 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.

5.5 O ambiente físico da contratada deverá atender os seguintes requisitos mínimos de segurança:

5.5.1 Dispor de sistema de gerenciamento de controle de acesso físico que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;

5.5.2 Dispor de controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura de digital ou análise de retina;

5.5.3 Possuir registro de entrada e saída de pessoas mantidos por pelo menos 90 dias.

5.5.4 Utilizar MFA (Múltiplo Fator de Autenticação) para acessos VPN;

5.5.5 Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

5.5.6 Dispor de sistema de autenticação de identificação única para acesso.

5.6 O BASA poderá promover a qualquer tempo diligência para checar a veracidade das informações para confrontação do detalhamento das especificações técnicas do termo.

6. COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM

6.1 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.

6.2 A contratada deverá:

6.2.1 cumprir integralmente as diretrizes da Resolução CMN 4.893/21;

6.2.2 fornecer acesso ao BASA aos dados e às informações a serem processados ou armazenados pela empresa contratada;

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



- 6.2.4** 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;
- 6.2.5** fornecer informações e recursos de gestão para possibilitar o monitoramento dos serviços a serem prestados;
- 6.2.6** 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;
- 6.2.7** assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do BASA;
- 6.2.8** 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). Deve-se utilizar o recurso SSO disponibilizado pelo BASA para esta configuração.
- 6.2.9** registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.
- 6.2.10** 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.
- 6.2.11** 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;
- 6.2.12** 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;
- 6.2.13** 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;
- 6.2.14** 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;



- 6.2.15** notificar ao BASA sobre a subcontratação de serviços relevantes para a prestação do serviço contratado;
- 6.2.16** 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;
- 6.2.17** 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;
- 6.2.18** 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;
- 6.2.19** 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;
- 6.2.20** realizar a análise e gestão de riscos de segurança de informação dos ativos envolvidos na prestação do serviço. A análise deve ter periodicidade no mínimo mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes;
- 6.2.21** 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;
- 6.2.22** 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;
- 6.2.23** realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) e auditorias por terceira parte reconhecidamente confiável, disponibilizando relatório comprobatório a cada três meses para o BASA;
- 6.2.24** prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;



- 6.2.25** 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;
- 6.2.26** 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);
- 6.2.27** realizar backups e salvaguardas dos conteúdos das comunicações realizadas por meio da solução e permitir a consulta desses dados;
- 6.2.28** 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.
- 6.2.29** comprometer-se a preservar os dados do BASA contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente à BASA qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados;
- 6.2.30** 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;
- 6.2.31** atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:
- 6.2.31.1** as diretrizes de tratamento;
 - 6.2.31.2** o modo de atendimento a solicitações de titulares de dados pessoais;
 - 6.2.31.3** as medidas protetivas para garantia da confidencialidade dos dados pessoais;
 - 6.2.31.4** as medidas protetivas durante as comunicações com o BASA;
 - 6.2.31.5** o registro de atividades de tratamento de dados pessoais;
 - 6.2.31.6** a solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;
 - 6.2.31.7** as medidas de devolução / descarte dos dados.
- 6.3** A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:
- 6.3.1** inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;
 - 6.3.2** inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;



- 6.3.3** 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;
- 6.3.4** fornecer ao BASA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BASA.
- 6.4** Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo BASA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se que:
 - 6.4.1** pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;
 - 6.4.2** a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, desde que em conformidade com a Resolução CMN 4.893/21.
- 6.5** 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.
- 6.6** 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.
- 6.7** É vedado o uso de informações do BASA pela contratada para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;
- 6.8** 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.
- 6.9** Em caso da decretação de regime de resolução do Banco da Amazônia pelo Banco Central do Brasil, a contratada deverá:
 - 6.9.1** 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
 - 6.9.2** 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.

7. TRANSIÇÃO CONTRATUAL

- 7.1** O período de transição contratual representa os últimos 6 (seis) meses de vigência do Contrato apenas quando não houver e/ou não for possível a prorrogação do Contrato.
- 7.2** Durante esse período, a CONTRATADA deverá elaborar e entregar documentação técnica de transição contratual para cada um dos Serviços Gerenciados de Segurança, como subsídio para contratações futuras. Tais documentos são responsáveis por assegurar a confidencialidade, integridade e disponibilidade dos serviços de TI no momento de migrações futuras da solução implementada, incluindo as seguintes informações:
- 7.2.1** Documentação técnica atualizada de as-built da solução, incluindo parâmetros de instalação, configuração, arquitetura e topologias implementadas;
 - 7.2.2** Demonstrativo de crescimento anual, compreendendo toda a vigência do contrato, para cada ambiente de produção;
 - 7.2.3** Baseline de dados que subsidiem a planejamento de capacidade dos serviços.
 - 7.2.4** Fornecimento de arquivos de configuração dos softwares utilizados para a prestação dos serviços; e
 - 7.2.5** Esclarecimento de dúvidas de configuração, dimensionamento ou operação dos serviços;
- 7.3** A transição entre os serviços de cópias de segurança (backup) e disponibilização de dados (restore) que estão em produção e os que serão implantados deve ser feita de forma que não haja interrupção, que deve, inclusive, operar paralelamente por um Período de Transição, que será considerado finalizado ao término da migração dos dados legados;
- 7.4** A CONTRATADA deverá participar, a critério do BASA, do projeto de transição dos serviços contratados em conjunto com a empresa sucessora e o Banco, em especial na documentação das regras e alertas desenvolvidos para o BASA, disponibilização de documentos, base de conhecimento, auxílio em dúvidas e procedimentos e pela passagem do conhecimento para equipe interna do BASA e/ou eventual novo fornecedor sem prejuízo à prestação do serviço e sem custo adicional para o Banco.
- 7.5** A CONTRATADA também será responsável por acompanhar e orientar as atividades executadas pelo novo fornecedor.
- 7.6** A CONTRATADA deverá disponibilizar todas as informações pertinentes aos serviços prestados solicitadas pela empresa que irá sucedê-la no serviço.



7.7 Durante o período de transição contratual as equipes da CONTRATADA prestarão os serviços previstos no Edital conforme item 3.6 Serviço de Suporte e Operação, observando os níveis mínimos de serviço estabelecidos no **Anexo I-B – Níveis Mínimos De Serviço**.

7.8 Eventuais descumprimentos dos níveis mínimos de serviço poderão resultar em ajustes de pagamento.

8. CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR

8.1 Documentação complementar à Proposta de Preço: Juntamente com a Proposta de Preço, o licitante deverá encaminhar planilha de composição de custo e documentação técnica das soluções ofertadas, acrescida de Planilha de Atendimento aos Requisitos Técnicos indicando para cada item (exigência), o documento ou manual e o número da página, na documentação técnica fornecida, que permita a verificação das características técnicas obrigatórias, observado que o licitante deverá fornecer todas as informações que sejam solicitadas pela equipe do BANCO, visando completa validação de atendimento às características técnicas;

8.2 Qualificação técnica (habilitação):

8.2.1 A contratada deverá apresentar um ou mais atestado(s) de capacidade técnica-Operacional, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, em nome da CONTRATADA, que comprove(m) que a referido CONTRATADA executou ou executa, sem ressalvas quanto à qualidade, serviços pertinentes e compatíveis em características técnicas, quantidades e prazos compatíveis ou similares com o objeto desta licitação, ou com o item pertinente.

8.2.2 A comprovação de que trata o item anterior será feita por meio de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, em papel timbrado da(s) emitente(s) e com a identificação do(s) signatário(s), de que a participante foi contratada para fornecimento de objetos similares ao dessa licitação, restrita a parcelas do objeto técnica ou economicamente relevantes, de acordo com parâmetros estabelecidos de forma expressa no instrumento convocatório.

8.2.3 Somente serão aceitos atestados expedidos após a conclusão do contrato ou decorrido no mínimo 12 (doze) meses do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior.

8.2.4 Para fins de aferição de pertinência e compatibilidade, o(s) atestado(s) apresentado(s) deverá(ão) mencionar:

8.2.4.1 Atestado de capacitação técnica emitida por empresa de direito público ou privado, comprovando experiência da licitante no fornecimento de Solução de Administração e Governança de Identidade (IGA), e/ou serviços gerenciados de Segurança da Informação (MSSP – Managed Security Service Provider), incluindo Serviços de implantação, suporte e operação da solução em empresas com, no mínimo, 1700 (Hum mil e setecentos) usuários, o que correspondem a, aproximadamente, 50% (cinquenta por cento) da necessidade do BASA; e

8.2.4.2 Serviços de suporte e operação de solução de Administração e Governança de Identidade (IGA), e/ou serviços gerenciados de Segurança da Informação (MSSP – Managed Security Service Provider), em empresas com, no mínimo,



1700 (um mil e setecentos) usuários, o que correspondem a, aproximadamente, 50% (cinquenta por cento) da necessidade do BASA;

- 8.2.5** Para obtenção da quantidade exigida, será admitido o somatório de dois ou mais atestados/certidões/declarações/contratos compatíveis com o objeto do Edital de períodos concomitantes.
- 8.2.6** Cada atestado deverá conter:
- 8.2.6.1** Nome, endereço eletrônico e telefone do(s) contato(s), ou outra forma que permita ao BASA estabelecer contato com a empresa atestadora, se necessário;
- 8.2.6.2** Discriminação do serviço prestado, detalhando: o produto/ marca/ módulo/ função e respectiva versão; quantitativo de usuários que utilizam a solução, bem como demais detalhes que permitam a sua perfeita identificação, devendo ser, necessariamente, compatível com os ambientes e aplicações desta licitação.
- 8.2.6.3** Elementos que comprovem o conteúdo do atestado, como contratos ou propostas aprovadas de prestação de serviço.
- 8.2.7** Caso o atestado não faça referência expressa ao número de usuários, tal quantidade será considerada como o quantitativo de microcomputadores mencionado no documento.
- 8.2.8** Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente.
- 8.2.9** O BASA poderá realizar diligência/visita técnica, a fim de complementar informações ou de comprovar a veracidade do(s) Atestado(s) de Capacidade Técnica apresentado(s) pelo LICITANTE convocado, quando poderá ser requerida cópia do(s) Contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove inequivocamente que o serviço apresentado no (s) atestado(s) foi prestado.
- 8.2.10** Comprovação que LICITANTE é certificada ABNT NBR ISO 27001. Esta exigência garante que a CONTRATADA segue os principais controles de segurança da informação, assim como também possui processos para tratamento de incidente e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com o cliente
- 8.2.11** O licitante deverá emitir declaração garantindo que possui capacidade técnica para atender a demanda do BASA, conforme **Anexo I-D – Modelo de Declaração de Capacidade Técnica**.
- 8.3** Visando aferir os requisitos funcionais e as condições de operação da solução de IGA ofertada, a licitante classificada em primeiro lugar deverá realizar Prova de Conceito (PoC), conforme descrito no **Anexo I-C – Prova de Conceito**.
- 8.4** A empresa só será considerada habilitada pelo Pregoeiro, após a aprovação pela área técnica na prova de conceito, além da conformidade nos documentos de habilitação.



9. DILIGÊNCIAS E VERIFICAÇÕES

- 9.1** A CONTRATADA permitirá, a qualquer momento, a realização de diligências e vistorias em suas dependências, bem como prestar informações, com o intuito de avaliar os requisitos de Segurança da Informação, ficando a CONTRATADA responsável pelo atendimento das recomendações efetuadas.
- 9.2** A CONTRATADA permitirá, a qualquer momento, a realização de testes visando identificar falhas e vulnerabilidades no seu ambiente de TI, em suas dependências, bem como prestar informações, com o intuito de avaliar os requisitos de Segurança da Informação, ficando a CONTRATADA responsável pelo atendimento das recomendações efetuadas.
- 9.3** Caso a CONTRATADA possua rotina de verificação de vulnerabilidades do ambiente de TI, desde já se compromete a enviar relatórios destes testes, sempre que solicitado pelo CONTRATANTE, comprometendo-se a implementar as sugestões de melhorias que porventura forem produzidas.

10. PLANO DE CONTINUIDADE DE NEGÓCIOS

- 10.1** A CONTRATADA deve apresentar o Plano de Continuidade de Negócios (PCN), embasado em norma (ABNT NBR ISO 22301:2013 - Segurança da Sociedade - Sistema de Gestão de Continuidade de Negócios - Requisitos) ou boas práticas reconhecidas pelo mercado (ITIL v3, COBIT 5, Good Practice Guidelines - Business Continuity Institute, Professional Practices - Disaster Recovery International Institute), para mitigar graves perdas decorrentes de riscos operacionais que possam comprometer o Níveis Mínimos de Serviço previstos neste CONTRATO.
- 10.2** O referido PCN e as evidências dos testes realizados devem ser entregues pela CONTRATADA para o CONTRATANTE, ao final da Etapa de Implantação do serviço, quando da emissão do Termo de Aceitação Definitiva, anualmente e sempre que solicitado.
- 10.3** PCN apresentado pela CONTRATADA será analisado pelo CONTRATANTE que, motivadamente, pode rejeitar ou sugerir adequações de forma a atender aos Requisitos do Níveis Mínimos de Serviço.
- 10.4** Em caso de rejeição ou havendo necessidade de ajustes a CONTRATADA terá mais 30 (trinta) dias corridos, a partir da comunicação do CONTRATANTE, para retornar o plano atualizado.

11. CONDIÇÕES DE PAGAMENTO

- 11.1** O pagamento seguirá o seguinte critério:



Descrição	Periodicidade	Condições de Pagamento
Serviço anual de subscrição da solução de IGA	Anual	Primeiro ano: após a ativação da licença, mediante apresentação da NF. Demais anos: a cada início de cobertura de 12 (doze) meses, mediante comprovação da licença ativada, e entrega e apresentação da NF.
Serviço anual de subscrição do módulo de CIEM	Anual	A cada início de cobertura de 12 (doze) meses, mediante entrega e apresentação da NF
Serviço de implantação da solução	Única	Após a emissão do TERMO DE ACEITAÇÃO DEFINITIVO DA SOLUÇÃO (TAD), mediante apresentação da NF.
Serviço de suporte técnico e operação da solução.	Mensal	Após a emissão do Relatório de Serviços Prestados (RSP) pela CONTRATADA, validação do relatório pelo BASA, conforme Anexo I-B – Níveis Mínimos De Serviço (NMS), e mediante apresentação da NF.
Serviço de capacitação	Sob demanda respeitando o quantitativo contratado	Após a entrega do resultado da pesquisa de reação com resultado SATISFATÓRIO e apresentação da NF ao final do treinamento.
Serviços técnicos especializados	Sob demanda respeitando o escopo definido em UST	Mediante entrega esperada definida na OS e apresentação da NF ao final do treinamento.

- 11.2** O pagamento relativo ao item 3.6 - Suporte técnico e operação da solução será realizado pelo BASA em parcelas em intervalos não inferiores a 30 dias, quando concluídos os serviços. O pagamento apenas será realizado após a aprovação do Relatório de Serviços Prestados (RSP), conforme Anexo I-B – Níveis Mínimos De Serviço, quando o gestor do Contrato autorizará o faturamento do respectivo período pela CONTRATADA. A aprovação do relatório constitui condição indispensável para o pagamento do valor ajustado.
- 11.3** O BASA deduzirá da fatura referente à prestação dos serviços de suporte e operação, os valores dos descontos aplicados em virtude do descumprimento, pela CONTRATADA, dos Níveis de Serviço, conforme Anexo I-B – Níveis Mínimos De Serviço. Os descontos serão efetuados na fatura imediatamente subsequente a ocorrência dos eventos de descumprimento ou na fatura posterior, caso, a critério do BASA, não seja possível aplicar o desconto imediatamente a ocorrência do descumprimento.
- 11.4** Os pagamentos serão realizados através de crédito em conta corrente da CONTRATADA, preferencialmente, por meio de crédito em conta corrente de titularidade da CONTRATADA, mantida junto ao Banco da Amazônia, previamente indicada por aquela, nos dias 05 (cinco), 15 (quinze) ou 25 (vinte e cinco), desde que a CONTRATADA efetive a entrega das Notas Fiscais e Faturas discriminativas com 10 (dez) dias de antecedência da data prevista para pagamento, e após a conferência e confirmação da execução do serviço, acompanhadas do Termo de Recebimento dos Serviços nas condições dos subitens abaixo:
- 11.4.1** A Nota Fiscal/Fatura correspondente será examinada diretamente pelo Fiscal designado pelo BASA, o qual atestará o fornecimento dos produtos e serviços contratados e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela CONTRATADA, todas as condições pactuadas.
- 11.4.2** As Notas Fiscais não aprovadas pelo Banco serão devolvidas à CONTRATADA para as necessárias correções ou apresentação de documentos, inclusive os



relativos às retenções legais, com as informações referentes aos motivos de sua rejeição, contando-se os prazos estabelecidos a partir das suas reapresentações devidamente corrigidas, não respondendo o BASA por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

- 11.4.3** O pagamento será realizado em até 10 (dez) dias úteis, contados a partir da emissão do Termo de Recebimento dos Serviços pelo BASA, com emissão de Ordem Bancária para crédito em conta corrente da CONTRATADA.
- 11.4.4** O pagamento será automaticamente transferido para o dia útil subsequente, caso não haja expediente no Banco na data prevista para tal. O atraso na entrega da Nota Fiscal/Fatura implicará a transferência automática do pagamento para o próximo mês, sem qualquer acréscimo financeiro ao Banco.
- 11.4.5** Caso a CONTRATADA opte pelo recebimento do pagamento em conta corrente mantida em outra instituição financeira será cobrado o valor da tarifa TED ou DOC correspondente ao da tabela de tarifas e serviços do Banco, sendo que esse valor será de responsabilidade da CONTRATADA e deduzida do valor do crédito a ser enviado.
- 11.5** Em hipótese alguma a devolução de Nota Fiscal e Fatura discriminativa não aprovada pelo Banco servirá de pretexto para que a CONTRATADA suspenda a execução dos serviços ou deixe de efetuar o pagamento devido aos seus empregados ou fornecedores.
- 11.6** Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, ela deverá apresentar, juntamente com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.
- 11.7** Não serão efetuados quaisquer pagamentos, enquanto perdurar pendência de liquidação de obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação ou execução do objeto deste Edital.
- 11.8** O CNPJ/MF constante da Nota Fiscal e de todos os documentos nos quais deva constar será o mesmo indicado no preâmbulo do contrato e na carta-proposta de preços apresentada por ocasião do Pregão Eletrônico.
- 11.9** Para efeito do pagamento, a CONTRATADA deverá apresentar juntamente com as Notas Fiscais/Faturas discriminativas os documentos a seguir relacionados, caso não estejam **disponíveis no Cadastro Único de Fornecedores (SICAF)**:
 - 11.9.1** Certidão negativa ou positiva com efeitos de negativa de débitos relativos aos tributos federais, inclusive contribuições previdenciárias, e à dívida ativa da União emitida pela Secretaria da Receita Federal;
 - 11.9.2** certidão negativa ou positiva com efeitos de negativa de débitos emitida pelas Fazendas Estadual e Municipal do domicílio ou sede da contratada;
 - 11.9.3** Certificado de Regularidade do FGTS (CRF);
 - 11.9.4** Certidão negativa de débitos trabalhistas (CNDT); e
 - 11.9.5** Atestado, se for o caso, de optante pelo SIMPLES (ANEXO I-AV da Instrução Normativa SRF n.º 480, de 15.12.2004);



11.10 A não apresentação dos documentos referidos no item anterior poderá ensejar, a critério do Banco, a rescisão do contrato, sem que caiba à CONTRATADA o direito a qualquer indenização.

11.11 No caso de atraso no pagamento por culpa exclusiva do Banco, o(s) valor(es) devido(s) será(ão) acrescido(s) de encargos financeiros de 0,5% (cinco décimos por cento) ao mês, calculados "pro rata die" até o dia do efetivo pagamento.

12. DA ASSINATURA DO CONTRATO

12.1 O LICITANTE deve comprovar que possui em sua equipe profissionais especialistas certificados nas soluções ofertadas para prestação do serviço, comprovando por meio de certificações emitidas pelo fabricante do software.

13. OBRIGAÇÕES DA CONTRATADA

13.1 Alocar todos os recursos necessários para obter uma fiel execução dos serviços previstos no objeto da contratação, de forma plena e satisfatória, iniciando e prestando os serviços no prazo estipulado, na forma e nas condições pactuadas, em estrita conformidade com as especificações, prazos e condições estabelecidas nos termos contratuais e na sua proposta.

13.2 Planejar, desenvolver, implantar, executar e manter o serviço objeto do Contrato dentro dos acordos de níveis mínimos de serviço estabelecidos.

13.3 Qualquer problema que venha a comprometer o bom andamento dos serviços ou o alcance dos níveis mínimos de serviço acordados, deve ser imediatamente comunicado ao BASA, que colaborará com a CONTRATADA na busca da melhor solução.

13.4 Notificar ao BASA, imediatamente e por escrito, qualquer anormalidade que verificar na execução dos serviços.

13.5 Responder pelos danos comprovadamente causados ao BASA ou a terceiros, decorrentes de sua culpa ou dolo, inclusive de seus empregados, quando da execução do objeto contratado. A fiscalização ou o acompanhamento do BASA não excluirá ou reduzirá essa responsabilidade da CONTRATADA.

13.6 Observar boas práticas relativas à segurança da informação, especialmente as indicadas nos normativos internos do Banco da Amazônia, sobretudo na Política de Segurança da Informação e Cibernética, em todas as atividades executadas durante o ciclo de desenvolvimento das aplicações.

13.7 Emitir, por ocasião da assinatura do Contrato, o **Adendo I** – Termo De Confidencialidade E Sigilo deste Edital, pelo qual se compromete a 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.

13.8 Fornecer, antes do início da prestação do serviço, o **Adendo II** – Termo De Confidencialidade E Sigilo Do Profissional a ser assinado por cada profissional que venha a prestar os seus serviços, pelo qual se comprometem a manter o sigilo e a confidencialidade de todos os dados e informações de que venha a ter conhecimento no exercício de suas atribuições.

13.9 Em caso de não cumprimento das condições estabelecidas nos Termos mencionados nos itens 13.7 e 13.8, e/ou em caso de quebra da guarda e sigilo, aludidos, ou de utilização dos dados fornecidos pelo BASA, para outros fins de qualquer natureza ou espécie, que não os expressamente autorizados e para uso exclusivo dos serviços prestados a este, a CONTRATADA responderá de forma



incondicional, civil, criminal e administrativamente pelo fato, sem prejuízo do direito do BASA de promover a rescisão contratual, com a aplicação das penalidades previstas neste ajuste.

- 13.10** Possuir em sua equipe profissionais especialistas certificados nas soluções ofertadas para prestação do serviço, comprovada por meio de certificações emitidas pelo fabricante do software.
- 13.11** Devolver e eliminar de suas bases de dados, após a realização dos serviços, toda e qualquer informação ou documentos porventura encaminhados pelo BASA para auxiliar na realização dos serviços.
- 13.12** Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação para contratar com a Administração Pública, apresentando sempre que exigido os comprovantes de regularidade.
- 13.13** Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o BASA.
- 13.14** Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à prestação dos serviços, originariamente ou vinculados por prevenção, conexão ou contingência.
- 13.15** Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do Contrato a ser firmado.
- 13.16** Assumir inteira responsabilidade técnica e administrativa pelo respectivo objeto contratado, não podendo, em qualquer hipótese, transferir a outras empresas a responsabilidade por problemas ocorridos na execução do serviço.
- 13.17** 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 Banco 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.
- 13.18** Assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BANCO através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado.
- 13.19** Indicar formalmente um profissional para a função de preposto da CONTRATADA apto a representá-la junto ao BASA, que deverá responder pela fiel execução do Contrato.
- 13.20** Prestar todos os esclarecimentos que lhe forem solicitados pelo BASA.
- 13.21** Aceitar, por parte do BASA, em todos os aspectos, a fiscalização no cumprimento do objeto contratado.
- 13.22** Além das obrigações usualmente aplicadas à CONTRATADA, permitir ao Banco Central do Brasil acesso a termos firmados, documentos e informações atinentes aos serviços prestados, bem como às suas dependências, nos termos do § 1º do artigo 33 da Resolução CMN nº 4.557/2017.

14. OBRIGAÇÕES DA CONTRATANTE

- 14.1** O BASA deverá indicar o responsável pela gestão e fiscalização do Contrato.



CONTRATO Nº 2025/154-01

- 14.2** O BASA deverá disponibilizar todas as informações necessárias à CONTRATADA, com o intuito de fornecer subsídios, para prestação dos serviços contratados.
- 14.3** O BASA deverá efetuar o pagamento devido pela prestação dos serviços, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas no Edital e seus Anexos.
- 14.4** O BASA deverá permitir, sempre que necessário, acesso dos profissionais da CONTRATADA às dependências, equipamentos, softwares e sistemas de informação do BASA, relacionados ao objeto do Contrato ou necessários à execução dos serviços.
- 14.5** O BASA deverá fiscalizar o cumprimento dos requisitos de qualificação profissional exigidos neste Termo de Referência e Anexos, solicitando à CONTRATADA, sempre que necessário, substituição de profissional, treinamentos e certificações necessárias.
- 14.6** O BASA deverá comunicar, formalmente, a CONTRATADA qualquer falha verificada no cumprimento do Contrato.
- 14.7** Fornecer cópia dos normativos internos vigentes do Banco da Amazônia que estiverem relacionados à prestação dos serviços.

15. SANÇÕES ADMINISTRATIVAS

- 15.1** Comete infração administrativa nos termos da legislação vigente, a CONTRATADA que:
 - 15.1.1** inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação.
 - 15.1.2** ensejar o retardamento da execução do objeto.
 - 15.1.3** falhar ou fraudar na execução do contrato.
 - 15.1.4** comportar-se de modo inidôneo; e
 - 15.1.5** fraude fiscal.
- 15.2** Pela inexecução total ou parcial do objeto deste contrato, o BASA poderá aplicar à CONTRATADA as seguintes sanções:
 - 15.2.1** Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.
 - 15.2.2** Multa de:
 - 15.2.2.1** 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério do Banco, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão da avença.
 - 15.2.2.2** 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima ou de inexecução parcial da obrigação assumida.



- 15.2.2.3** 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida.
- 15.2.2.4** 0,2% a 3,2% por dia sobre o valor do contrato, conforme detalhamento constante das tabelas 1 e 2 abaixo.
- 15.2.2.5** até 1% (um por cento) por dia útil de atraso na implantação dos serviços. A referida multa terá como base o valor global referente ao serviço descumprido;
- 15.2.2.6** até 10% (dez por cento) sobre o valor global do Contrato, a critério da autoridade competente do BASA, em razão de qualquer descumprimento das demais obrigações contratuais, não previstas nos itens acima.
- 15.2.3** Suspensão temporária de participação em licitação e impedimento de contratar com o BASA, por prazo não superior a 2 (dois) anos, apurado em razão da natureza e gravidade da infração cometida.
- 15.3** O total das multas aplicadas não poderá exceder o montante de 30% (trinta por cento) do valor global do Contrato.
- 15.4** O valor da multa poderá ser descontado da nota fiscal ou de crédito existente no BASA em relação à CONTRATADA. Caso o valor da multa seja superior ao crédito existente, a diferença será cobrada na forma da lei.
- 15.5** As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.
- 15.6** A aplicação de qualquer das penalidades previstas somente poderá ser aplicada após procedimento administrativo, e desde que assegurados o contraditório e a ampla defesa, facultada ao CONTRATADO a defesa prévia, no prazo de 10 (dez) dias úteis, observando-se o procedimento previsto na Legislação Vigente.
- 15.7** Contra a decisão de aplicação de penalidade, o CONTRATADO poderá interpor o recurso cabível, na forma e no prazo previstos no Regulamento de Formalização, Execução e Fiscalização de Contratos Administrativos.
- 15.8** A imposição de penalidades não impede a extinção do Contrato pelo BASA, nos termos da legislação aplicável.
- 15.9** As sanções de advertência e de impedimento de licitar e contratar com o BASA poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.
- 15.10** A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Contratante, observado o princípio da proporcionalidade.
- 15.11** As penalidades serão obrigatoriamente registradas no SICAF.
- 15.11.1** Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor do contrato
2	0,4% ao dia sobre o valor do contrato
3	0,8% ao dia sobre o valor do contrato
4	1,6% ao dia sobre o valor do contrato
5	3,2% ao dia sobre o valor do contrato

INFRAÇÃO		
ITEM	DESCRIÇÃO	GRAU
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
3	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
4	Deixar de cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
5	Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03
6	Deixar de indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01

16. AVALIAÇÃO DO FORNECEDOR

16.1 Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, o BASA realizará no início de cada semestre a Avaliação de Desempenho de Fornecedores, o que permitirá a adoção de eventuais ajustes no modelo de atendimento.

16.2 Serão avaliados os seguintes critérios:

16.2.1 Comunicação: Avaliação qualitativa da comunicação do fornecedor, como: clareza na informação, formas de solicitações e questionamentos ao BASA, educação e nível de formalidade no atendimento, e tempo de resposta às solicitações do BASA.

16.2.2 Confiabilidade: Prestação correta (isenta de falhas e erros) do serviço / atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas.

16.2.3 Organização: Demonstração do planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

16.3 Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos conceitos abaixo:

16.3.1 Péssimo (de 0 a 4,9)

16.3.2 Regular (de 5 a 7,4)

16.3.3 Bom (de 7,5 a 8,9)

16.3.4 Ótimo (de 9 a 10)

16.4 A CONTRATADA será informada do conceito médio obtido no período e registrado nos controles do BASA, resultado este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

17. PREPOSTO DO CONTRATO



- 17.1** A CONTRATADA deverá indicar formalmente, no ato de assinatura do CONTRATO ou sempre que alterado, o preposto que atuará como Supervisor Geral de CONTRATO e será seu representante principal junto ao CONTRATANTE.
- 17.2** O preposto de Contrato será responsável pela interlocução técnica com o Banco acerca da qualidade e andamento dos serviços. São responsabilidades do preposto de contrato:
- 17.2.1** Apresentar ao BASA o planejamento de atendimento das etapas do Projeto encaminhadas para a CONTRATADA e zelar pela qualidade geral dos serviços prestados pela CONTRATADA;
 - 17.2.2** Supervisionar, tecnicamente, a atuação dos seus empregados indicados como responsáveis pela execução dos serviços descritos nas especificações técnicas do Termo de Referência;
 - 17.2.3** Participar das reuniões regulares de acompanhamento do Contrato, em periodicidade a ser definida pelo BASA;
 - 17.2.4** Avaliar, em conjunto com o BASA, os níveis de serviço alcançados;
 - 17.2.5** Participar, sempre que convocado pelo BASA, de reuniões de abertura, acompanhamento ou encerramento de etapas de Projeto, quando aplicável;
 - 17.2.6** Apresentar e negociar com o BASA medidas corretivas para sanar os problemas encontrados na execução do Projeto, ou com vistas a atingir ou restabelecer níveis de serviço previstos neste Termo de Referência;
 - 17.2.7** Assegurar que as medidas negociadas com o BASA sejam devidamente observadas;
 - 17.2.8** Assegurar a correta aplicação do fluxo de trabalho definido para a execução dos serviços definidos neste Termo de Referência;
 - 17.2.9** Responsabilizar-se pelo controle de qualidade dos serviços definidos neste Termo de Referência;

18. PROPOSTAS DE PREÇO

- 18.1** As LICITANTES deverão cotar os valores unitários, totais e global de acordo com as exigências deste documento.
- 18.2** Nos preços cotados deverão estar incluídas todas as despesas com salários, softwares, encargos sociais, fiscais e comerciais, impostos, taxas e quaisquer outros tributos, quando aplicáveis, necessárias ao integral cumprimento do objeto pela CONTRATADA. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais designados para a prestação dos serviços, tais como deslocamentos, hospedagens, treinamentos etc.
- 18.3** As LICITANTES deverão, ainda, apresentar juntamente com a proposta, as planilhas de composição de custos e formação de preços detalhando a formação de preços com todos os insumos (mão de obra, remuneração, encargos, impostos e taxas, reserva técnica, lucro etc.).



- 18.4** Todos os softwares e equipamentos que comporão as propostas de prestação de serviço devem ser fornecidos na versão mais nova comercializada na data da abertura das propostas.
- 18.5** A LICITANTE deverá informar o modelo de cada item de software e hardware que será ofertado e suas características/especificações técnicas.
- 18.6** A LICITANTE deverá informar sobre a concordância com todos os termos descritos neste Edital;
- 18.7** A proposta técnica comercial deverá ser apresentada em papel timbrado, assinada pelo responsável.
- 18.8** A proposta de preços deverá conter no mínimo:
 - 18.8.1** A razão social da empresa CONTRATADA, endereço completo, número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ, do Ministério da Fazenda.
 - 18.8.2** Declaração expressa de estarem incluídos nos preços propostos, todos os custos e despesas de qualquer natureza. Na falta de tal declaração, será considerada como inclusa nos preços toda e qualquer despesa;
 - 18.8.3** Prazo de validade não inferior a 60 (sessenta) dias, contados da data de abertura da sessão pública estabelecida no Edital. Na falta de tal informação será considerado aceito o prazo citado nesta alínea.
 - 18.8.4** Indicação do nome e número do banco, agência e conta corrente, para efeito de pagamento. Na falta de tal informação, a Administração poderá solicitá-la em outro momento.
 - 18.8.5** Número de telefone e fax ou número 0800 e o e-mail (correio eletrônico), onde poderão ser efetuados os contatos necessários durante o período de vigência do contrato.
 - 18.8.6** A CONTRATADA deverá seguir o modelo de proposta de preços estabelecido no Anexo II - Modelo De Proposta De Preço.

19. GARANTIAS CONTRATUAIS

- 19.1** A CONTRATADA se obriga a manter durante toda a vigência, a 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, de acordo com as seguintes condições:
 - 19.1.1** Garantia de 5% (cinco por cento) do valor do Contrato.
 - 19.1.2** A garantia oferecida pela CONTRATADA deve assegurar o cumprimento tanto do objetivo contratado, quanto das obrigações acessórias, inclusive trabalhistas.
 - 19.1.3** A CONTRATADA deverá providenciar a garantia contratual impreterivelmente em 05 (cinco) dias úteis, contados da assinatura do Contrato.
- 19.2** No caso de CAUÇÃO EM DINHEIRO, o valor depositado será administrado pelo CONTRATANTE e devolvido à CONTRATADA no término do Contrato.



- 19.2.1** O CONTRATANTE reserva-se o direito de utilizar, a qualquer tempo, no todo ou em partes, o valor da garantia para cobrir danos diretos eventualmente apurados, decorrentes de descumprimento de qualquer obrigação contratual ou falha dos serviços ora contratados, inclusive motivados por greve ou atos dos empregados da CONTRATADA.
- 19.2.2** Utilizada a garantia, por qualquer que seja o motivo, a CONTRATADA fica obrigada a integralizá-la no prazo de 05 (cinco) dias úteis contados da data em que for notificada formalmente pelo CONTRATANTE, sob pena de rescisão do Contrato.
- 19.2.3** 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.
- 19.3** No caso de SEGURO-GARANTIA o CONTRATANTE deverá ser indicado como beneficiário do seguro-garantia.
- 19.3.1** O seguro-garantia deverá assegurar o pagamento de todas as obrigações contratuais previstas.
- 19.3.2** A CONTRATADA obriga-se a apresentar nova apólice, até 05 (cinco) dias úteis após o vencimento da anterior e a comprovar o pagamento do prêmio respectivo, até 02 (dois) dias úteis após o seu vencimento.
- 19.4** No caso da FIANÇA BANCÁRIA deverão constar do instrumento os seguintes requisitos:
- Prazo de validade correspondente ao período de vigência do Contrato;
- 19.4.1** 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;
- 19.4.2** Cláusula que assegure a atualização do valor afiançado.
- 19.5** Na assinatura de cada Aditivo de prorrogação de vigência do Contrato, a CONTRATADA obriga-se a renovar a garantia no valor correspondente a 5% (cinco por cento) do valor total referente ao período de vigência do Aditivo.
- 19.6** A garantia também deverá ser integralizada quando houver redimensionamento do volume de serviços, repactuação contratual ou revisão de preços, de modo que permaneça correspondendo a 5% (cinco por cento) do valor global contratado.
- 19.7** A qualquer tempo, mediante prévia comunicação ao CONTRATANTE, poderá ser admitida a substituição da garantia, observadas as modalidades previstas no Contrato.
- 19.8** 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 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.



CONTRATO Nº 2025/154-01

20. FISCALIZAÇÃO E GESTÃO DO CONTRATO

- 20.1** O CONTRATANTE providenciará os seguintes responsáveis pelo acompanhamento da execução do Contrato:
- 20.1.1** Gestor do Contrato: Empregado do CONTRATANTE com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do Contrato, indicado por autoridade competente;
 - 20.1.2** Fiscal Técnico do Contrato: Empregado do CONTRATANTE representante da Área de Segurança Corporativa, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o Contrato;
 - 20.1.3** Fiscal Administrativo do Contrato: Empregado do CONTRATANTE representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o Contrato quanto aos aspectos administrativos;
- 20.2** Nas ausências ou impedimentos dos empregados de que trata o item anterior, os encargos a ele atribuídos passarão a ser exercidos por quem o substituir na forma regulamentar.
- 20.3** A ausência ou omissão da fiscalização do BASA não eximirá a CONTRATADA das responsabilidades previstas neste Edital e seus Anexos e no Contrato.
- 20.4** Os contatos entre o BASA e a detentora serão mantidos por intermédio da Fiscalização do BASA.
- 20.5** A comunicação formal entre a Fiscalização e a detentora, e vice-versa, será feita por escrito, preferentemente por meio eletrônico, e os documentos gerados constarão dos autos do processo.
- 20.6** Todas as ordens de serviço ou comunicações entre a Fiscalização e a CONTRATADA serão transmitidas por escrito, por meio eletrônico, e constarão dos autos do processo.
- 20.7** A ausência ou omissão da fiscalização do Banco não eximirá a CONTRATADA das responsabilidades previstas neste Edital e seus Anexos e no Contrato.
- 20.8** O Gestor do serviço será responsável pela homologação e assinatura dos Termos de Recebimento Provisório e Definitivo dos Serviços.
- 20.9** O Gestor do serviço será responsável ainda por:
- 20.9.1** Cumprir e fazer cumprir as disposições e condições avençadas no Contrato e seus Anexos;
 - 20.9.2** Atestar as Notas Fiscais/Faturas e a documentação exigível para pagamento;
 - 20.9.3** Consolidar o Termo Circunstanciado elaborado pelo Fiscal do Contrato, a partir da apuração das possíveis ocorrências e das Sansões Administrativas definidas neste Edital e seus Anexos;
 - 20.9.4** Apurar eventuais faltas da CONTRATADA que possam gerar a aplicação de sansões prevista neste Termo;



20.9.5 Comunicar à CONTRATADA a ocorrência de irregularidades, diligenciando para que sejam plenamente corrigidas; e

20.9.6 Exigir da CONTRATADA, a qualquer tempo, a comprovação das condições de habilitação e qualificação exigidas neste Edital e seus Anexos.

20.10 O contrato será acompanhado pelo Gestor do Serviço, que ficará encarregado de atestar a execução dos serviços, para posterior encaminhamento para o pagamento. Os valores a serem pagos estão condicionados à execução satisfatória dos serviços contratados.

20.11 As decisões e providências que ultrapassarem a competência do Fiscal do contrato deverão ser autorizadas pela autoridade competente do CONTRATANTE, em tempo hábil para adoção das medidas convenientes.

21. DO ORÇAMENTO

21.1.1.1 O pagamento da despesa, objeto deste Edital será registrado nas rubricas:

21.1.2 82.546-8 - DESPESAS SEGURANÇA INFORMAÇÃO - SUBSCRIÇÃO DE SOLUÇÃO/SOFTWARE;

21.1.3 82.543-3 - DESPESAS DE SEGURANÇA - EXEC. SERV. (IMPLANT, INSTAL) - C/INSS PJ;

21.1.4 82.547-6 - DESPESAS SEGURANÇA INFORMAÇÃO - SUPORTE TÉCNICO SOLUÇÕES; e

21.1.5 82.548-4 - DESP SEGURANÇA INFORMAÇÃO - TREINAM P/IMPLANT - INSTRUT. EXTERNOS S/INSS.

22. ALTERAÇÃO SUBJETIVA

22.1 É vedada a subcontratação de parte do objeto desde contrato

22.2 É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do Contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do BASA S/A à continuidade do Contrato.

23. DA SUBCONTRATAÇÃO

23.1 As empresas participantes, doravante denominadas LICITANTES, deverão ser capazes de executar todo o conjunto de serviços, objeto da presente Licitação.

23.2 Não será aceita a participação de consórcios e sublocação/subcontratação de serviços em parte ou de modo global para a execução do objeto deste certame.

24. VIGÊNCIA CONTRATUAL E REAJUSTE

24.1 A vigência do Contrato será de 36 meses, a partir da data de sua assinatura, podendo ser prorrogado, mediante Aditivo Contratual, por mais 24 meses, de acordo com a Lei nº 13.303/2016.

24.2 Os preços dos serviços poderão ser reajustados pela ICTI (Índice de Contratos da TI), mantidos pelo IPEA, desde que observado o interregno de 12 (doze) meses a contar da data da assinatura do contrato ou, nos reajustes subsequentes ao primeiro, da data do início dos efeitos financeiros do último reajuste ocorrido.

24.3 Os reajustes deverão ser precedidos da solicitação da CONTRATADA.



24.4 Caso a CONTRATADA não solicite tempestivamente o reajuste e prorrogue sem pleiteá-lo ocorrerá preclusão do direito.

24.5 Também ocorrerá a preclusão do direito ao reajuste se o pedido for formulado depois de extinto o contrato.

25. VEDAÇÃO

25.1 O Contrato não poderá ser no todo ou em parte objeto de cessão ou transferência, salvo na hipótese de reorganização societária da CONTRATADA.

25.2 É vedado à CONTRATADA, salvo se estiver expressamente autorizada pelo CONTRATANTE:

25.2.1 Subcontratar terceiros para prestar os serviços objeto do Contrato;

25.2.2 Veicular publicidade que tenha como apelo mercadológico o fato de ter prestado ou estar prestando serviços ao CONTRATANTE, ou qualquer outra informação acerca das atividades e programas do CONTRATANTE;

25.2.3 Utilizar o presente Contrato como garantia perante terceiros ou cessão dos direitos creditícios em operações de desconto bancário;

25.2.4 Usar, copiar, duplicar ou de alguma outra forma reproduzir ou reter quaisquer informações do CONTRATANTE.

25.3 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 à CONTRATADA 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 Banco que exerça cargo em comissão ou função de confiança.

26. DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

26.1 Será de total responsabilidade da Contratada o cumprimento das normas ambientais vigentes para a execução dos serviços, no que diz respeito à poluição ambiental e destinação de resíduos;

26.2 A Contratada deverá tomar todos os cuidados necessários para que a partir da consecução dos serviços não decorra qualquer degradação ao meio ambiente;

26.3 A Contratada deverá assumir todas as responsabilidades e tomar as medidas cabíveis para a correção dos danos que vierem a ser causados, caso ocorra passivo ambiental, em decorrência da execução de suas atividades objeto desta licitação;

26.4 Para amenizar impacto ambiental dos resíduos produzidos pelas máquinas, os mesmos deverão ser encaminhados para os postos de coleta que fazem o reaproveitamento de embalagens, palhetas e copos e o pó para ser transformado em adubo orgânico.

26.5 A Contratada deverá promover a economia de energia elétrica pela função de desligamento automático das máquinas de café quando não estiverem em uso;



26.6 A Contratada deverá cumprir as orientações da Instrução Normativa nº 1, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, referente aos critérios de Sustentabilidade Ambiental, em seus Artigos 5º e 6º, no que couber;

26.7 Conforme dispõe o Capítulo III, Artigo 5º, Inciso III da Instrução Normativa/MPOG nº 1, de 19 de janeiro de 2010, poderá ser exigido o seguinte critério de sustentabilidade ambiental: “que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento”.

27. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

27.1 A CONTRATADA, por si e por seus colaboradores, deverá:

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

27.1.2 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

27.1.3 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.

27.2 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:

27.2.1 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 em 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.

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

27.2.3 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.



- 27.2.4** 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.
- 27.2.5** 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.
- 27.2.6** 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.
- 27.2.7** 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.
- 27.2.8** 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.
- 27.2.9** Registro 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.
- 27.2.10** Conformidade da CONTRATADA: A CONTRATADA deverá monitorar, por meios adequados, sua própria conformidade e a de seus empregados e subcontratadas 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.
- 27.2.11** Os relatórios acima citados deverão incluir, pelo menos:
- 27.2.11.1** o status dos sistemas de processamento de Dados Pessoais;
 - 27.2.11.2** as medidas de segurança;
 - 27.2.11.3** o tempo de inatividade registrado das medidas técnicas de segurança;



- 27.2.11.4** a (não) conformidade estabelecida com as medidas organizacionais;
- 27.2.11.5** quaisquer eventuais violações de dados e/ou incidentes de segurança;
- 27.2.11.6** as ameaças percebidas à segurança e aos Dados Pessoais; e
- 27.2.11.7** as melhorias exigidas e/ou recomendadas.
- 27.2.12** 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.
- 27.2.13** Notificação: A CONTRATADA deverá notificar a CONTRATANTE em até 24h (vinte e quatro) horas em caso de:
- 27.2.13.1** qualquer descumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais;
- 27.2.13.2** qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais;
- 27.2.13.3** qualquer violação de segurança na CONTRATADA;
- 27.2.13.4** quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; e
- 27.2.13.5** ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente.
- 27.2.14** Colaboração: A CONTRATADA compromete-se a auxiliar a CONTRATANTE:
- 27.2.14.1** 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
- 27.2.14.2** no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.
- 27.2.15** 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.



- 27.2.16** Tratamento de dados no exterior: Todo e qualquer tratamento de dados fora do Brasil, dependerá de autorização prévia e por escrito pela CONTRATANTE à CONTRATADA.
- 27.2.17** 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.
- 27.2.18** 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.
- 27.2.19** 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.
- 27.2.20** Solicitação de Dados ou Registros: Sempre que Dados ou Registros forem solicitados pela CONTRATANTE à CONTRATADA, ela 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.
- 27.2.21** Devolução dos Dados: A CONTRATADA deverá devolver todos os Dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que:
- 27.2.21.1** a CONTRATANTE solicitar;
 - 27.2.21.2** o Contrato for rescindido; ou
 - 27.2.21.3** com o término do contrato.
- 27.2.22** A CONTRATADA não deverá guardar, armazenar ou reter os Dados por tempo superior ao prazo legal ou necessário para a execução do Contrato.
- 27.2.23** 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.



- 27.2.24** 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.

ANEXO IV
ESPECIFICAÇÕES TÉCNICAS**REQUISITOS TÉCNICOS DA SOLUÇÃO DE GOVERNANÇA E**
ADMINISTRAÇÃO DE IDENTIDADE

Todos os requisitos da contratação devem ser entregues licenciados e palavras como deve, permite, suporta, efetua, proporciona, possui etc. significam que a funcionalidade deve ser entregue operacional, sem ônus adicional à CONTRATANTE.

1. Gerais

1.1. Todas as capacidades são especificadas em seu requisito mínimo, podendo ser entregue capacidade superior. Todos os requisitos devem garantir a compatibilidade às versões especificadas e superiores.

1.2. Não serão aceitas soluções de segurança customizadas para o BASA. Serão aceitos somente aquelas soluções que fizerem parte do portfólio de soluções oferecidas pelos fabricantes para o mercado corporativo.

1.3. A solução deve ser oferecida na modalidade SaaS baseada em microsserviços, garantindo escalabilidade e alta disponibilidade automatizados.

1.4. A solução deve possuir uma interface responsiva que permita que a experiência do usuário final seja simples, independente do dispositivo usado.

1.5. A solução deve fornecer atualizações automáticas, sem exigir tempo de parada (downtime), janelas de manutenção programadas ou intervenção dos administradores.

1.6. A solução deve ser projetada para alta disponibilidade e redundância, com infraestrutura projetada para maximizar o tempo de atividade e minimizar interrupções, utilizando estratégias contra falhas de forma automatizada assim como balanceamento de carga. Como parte da redundância, a solução deverá ter mecanismos contra recuperação de desastres (ambiente segregado) incluso na oferta da solução.

1.7. A CONTRATADA deverá fornecer plano de contingência para o caso de indisponibilidade da solução de modo que não haja impactos para o usuário final.

1.8. O fabricante deve fornecer um painel de acompanhamento de disponibilidade e saúde da solução para que o time do BASA possa visualizar as estatísticas de tempo de atividade da plataforma e detalhes sobre quaisquer interrupções de serviço.

1.9. A solução deve ser dimensionada automaticamente para acomodar picos de uso, como por exemplo certificações trimestrais ou anuais.

1.10. A solução deve suportar a integração com soluções de segurança e gerenciamento de eventos (SIEM).

1.11. A solução deve possuir mecanismos de backup (incluso na oferta da solução) que permita realizar backups e restaurações de configurações, assegurando a recuperação eficiente e a continuidade operacional em caso de falhas ou necessidades de recuperação de dados.

1.12. Caso o conector da solução seja fornecido na forma de Appliance Virtual, as máquinas virtuais devem ser compatíveis com VMware ESXi versão 7 ou superior;

1.13. Caso o conector a solução seja fornecido em máquinas virtuais Windows Server, não é necessário fornecer licenças para o referido sistema operacional. A solução deve ser compatível com a versão Windows Server 2022 Datacenter ou superior;

1.14. Caso o conector da solução seja fornecido em máquinas virtuais Red Hat, esta deve ser compatível com a versão Enterprise Linux 8 ou superior;



1.15. Serão admitidas soluções que possuam banco de dados proprietários, desde que estejam instalados em Appliances Virtuais;

1.16. Caso a solução não possua banco de dados proprietário, ela deverá ser compatível com Microsoft SQL Server (versão atual) Enterprise Edition ou superior ou Oracle 19c ou superior;

2. Plataforma.

2.1. A solução deve possuir uma interface web única para os administradores configurarem conectores e fluxos de trabalho para integrações com os sistemas conectados.

2.2. A solução deve fornecer templates de e-mail pré-definidos e permitir customizações para adequar ao plano de comunicação corporativo.

2.3. A solução deve fornecer atualizações automáticas aos conectores sem gerar indisponibilidade nas integrações.

2.4. A plataforma deve possuir Inteligência Artificial Generativa para auxiliar na codificação de conectores e integrações, incluindo sugestões de melhor utilização das APIs da plataforma, sugestões de como criar um workflow de integração para melhor alinhar a necessidade de negócio com as capacidades da plataforma e sugestões de criação de conectores customizados para integração com sistemas legados.

2.5. A solução deve fornecer atualizações para adoção de novas funcionalidades para uso imediato, sem a necessidade de upgrades de versão ou migrações.

2.6. A solução deve fornecer a capacidade de aplicar algoritmos de IA avançados (LLM) para gerar sugestões de descrições dos acessos do catálogo de direitos, abrangendo todos os direitos descobertos pela solução dos sistemas integrados.

2.7. A solução deve fornecer um fluxo de autosserviço para que as pessoas chave (como por exemplo os responsáveis pelos direitos de acesso) possam revisar (acatar ou ajustar) as descrições geradas por IA melhorando a qualidade dos dados e enriquecendo os acessos do ambiente.

2.8. A solução deve ser capaz de fornecer recomendações baseadas em inteligência artificial sobre regras de correlação entre contas e identidades.

2.9. A solução deve possuir métodos de aprendizado de máquina, facilitando a adoção e a eficácia dos controles de segurança com base em dados analíticos e preditivos.

2.10. A solução deve possibilitar a exportação e importação das configurações de forma simples e segura, facilitando a migração e o gerenciamento de mudanças sem comprometer a integridade dos dados.

2.11. A solução deve incluir funcionalidades para criar formulários web personalizáveis que possam ser integrados em processos de negócios maiores, facilitando a interação humana necessária para respostas a eventos específicos.

2.12. A solução SaaS deve ser capaz de se conectar nos sistemas on-premises e aplicações autoritativas ao qual irá realizar o provisionamento e atualização de dados sem a necessidade de abertura de portas adicionais no firewall além das portas já abertas.

3. Ciclo de vida de Identidade

3.1. A solução deve funcionar como um sistema de registro (fonte cadastral/autoritativa) das populações de identidades caso não exista uma fonte autoritativa através de formulários próprios da solução.

3.2. A solução deve ser capaz de utilizar informações de qualquer atributo da identidade para geração do identificador único, inclusive com a possibilidade de gerar este valor de forma automática, tanto na plataforma de governança quanto ao provisionar contas nas aplicações integradas.



3.3. A solução deve oferecer suporte a um esquema de atributos de identidade flexível para modelagem das identidades.

3.4. A solução deve permitir a criação de novos atributos de uma identidade por meio de sua interface gráfica de administração.

3.5. A solução deve permitir que determinados atributos de identidade sejam obtidos de múltiplos sistemas, além da fonte autoritativa de pessoas.

3.6. A solução deve permitir manipular (transformar) os valores de atributos antes de definir o valor dos atributos de identidade.

3.7. A solução deve permitir manipular (transformar) valores de atributos antes de provisioná-los para contas vinculadas nos sistemas integrados.

3.8. A solução deve permitir que os atributos das identidades da plataforma possam ser sincronizados com os sistemas conectados de acordo com a necessidade.

3.9. A solução deve permitir o mapeamento de quais atributos de usuário serão coletados em sistemas proprietários, pacotes de mercado, aplicações SaaS e provedores de infraestrutura de nuvem.

3.10. A solução deve fornecer uma maneira configurável de identificar o conjunto de atributos que irão vincular automaticamente as contas dos sistemas conectados às identidades conhecidas pela plataforma.

3.11. A solução deve permitir o relacionamento de uma determinada identidade digital a múltiplas contas dos sistemas conectados.

3.12. A solução deve permitir criar diferentes estados do ciclo de vida de uma identidade com base nas informações dos sistemas autoritativos, como por exemplo: ativo, em férias, licença/afastamento, desligado etc.

3.13. A solução deverá permitir o gerenciamento dos acessos nos sistemas conectados, de acordo com informações organizacionais dos sistemas autoritativos, ou com base no estado do ciclo de vida de uma identidade, como por exemplo: ativo, licença, em férias, desligado etc.

4. Conectores e Integrações

4.1. A solução deve oferecer conectores nativos, que suportem processos de provisionamento e reconciliação, capazes de se conectar com sistemas on-premises:

- 4.1.1. Oracle PeopleSoft;
- 4.1.2. Beyondtrust (solução de PAM);
- 4.1.3. Diretórios LDAP diversos;
- 4.1.4. Red Hat Single Sign-On (RHSSO);
- 4.1.5. Infraestrutura de Banco de Dados (Oracle, Microsoft SQL Server);
- 4.1.6. Sistemas Operacionais (Servidores Linux RedHat, Ubuntu, CentOS);
- 4.1.7. Sistemas Operacionais (Servidores Windows).

4.2. A solução deve oferecer conectores nativos, que suportem processos de provisionamento e reconciliação, capazes de se conectar com sistemas em nuvem (Aplicações SaaS):

- 4.2.1. AzureAD/Office365 (Entra ID);
- 4.2.2. WebServices (REST, SOAP, SCIM);
- 4.2.3. Service Now;
- 4.2.4. Tenable One;



4.2.5. KnowBe4;

4.2.6. CrowdStrike Falcon.

4.3 A solução deve ser capaz de se integrar a vários domínios/florestas do Active Directory e a várias tecnologias de diretório LDAP, além de apenas um único domínio do Active Directory.

4.4. A solução deve ser capaz de se integrar a aplicações legadas ou proprietárias, através de conectores nativos da solução, utilizando protocolos de mercado, tais como REST, SOAP, SCIM e JDBC.

4.5. A solução deve permitir o desenvolvimento de conectores customizados e integrações com outras plataformas, através da disponibilização de SDKs.

4.6. Os conectores devem oferecer suporte a operações padrão de provisionamento de contas: criar, modificar, excluir, ativar, desativar e desbloquear.

4.7. Os conectores devem ser compatíveis com a adição e a remoção de acesso a contas nos sistemas integrados.

4.8. A solução deve ser capaz de se integrar a soluções IPaaS (Integration Platform as a Service) de terceiros, fluxos de trabalho externos ou outros barramentos de eventos.

4.9. A solução deve ser capaz de executar chamadas de APIs externas, com base em gatilhos disparados por eventos da própria solução.

4.10. A solução deve oferecer integração nativa com sistemas de colaboração, como por exemplo o Microsoft Teams, para iniciar e aprovar solicitações de acesso.

4.11 A solução deverá ter a capacidade de ser integrar com sistemas de gerenciamento de solicitações de serviço ou ITSM de terceiros, como o Service Now, BMC e Cherwell.

4.12. Para o caso de sistemas desconectados, a solução deve oferecer integração com os principais sistemas de ITSM para abertura tíquetes em vez de efetuar provisionamento direto.

4.13. A solução deve disponibilizar todas as suas funcionalidades através de APIs REST. Tais APIs devem possibilitar, por exemplo, criar perfis, gerenciar regras de concessão, iniciar e consultar campanhas de revisão de acesso, consumir dados, carregar dados, entre outros;

4.14. A solução deve disponibilizar os links para a documentação da configuração do conector desejado diretamente da interface web de configuração e administração de conectores.

4.15. A solução deve ser capaz de se integrar com a solução de PAM Beyondtrust para realizar o consumo de credenciais/senhas de acesso dos conectores de integração utilizados na plataforma, evitando armazenar as senhas das contas de serviço.

4.16. A solução não deve exigir que plug-ins ou outros softwares sejam instalados diretamente no Controlador de Domínio do Active Directory.

4.17. A solução deve fornecer conectividade para aplicativos não baseados em UI, como Linux e Unix.

4.18. Os conectores devem suportar reconciliação agendada, para que as alterações feitas fora da solução IGA sejam carregadas e visíveis.

4.19. A solução deve ser capaz de carregar (agregar) contas de usuários e direitos de aplicativos conectados, para detectar alterações feitas nesses sistemas.

4.20. A solução não deve ter conhecimento de credenciais/tokens de contas de serviço durante o provisionamento de aplicativos e serviços corporativos.



- 4.21. A solução deve ser orientada a eventos, garantindo que tanto a própria plataforma quanto os sistemas de terceiros tenham a capacidade de receber notificações em tempo real sobre eventos que ocorram dentro da plataforma.
- 4.22. A solução deve oferecer suporte ao provisionamento e à integração de terceiros por meio do processo de fluxo de trabalho.
- 4.23. A solução deve possuir a capacidade de armazenar e rotacionar as credenciais utilizadas nos conectores através um cofre de senhas externo.
- 4.24. A solução deve possuir a capacidade de descobrir, conectar e configurar novas integrações de forma automática utilizando inteligência artificial.
5. Gerenciamento de Direitos
 - 5.1. A solução deve ser capaz de efetuar a leitura de contas de usuários e permissões de acessos (direitos) dos aplicativos integrados e consolidar em um catálogo centralizado de governança, para ser possível a detecção de alterações feitas de forma direta nesses aplicativos.
 - 5.2. Os conectores devem oferecer suporte ao agendamento das atividades de reconciliação de contas e direitos, além de permitir execuções manuais através de sua interface WEB e/ou através de execução de APIs.
 - 5.3. A solução deve se integrar aos principais fornecedores de PAM, como por exemplo o BeyondTrust, fornecendo ampla visibilidade das permissões de acesso, facilitando a governança centralizada e o gerenciamento/provisionamento do ciclo de vida dos usuários com acesso a contas privilegiadas gerenciadas pelo sistema de PAM.
 - 5.4. A solução deve permitir solicitações de acessos a direitos individuais (grupos, telas, funcionalidades), conjuntos de direitos/grupos de direitos (perfis de acessos) e/ou perfis funcionais.
6. Gerenciamento de Senhas
 - 6.1. A solução deve fornecer uma função de autoatendimento para alterar a senha de um sistema específico ou de um grupo de sistemas cuja senha deverá ser sincronizada.
 - 6.2. A solução deve ter a capacidade de exigir autenticação multifator no processo de troca ou esquecimento de senha (sem a necessidade de interação direta com a central de ajuda), utilizando métodos como envio de Tokens OTP através de SMS, chamada de voz e e-mail ou outros métodos para verificar a identidade pessoal. O envio de OTPs através de SMS/Chamada de Voz não deve gerar custo adicional.
 - 6.3. A solução deve ofertar interface nativa para permitir que os usuários finais possam cadastrar suas informações, tais como e-mail pessoal, telefone pessoal e perguntas de segurança.
 - 6.4. A solução deve permitir que usuários com perfis de helpdesk possam enviar um link de acesso para que usuários redefinam suas senhas.
 - 6.5. A solução deve incluir um plug-in do MS Windows Credential Provider/GINA para acessar o recurso de redefinição de senha nas telas de login e bloqueio do Windows.
 - 6.6. A solução deve oferecer suporte à interceptação de senha para domínios Microsoft Active Directory visando o sincronismo da senha entre a solução e as demais aplicações integradas quando a senha é alterada diretamente no controlador de domínio ou através de Desktops.
 - 6.7. A solução não deve armazenar nenhuma senha de usuário em texto claro ou em um formato de criptografia reversível para identidades gerenciadas.
 - 6.8. A solução deve fornecer políticas de senha configuráveis, permitindo opções de comprimento de senha, complexidade, tipos de caracteres e data de expiração que podem ser aplicadas em sistemas individuais ou em grupos de sistemas.



- 6.9. A solução deve permitir a criação de políticas de senha que não permitam que valores de atributos da conta sejam utilizados na composição da senha.
 - 6.10. A solução deve oferecer suporte à validação das senhas no próprio sistema de origem sempre que a senha esteja sendo definida a partir da solução de IGA, de forma que o histórico de senhas (do sistema de origem) possa ser um dos critérios para definição de novas senhas.
 - 6.11. A solução deve suportar diferentes políticas de senha, diferentes fontes para autenticação e possibilitar a configuração de diferentes mecanismos de autenticação forte de acordo com o tipo de identidade.
 - 6.12. A solução deve fornecer uma interface responsiva onde o usuário final possa restabelecer a sua senha de acesso através de navegadores Desktop ou mobile.
 - 6.13. A solução deve fornecer a capacidade de gerenciamento de senhas entre vários tipos de sistemas, por exemplo, bancos de dados, diretórios como Active Directory, aplicações SaaS etc., incluindo a possibilidade de sincronizar a alteração destas senhas, conforme política configurada.
 - 6.14. A solução não deve permitir que a equipe de suporte técnico defina ou veja a senha de uma identidade.
 - 6.15. A solução não deve armazenar senhas redefinidas ou sincronizadas por meio do sistema.
 - 6.16. A solução deve prover um sistema de gestão de senhas integrado que funcione com aplicações tanto locais quanto em ambientes de nuvem, que possibilite ao usuário a recuperação e alteração de suas próprias senhas, assegurando a administração de credenciais em diversas plataformas de forma centralizada.
 - 6.17. Deve haver suporte para gerenciamento de senhas em sistemas legados, garantindo compatibilidade e segurança em todo o ecossistema tecnológico.
 - 6.18. A solução deve permitir a criação de exceções nas políticas de senha para grupos específicos de usuários, levando em consideração atributos de identidade distintos, possibilitando uma gestão de segurança flexível e adaptada às necessidades organizacionais.
 - 6.19. A solução deve prover uma interface intuitiva e segura para que os administradores realizem alterações ad hoc em senhas, atendendo a situações imprevistas ou requisitos emergenciais de segurança.
 - 6.20. É fundamental que a solução permita a implementação e gerenciamento de múltiplas políticas de senha, personalizáveis para cada aplicação, reforçando a segurança e adequação ao contexto de uso de cada sistema.
7. Gestão de Perfis
- 7.1. A solução deve suportar a criação de perfis funcionais (mapeadas para um cargo/função ou estrutura organizacional) e perfis de acesso (pacotes ou conjuntos de direitos).
 - 7.2. A solução deve permitir a criação de perfis funcionais e perfis de acesso no modelo RBAC.
 - 7.3. A solução deve permitir que os perfis de negócio possuam uma regra de associação automática, e que tais regras possam ser baseadas em atributos da identidade, atributos da conta ou ainda baseada em algum acesso específico da aplicação (por exemplo, um grupo LDAP).
 - 7.4. A solução deve permitir que novos acessos incluídos num perfil sejam provisionados automaticamente para as identidades que possuírem o perfil previamente atribuído.



- 7.5. A solução deve permitir configurar os perfis de acesso de forma granular, controlando a obrigatoriedade (ou não) de etapas de aprovação para concessão ou revogação de acessos.
- 7.6. A solução deve possuir a funcionalidade de mineração de perfis, onde novos perfis são automaticamente sugeridos através das combinações de acessos atuais e de atributos das identidades previamente definidos, analisados utilizando inteligência artificial.
- 7.7. A solução deve auxiliar no processo de evolução de perfis, utilizando inteligência artificial, para sugerir automaticamente novas permissões (direitos) a serem adicionadas nos perfis existentes.
- 7.8. A solução deve identificar acessos comuns aos perfis minerados ou sugeridos, evitando gerar sobreposição e duplicidade de acessos nos perfis.
- 7.9. A solução deve analisar continuamente as combinações de acessos das identidades de um sistema integrado e sugerir a atualização de perfis existentes ou a criação de novos perfis.
- 7.10. A solução deve possibilitar a configuração de papéis especializados alinhados com projetos específicos, departamentos ou funções, reforçando a gestão de acessos baseada nas responsabilidades organizacionais.
- 7.11. A solução deve apresentar uma funcionalidade para salvar configurações de papéis em estado de rascunho, permitindo revisões futuras e ativação conforme necessário.
- 7.12. A solução deve oferecer um mecanismo automatizado para a atribuição e revogação de papéis de usuários, baseando-se em critérios pré-estabelecidos para garantir a governança de acesso.
- 7.13. A solução deve possuir uma interface centralizada que consolide a visualização e gestão de papéis, direitos e identidades associadas, permitindo uma visão integrada e simplificada ('single pane of glass') para administradores.
- 7.14. A solução deve oferecer a capacidade de incorporar e exibir dados de atividades, com base na atividade do usuário, ao recomendar o acesso a ser potencialmente incluído nas funções (papéis).
- 7.15. A solução deve possibilitar a criação e atribuição de papéis comuns, adaptáveis a todos os colaboradores ou segmentados por localização e outros critérios não relacionados à função específica do empregado.
- 7.16. A solução deve disponibilizar um portal para solicitações de papéis e acesso de forma self-service, integrada a um fluxo de trabalho de aprovação para gerenciamento e controle de concessões de acesso.
8. Governança e Auditoria
 - 8.1. A solução deve ser capaz de efetuar reconciliações com os sistemas integrados e detectar de forma nativa quaisquer alterações a nível de contas gerenciadas, tais como mudanças de atributo, concessão ou remoção de acessos feitas fora da plataforma/processo de governança. Ao detectar tais alterações, a solução deve permitir ainda a configuração de fluxos de trabalho automatizados para análise e auto remediação do evento de mudança não autorizado.
 - 8.2. A solução deve identificar contas órfãs (contas de sistemas que não possuem uma identidade relacionada) de forma automática e oferecer opções para lidar com essas contas, como por exemplo, revisar os seus acessos.
 - 8.3. A solução deve descobrir novas contas em sistemas gerenciados, que foram criadas fora da solução de governança.
9. Provisionamento



- 9.1. A solução deve oferecer flexibilidade para determinar a situação empregatícia (status), como por exemplo pré-contratação, ativo, férias, desligado etc. e ser capaz de provisionar ações nos sistemas conectados com base nas mudanças de estado.
- 9.2. A solução deve ser capaz de configurar regras para o provisionamento com base no tipo de usuário (ex. Funcionário, terceiro, parceiro etc.).
- 9.3. A solução deve oferecer suporte à configuração de fluxos de trabalho com base em cenários de admissão (joiner), transferência (mover) ou desligamento (leaver).
- 9.4. A solução deve oferecer suporte a desligamento de contas de forma unificada e imediata.
- 9.5. A solução deve suportar processos flexíveis para cenários de desligamento com base nas aplicações, como por exemplo: desativar conta, excluir conta, mover conta de estrutura organizacional etc.
- 9.6. A solução deve oferecer suporte ao provisionamento ou desprovisionamento automático de acessos das contas nos sistemas de destino com base nos atributos da identidade ou da fonte autoritativa.
- 9.7. A solução deve ser capaz de provisionar acessos com base em perfis funcionais usando critérios personalizados de atribuição.
- 9.8. A solução deve permitir que administradores definam os critérios de atribuição dos perfis funcionais ou políticas de provisionamento através de mecanismos "no-code". Tais mecanismos devem estar disponíveis na interface web da solução.
- 9.9. A solução deve oferecer suporte a eventos de provisionamento com base em atributos de várias fontes para cada identidade.
- 9.10. A solução deve oferecer mecanismos de sincronismo de atributos de forma imediata para manter os principais dados de uma identidade sempre atualizados nos sistemas conectados, tais como e-mail, nome, sobrenome, departamento etc.
- 9.11. A solução deve permitir que sistemas externos (aplicações personalizadas, SIEM etc.) sejam capazes de extrair dados da plataforma para fins de monitoramento.
- 9.12. A solução deve ser capaz de enviar logs de eventos para uma solução de SIEM em formato compatível com o padrão de mercado (ex: syslog).
- 9.13. A solução deve ser capaz de gerar atributos exclusivos no momento do provisionamento com base nos dados coletados de uma identidade.
- 9.14. A solução deve permitir a criação de atributos de identidade personalizados.
- 9.15. A solução deve permitir a criação de atributos baseados em regras complexas, como por exemplo a junção de dois atributos diferentes (nome completo) ou atributos calculados (status baseados em datas).
- 9.16. A solução deve suportar provisionamento e desprovisionamento flexíveis, ajustando-se automaticamente ao status de emprego do indivíduo. Por exemplo: Pré-contratação (fornecer acesso básico necessário antes da data de início) e licença de longo prazo (Retenção de acesso apenas ao email).
- 9.17. A solução não deve depender primariamente de agentes instalados juntos com os sistemas e aplicações existentes para as operações de provisionamento, assegurando uma redução de risco de impacto nos sistemas atuais. Caso seja requerido a interceptação de credenciais no AD para replicação e sincronismo de senhas, para este caso, será permitido a instalação local.
- 9.18. A solução deve permitir a configuração para reagregar (atualizar) contas de usuários e acessos, além de detectar quaisquer mudanças nativas realizadas fora da plataforma, garantindo consistência e integridade dos dados de acesso.



- 9.19. A solução deve ser capaz de identificar alterações realizadas diretamente nos sistemas de origem, permitindo que os administradores realizem ações de auto remediação ou configuração de alertas baseados no risco associado a essa mudança.
- 9.20. A solução deve ter a capacidade de executar transformações nos valores dos atributos durante dois processos chave:
 - 9.20.1. ao importar os dados das fontes autoritativas para a plataforma;
 - 9.20.2. ao atualizar dados aos sistemas.
- 9.21. A solução deve oferecer suporte ao direcionamento do acesso a contas específicas sempre que houver múltiplas contas em vigor para a mesma identidade.
- 9.22. Ao conceder acesso aos direitos dentro dos sistemas-alvo, a solução deve ser capaz de verificar se as contas necessárias já existem e, caso não existam, deve ser capaz de criar as contas antes do concedimento do acesso, facilitando um gerenciamento de acesso mais eficaz e seguro.
10. Relatórios, Analytics e Extração de Dados
 - 10.1. A solução deve recalcular automaticamente o risco potencial de uma identidade e identificar possíveis "acumuladores" de privilégios (acessos atípicos), com base em algoritmos de Inteligência Artificial.
 - 10.2. A solução deve rastrear e registrar as atividades de acesso às aplicações, fornecendo dados essenciais para o gerenciamento de licenças, análise de utilização e monitoramento de acesso para fins de segurança e conformidade.
 - 10.3. A solução deve possuir dashboards que suportem KPIs de provisionamento, contendo por exemplo, número de identidades e provisionadas por sistema, adesão a SLAs etc.
 - 10.4. A solução deve fornecer dashboards que suportem KPIs relacionados a solicitações de acesso ad-hoc, por exemplo, fornecendo informações sobre itens de acesso mais solicitados, proporção de acessos aprovados/rejeitados por aplicação, tempo médio de requisição até o provisionamento, departamentos com mais solicitações de acessos por período etc.;
 - 10.5. A solução deve permitir que administradores personalizem dashboards / KPIs na solução sem a necessidade de codificação ou customização.
 - 10.6. A solução deve prover relatórios de histórico de acesso para mostrar as alterações de uma identidade, seus acessos e eventos de governança relacionados ao longo do tempo.
 - 10.7. A solução deve ser capaz de exportar relatório em formato CSV, XLSX e PDF.
 - 10.8. A solução deve permitir a criação de gráficos e dashboards customizados, de forma flexível em sua própria interface web, sem a necessidade de desenvolvimento em ferramentas externas, com a possibilidade de compartilhamento com demais usuários autorizados, contendo indicadores do tipo:
 - 10.8.1. Métricas de Solicitações de Acessos por perfil, acesso, aplicação;
 - 10.8.2. Métricas de Revisão de Acessos por gestor, departamento, acessos revogados x mantidos;
 - 10.8.3. Métricas de Provisionamento de Acessos, como por exemplo volumetrias de acessos provisionados por aplicação com sucesso ou com falha;
 - 10.8.4. Volumetria de Onboarding x Transferências x Desligamento de Identidades;
 - 10.8.5. Volumetria de Identidades Ativas & Inativas;



- 10.9. A solução deve permitir comparar os acessos de um usuário em um intervalo de datas, mostrando as alterações que ocorreram com este usuário neste período.
- 10.10. A solução deve permitir a criação de políticas de acesso através do resultado de pesquisas realizadas na plataforma.
- 10.11. A solução deve incluir um painel de controle (dashboard) que possibilite o monitoramento automatizado e contínuo das identidades com padrões de acesso atípicos dentro da organização. Este painel deve ser capaz de identificar e destacar riscos sem necessitar de configurações ou parametrizações adicionais. Além disso, deve oferecer funcionalidades como o início de micro certificações de acesso para as identidades sinalizadas, facilitando ações imediatas de contenção e remediação de potenciais riscos identificados.
- 10.12. A solução deve disponibilizar um nível de pontuação automático que indique o potencial risco que a identidade com acessos atípicos representa na organização.
- 10.13. A solução deve prover contexto sobre as identidades e os acessos considerados atípicos, indicando por exemplo, uma visão quantitativa da combinação de acessos potencialmente excessivos, bem como quais são os acessos.
- 10.14. A solução deve fornecer dashboards nativos que suportem KPIs de certificação de acessos relacionados aos revisores - permitindo, por exemplo, identificar o comportamento dos revisores (se estão aprovando tudo, se estão demorando muito, se possuem muitos itens de revisão etc.);
- 10.15. A solução deve fornecer dashboards nativos que suportem KPIs de certificação de acessos relacionados a aplicações - permitindo, por exemplo, identificar aplicações com maior número de revogações, acessos com maior revogação / aprovação etc.
- 10.16. A solução deve fornecer um relatório nativo que mostre o status de qualquer item de acesso revogado numa campanha de revisão de acessos.
- 10.17. A solução deve fornecer relatórios de todas as atividades de revisão de acessos para análises de auditoria e para atender aos requisitos de conformidade.
- 10.18. A solução deve fornecer dashboards relacionados a solicitações de acesso - por exemplo, organizações com alto volume de solicitações, fornecendo insights sobre itens que podem ser candidatos a papéis, itens de acesso mais solicitados, solicitações de acesso mais rejeitadas etc.
- 10.19. A solução deve prover uma interface visual no formato de linha do tempo contendo dados históricos de acessos de uma identidade, permitindo por exemplo consultar de forma ágil e amigável eventos de adição/remoção acessos, incluindo alterações de atributos de identidade e contas, funções e direitos adicionados/removidos etc.
- 10.20. Deverá ser entregue um relatório detalhado de status das campanhas de revisão de acessos para evidenciar o processamento das decisões de revogação da certificação.
- 10.21. O relatório de status das campanhas deverá conter no mínimo, as seguintes informações:
 - 10.21.1. Nome e identificador da campanha de revisão de acessos
 - 10.21.2. Revisor(es)
 - 10.21.3. Identidades que foram revisadas
 - 10.21.4. Listas de sistemas e aplicações
 - 10.21.5. Administrador ou responsável pela campanha
 - 10.21.6. Conta no sistema
 - 10.21.7. Item de acesso revisado



- 10.21.8. Descrição do item de acesso revisado
- 10.21.9. Decisão tomada pelo revisor
- 10.21.10. Comentários da decisão (se comentado)
- 10.21.11. Data e hora da decisão feita
- 10.21.12. Se a decisão sobre o item de acesso for revogada, informar se a revogação foi executada
- 10.22. Deverá ser entregue um relatório detalhado de remediação das campanhas de revisão de acessos para evidenciar o processamento das decisões de revogação da certificação.
- 10.23. O relatório de remediação deverá conter no mínimo, as seguintes informações:
 - 10.23.1. Identidades que foram revisadas
 - 10.23.2. Listas de sistemas e aplicações
 - 10.23.3. Conta no sistema
 - 10.23.4. Item de acesso revisado
 - 10.23.5. Descrição do item de acesso revisado
 - 10.23.6. Comentários da decisão (se comentado)
 - 10.23.7. Status da revogação no sistema destino quando for decidido por ela
 - 10.23.8. Revisor que tomou a decisão de revogar
 - 10.23.9. Se a decisão sobre o item de acesso for revogada, informar se a revogação foi executada
- 10.24. Os relatórios de remediação devem estar disponíveis para mostrar o processamento em ciclo fechado das decisões de revogação de certificação
- 10.25. Os relatórios de histórico de acesso devem ser capazes de filtrar as informações baseado em datas específicas, mostrando uma "fotografia" dos acessos e perfis de uma identidade naquele momento, além de poder filtrar por um período de data. Também deve ser capaz de comparar duas datas e mostrar a diferença de acessos e perfis nesses dois períodos selecionados.
- 11. Buscas
 - 11.1. A solução deve suportar a realização de pesquisas complexas em toda a sua base de dados, a partir de um ponto único, incluindo a possibilidade de criação de pesquisas aninhadas.
 - 11.2. A solução deve possuir um mecanismo de pesquisa em linguagem natural para explorar os dados dentro do sistema.
 - 11.3. A solução deve permitir que o processo de busca nos dados seja realizado de forma simples e intuitiva, sem a necessidade de utilizar linguagens complexas como queries SQL.
 - 11.4. A solução deve possuir funcionalidade de busca onde o administrador possa realizar pesquisas sobre identidades, contas, perfis, atividades, eventos etc.
 - 11.5. A solução deve permitir que relatórios possam ser gerados a partir de pesquisas nos dados da solução.
 - 11.6. A solução deve permitir que os resultados de uma pesquisa possam ser exportados no formato CSV para facilitar o compartilhamento de informações.
 - 11.7. A solução deve ser capaz de salvar pesquisas realizadas para execução futura, sem a necessidade de reconstruir os parâmetros da pesquisa.



- 11.8. A solução deve permitir que histórico de pesquisa e pesquisas sugeridas fiquem disponíveis para facilitar a operação e administração da solução.
- 11.9. A solução deve sugerir pesquisas comumente executadas.
- 11.10. A solução deve permitir que uma pesquisa agendada possa iniciar um fluxo de trabalho e que os dados da pesquisa possam ser utilizados para integrações ou ações automatizadas na própria solução.
- 11.11. A solução deve possuir a capacidade de agendar e executar automaticamente pesquisas pré-configuradas em intervalos definidos e ajustáveis pelo usuário, com a finalidade de compilar e entregar relatórios periódicos que sintetizam os resultados obtidos dessas pesquisas.
- 11.12. A solução deverá oferecer uma interface de programação de aplicações (API) do tipo REST, que permita a execução de funções de pesquisa por sistemas externos, permitindo que sistemas de terceiros realizem consultas e recebam resultados para uso em seus próprios fluxos de trabalho.
- 11.13. A solução deve fornecer uma funcionalidade de pesquisa integrada, executável através de fluxos de trabalho, que permita a execução de consultas em tempo real. Os resultados obtidos devem poder ser utilizados no próprio fluxo de trabalho para tomadas de decisão.
- 11.14. A solução deve permitir a criação de relatórios dinâmicos a partir do resultado das pesquisas.
- 11.15. A solução deve permitir a criação de certificações de acesso a partir do resultado de pesquisas realizadas na plataforma.
- 11.16. A solução deve permitir a criação de políticas de acesso a partir do resultado de pesquisas realizadas na plataforma.
12. Revisão de Acessos
 - 12.1. A solução deverá fornecer a visualização do caminho de acesso (acesso efetivo) para acessos concedidos aos recursos de infraestrutura de provedores de nuvem (AWS, Azure e GCP) dentro das certificações de acessos, para oferecer suporte a decisões mais precisas e informadas aos revisores de acessos.
 - 12.2. A solução deve fornecer, de forma nativa, um relatório de confirmação das campanhas de revisão de acesso que indique que o acesso revogado tenha sido de fato removido nos sistemas de destino (closed-loop).
 - 12.3. A solução deve permitir a configuração de campanhas de revisão de acesso da composição dos perfis funcionais.
 - 12.4. A solução deve oferecer suporte a revisões de contas não vinculadas a uma identidade (órfãs), de modo que estas contas tenham seus direitos de acessos revisados conforme a necessidade.
 - 12.5. A solução deve permitir a geração de campanhas de revisão de acessos sob demanda.
 - 12.6. A solução deve permitir que as revisões de acesso sejam acionadas com base em eventos de uma identidade, como por exemplo, transferência de departamento, mudança de gestor etc.
 - 12.7. A solução deve permitir que aplicações externas possam enviar gatilhos que disparem revisões de acesso, como por exemplo, uma solução de ITDR, UEBA, SIEM etc.;
 - 12.8. A solução deve permitir que os administradores salvem as revisões de acesso como modelos para uso futuro.



- 12.9. A solução deve permitir que os administradores programem as revisões de acesso, para que sejam executadas de forma periódica e recorrente.
- 12.10. A solução deve permitir que os administradores visualizem os destinatários de uma campanha de revisão de acessos antes do início da campanha, e permita, por exemplo, que um administrador possa redefinir o(s) destinatário(s) da campanha.
- 12.11. A solução deve suportar várias campanhas de certificação ativas ao mesmo tempo.
- 12.12. A solução deve oferecer mecanismos de autosserviço para que o usuário efetue a redistribuição das campanhas de revisão de acesso por um período configurável.
- 12.13. A solução deve ser capaz de readequar o responsável pela campanha de revisão com base nos atributos da identidade, considerando processos internos de reestruturação, mudanças de gestores etc.
- 12.14. A solução deve notificar automaticamente os revisores de acesso quando uma campanha de revisão iniciar, bem como permitir o envio de lembretes antes do prazo final da campanha.
- 12.15. A solução deve permitir que os revisores de acesso tomem as decisões por aprovar ou revogar acessos, além de permitir que tais decisões possam ser alteradas pelos revisores antes de serem submetidas em definitivo.
- 12.16. A solução deverá exigir que o revisor "assine/ratifique" suas decisões, quando concluir todos os itens pendentes de revisão.
- 12.17. A solução deve permitir que o revisor indique uma data de revogação para um perfil de acesso ou função que está sendo revisada.
- 12.18. A solução deve permitir que os revisores tomem "decisões em massa" nas campanhas de revisão de acessos.
- 12.19. A solução deve fornecer informações sobre a identidade cujos acessos estão sendo revisados, devendo permitir que atributos da identidade como departamento, cargo, gestor, tipo de colaborador estejam disponíveis para aumentar o contexto do revisor do acesso. Se necessário, deve permitir a inclusão de novos atributos visíveis na identidade sem a necessidade de customizações ou codificação.
- 12.20. A solução deve fornecer recomendações de tomada de decisão durante as campanhas de revisão de acesso, por exemplo: recomendar se um determinado acesso deve ou não ser mantido e informar quais análises foram feitas para chegar a essa conclusão.
- 12.21. A solução deve permitir o fornecimento de dados de atividade (uso do sistema) aos revisores, pois tais dados podem ser relevantes para tomada de decisão (mitigação de riscos e/ou contenção de custos para aplicações SaaS).
- 12.22. A solução deve revogar automaticamente os acessos aos sistemas conectados assim que a campanha for finalizada e a decisão do revisor indicar pela revogação do acesso.
- 12.23. A solução deve permitir a configuração de campanhas de revisão de acesso de acordo com as características das identidades, permitindo, por exemplo, direcionar campanhas para todas as identidades ativas, de acordo com o gestor, estrutura departamental etc.;
- 12.24. A solução deve permitir a configuração de campanhas de revisão de acesso de acordo com os itens de acesso, como por exemplo, por sistema, função, perfil de acesso ou direito de acesso.
- 12.25. A solução deve permitir que nas campanhas de revisão da composição de acesso de perfis funcionais, os responsáveis possam contestar, por exemplo, o nome, a



descrição dos perfis, políticas de concessão automática e direitos de acesso que compõem os perfis funcionais.

- 12.26. A solução deve permitir que o escopo das campanhas de revisão de acessos possa ser filtrado com base nos resultados de pesquisas granulares, que permitam, por exemplo, combinar critérios de inclusão e/ou exclusão, de forma flexível.
- 12.27. A solução deve permitir que durante a definição de uma campanha de revisão de acessos, seja possível filtrar quais identidades e quais acessos devem fazer parte do escopo da campanha.
- 12.28. A solução deve permitir que as certificações de acesso sejam criadas automaticamente, de forma proativa, com base na detecção automática de combinações de acesso que possam representar riscos, por meio de algoritmos de IA.
- 12.29. A solução deve suportar a revisão de acessos a sistemas considerados como "desconectados", permitindo ainda que ações de provisionamento resultem na criação de tickets para execução manual numa solução de ITSM, ou à partir de tarefas manuais na própria solução.
- 12.30. A solução deve permitir que o revisor reatribua identidades ou itens de revisão em uma campanha de revisão de acesso.
- 12.31. A solução deve permitir que os revisores concluam as ações de certificação tanto em dispositivos móveis, como tablets, ou à partir de suas estações de trabalho por meio de uma aplicação web amigável para o usuário e responsiva.
- 12.32. A solução deve prover revisões de itens de acesso detalhadas por aplicação, função e direitos de acesso.
- 12.33. A solução deve permitir que as certificações sejam acionadas com base no nível de risco associado a cada identidade.
- 12.34. Deve ser possível reatribuir o trabalho de revisões de acesso dentro de um período configurável.
- 12.35. A solução deve prevenir a auto certificação, garantindo que a revisão e aprovação sejam realizadas por uma parte independente.
- 12.36. Os revisores devem ser informados sobre quais itens ainda não foram certificados anteriormente.
- 12.37. A solução deve prover uma validação para garantir que todos os acessos revogados sejam efetivamente removidos dos sistemas alvo.
- 12.38. A solução deve oferecer dashboards para KPIs de certificação, destacando questões como aprovações automáticas e atrasos na tomada de decisões dos revisores.
- 12.39. A solução deve possuir um dashboard destacando as aplicações com os maiores índices de revogação de acessos.
- 12.40. A solução deve gerar relatórios que mostrem o status atual de todos os itens de acesso revogados para garantir conformidade regulatória.
- 12.41. A solução deve permitir a criação de múltiplas certificações simultâneas.
- 12.42. A solução deve permitir que os revisores adicionem comentários e justificativas ao tomarem decisões sobre certificações.
- 12.43. A solução deve fornecer nas campanhas de revisão de acessos uma visão das informações de atividade (uso do sistema). Os dados de uso podem ser relevantes



para detectar baixo índice de atividades de uma identidade a um sistema e aumentar a efetividade das revisões de acessos.

- 12.44. A solução deve permitir revisões de identidade realizadas por gestores ou outros responsáveis designados.
- 12.45. A solução deve permitir filtrar e/ ou excluir identidades assim como acessos específicos para a execução de certificações de acesso
- 12.46. Os administradores devem ser capazes de definir certificações baseadas em critérios de pesquisa complexos de forma simplificada.
- 12.47. A solução deve fornecer aos certificadores contexto completo sobre os recursos de nuvem que um item de acesso concede, incluindo computação, armazenamento e rede.
- 12.48. Ao revisar, a solução deve suportar o reporte de uso ou não da aplicação/ acessos, auxiliando os revisores na tomada de decisão sobre a necessidade de acesso do usuário.

13. Segregação de Funções (SoD)

- 13.1. A solução deve suportar a criação de regras de segregação de funções entre diferentes tipos de aplicações.
- 13.2. A solução deve ser capaz de usar mecanismo de pesquisa granular para suportar a definição de políticas.
- 13.3. A solução deve permitir adicionar rótulos nas regras de SoD visando melhor identificação, como por exemplo risco, área de negócio, regulação etc.
- 13.4. A solução deve ser capaz de verificar as identidades para detectar violações das políticas de SOD.
- 13.5. A solução deve avaliar políticas de SoD de modo preventivo, ou seja, durante o processo de solicitação de acessos.
- 13.6. A solução deve permitir que relatórios de violações de SoD sejam agendados para execução em intervalos regulares e personalizáveis.
- 13.7. A solução deve permitir a criação de relatórios contendo as violações de regras de SoD.
- 13.8. A solução deve permitir descrever controles compensatórios para os riscos, e qual a recomendação de mitigação quando uma regra de SoD é criada, essas informações devem ficar visíveis para os solicitantes e aprovadores/revisores de uma solicitação de acessos quando detectado um conflito em potencial.
- 13.9. A solução deve detectar e permitir a criação de micro certificações de acessos direcionadas às identidades que possuem alguma violação de política de SoD.
- 13.10. A solução deve permitir que os aprovadores de uma solicitação de acesso sejam capazes de identificar facilmente que a solicitação está violando alguma política de SoD.

14. Segurança

- 14.1. A solução deve oferecer suporte à autenticação de um ID e senha locais.
- 14.2. A solução deve oferecer suporte à autenticação via Active Directory (LDAP).
- 14.3. A console de administração da solução deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.



- 14.4. A solução deve ser compatível com SAML2.0 ou OpenID Connect (OIDC) para autenticação por meio de provedores de soluções de Single Sign On.
- 14.5. A solução deve oferecer suporte a diferentes fontes de autenticação para diferentes populações de usuários.
- 14.6. A solução deve estar disponível a partir de qualquer rede, mas deve permitir por meio de sua interface de configuração que o administrador possa restringir, por exemplo, que o acesso seja feito a partir da rede corporativa. Esta funcionalidade deve poder ser aplicada de acordo com os diferentes tipos de identidade.
- 14.7. A solução deve ser compatível com Oauth 2.0 para autenticação em qualquer API REST disponível.
- 14.8. A solução deve ser capaz de se conectar com aplicações on-premises sem a necessidade de criação de túneis VPN, e sem a necessidade de abertura de conectividade do ambiente da solução para o datacenter.
- 14.9. O software fornecido deve permitir o acesso a suas interfaces através de um browser utilizando HTML5. A solução deve ser compatível com os navegadores: Google Chrome 126 e superiores, sendo executados no sistema operacional Windows 10 ou superior.
- 14.10. A solução deve proteger as credenciais das contas com pelo menos duas camadas de criptografia, incluindo os dados em repouso ou durante as movimentações
- 14.11. A solução deve prover suporte a criptografia dos backups armazenados.
- 14.12. O software deverá implementar o protocolo HTTPS, utilizando o TLS em sua versão 1.2 ou superior.
- 14.13. Todas as comunicações externas do software deverá ser encriptadas.
- 14.14. O software deve possuir mecanismo de múltiplo fator de autenticação (MFA);
- 14.15. O software deve possuir controles de segurança que protejam, no mínimo, contra os riscos de segurança mais críticos para aplicações web, conforme OWAPS Top10, quais sejam:
 - 14.15.1. Broken Access Control
 - 14.15.2. Cryptographic Failures
 - 14.15.3. Injection;
 - 14.15.4. Insecure Design
 - 14.15.5. Security Misconfiguration
 - 14.15.6. Vulnerable and Outdated Components
 - 14.15.7. Identification and Authentication Failures
 - 14.15.8. Software and Data Integrity Failures
 - 14.15.9. Security Logging and Monitoring Failures
 - 14.15.10. Server-Side Request Forgery (SSRF)
- 14.16. O fabricante da solução não deve possuir acesso às chaves de criptografia.
- 14.17. A solução deve prover rastreabilidade sobre as ações dentro do sistema, que podem ser usadas para atividades como auditoria, rastreamento de uso ou monitoramento de acesso.
15. Solicitação de Acessos



- 15.1. A solução deve suportar integração com sistemas como MS Teams e ServiceNow para iniciar e aprovar solicitações de acesso de forma nativa.
- 15.2. A solução deve oferecer suporte a solicitações de acesso ad-hoc, por meio de interface web, onde o usuário possa solicitar acessos a si próprio (autoatendimento), o gestor ou outros possam solicitar acessos para outras identidades na organização.
- 15.3. A solução deve suportar a solicitação de mais de um item de acesso para um ou para mais de um usuário simultaneamente.
- 15.4. A solução deve entregar recursos que reduzam atrito do usuário final através de mecanismos que destaquem automaticamente itens de acesso comuns que um usuário possa querer solicitar, com base em seu trabalho/função ou estrutura organizacional. Os itens de acesso em comum devem estar disponíveis e em destaque nas interfaces de solicitações de acesso do usuário, bem como disponíveis para consulta através de APIs REST.
- 15.5. A solução deve suportar solicitações de acesso temporário, onde uma data final para o acesso possa ser especificada. Ao término do período estipulado, o acesso deve ser revogado automaticamente no sistema conectado.
- 15.6. A solução deve oferecer suporte a verificações preventivas em relação às políticas de segregação de função (SOD) configuradas para evitar combinações tóxicas de acessos.
- 15.7. A solução deve permitir que os solicitantes de um acesso informem uma justificativa para a solicitação de um novo acesso.
- 15.8. A solução deve permitir que os administradores exijam (ou não) a inclusão de uma justificativa, de acordo com o item de acesso que é solicitado.
- 15.9. A solução deve permitir que os aprovadores possam adicionar comentários durante o processo de decisão de uma solicitação.
- 15.10. A solução deve oferecer suporte a fluxos de trabalho de aprovação por gestores imediatos, proprietários dos itens de acesso, proprietários de sistemas e grupos de aprovadores.
- 15.11. A solução deve ser configurável, de modo que diferentes itens de acesso possam exigir diferentes níveis/etapas de aprovação.
- 15.12. A solução deve suportar a opção de invocar fluxos externos que possam atualizar dinamicamente o processo de aprovação.
- 15.13. A solução deve oferecer suporte à capacidade de adicionar uma aprovação caso a(s) política(s) de SOD seja(m) violada(s) pelo provisionamento da solicitação.
- 15.14. A solução deve oferecer suporte à reatribuição dos itens de trabalho, tanto de forma temporária quanto permanente para a aprovação de solicitações de acesso.
- 15.15. A solução deve considerar uma solicitação como negada e interromper o fluxo, caso um dos aprovadores da cadeia de aprovação rejeite a solicitação.
- 15.16. A solução deve notificar por e-mail os atores envolvidos na solicitação, quando uma solicitação é negada.
- 15.17. A solução deve suportar a atribuição de aprovações a grupos ou equipes, onde qualquer pessoa do grupo possa aprovar em nome do grupo.
- 15.18. A solução deve exibir os passos do fluxo de solicitação de acesso, dando visibilidade ao solicitante de quais são as etapas do fluxo, desde a solicitação até a última milha de aprovação do acesso e provisionamento.



- 15.19. A solução deve permitir múltiplas aprovações na mesma solicitação de acesso.
- 15.20. A solução deve permitir que determinados itens de acessos tenham visibilidade restrita a populações de identidades específicas, evitando por exemplo que usuários de negócio tenham visibilidade para solicitar acessos a recursos administrativos (acessos privilegiados) inerentes à área de tecnologia.
- 15.21. A solução deve permitir que acessos a serem solicitados possam ser agrupados em aplicações lógicas, para garantir uma melhor experiência ao usuário final.
- 15.22. A solução deve permitir que usuários façam solicitações de acessos a partir de dispositivos móveis ou desktops, através de interface web amigável e responsiva.
- 15.23. A solução deve permitir que usuários efetuem aprovações de acessos a partir de dispositivos móveis ou desktops, através de interface web amigável e responsiva.
- 15.24. A solução deve efetuar o provisionamento de solicitações de acesso aprovadas de forma imediata aos sistemas conectados. Deve ser compatível tanto com o provisionamento direto pela plataforma quanto com o provisionamento indireto por meio do sistema de tíquetes.
- 15.25. A solução deve ser compatível com soluções de ITSM para efetuar a criação de tíquetes de provisionamento manual para solicitações de acesso aprovadas.
- 15.26. A solução deve disponibilizar APIs nativas para que requisições de acesso possam ser iniciadas(solicitadas), aprovadas/negadas, consultadas ou reatribuídas.

- 15.27. A solução deve suportar solicitações de acesso ad hoc por gerentes ou outros, solicitando em nome de outro indivíduo.
- 15.28. A solução deve fornecer sugestões de itens que um usuário possa querer solicitar, baseadas em seu trabalho/função ou equipe.
- 15.29. A solução deve suportar solicitações de acesso temporário, onde uma data final é especificada para acesso limitado.
- 15.30. A solução deve suportar a aprovação automática para itens de baixo risco, baseada em tags/metadados ou Inteligência Artificial (IA).
- 15.31. A solução deve manter um histórico de acesso para mostrar a linha do tempo de solicitação/aprovação de acesso.
- 15.32. O acesso solicitado deve poder ser agrupado em aplicações lógicas (baseadas em função de negócios), para abstrair detalhes dos usuários finais.
- 15.33. A solução deve suportar solicitações para direitos individuais, conjuntos/pacotes de direitos e papéis de negócios.
- 15.34. O provisionamento de solicitações de acesso aprovadas deve suportar tanto o provisionamento direto pela plataforma quanto o provisionamento indireto via sistema de tickets.
- 15.35. A solução deve permitir exceções no fluxo de trabalho de aprovação dos acessos. Por exemplo, um acesso crítico poderá ser aprovado por um responsável do Departamento Jurídico ou de Privacidade, e não pelo seu gerente imediato.
- 15.36. A solução deve permitir que gerentes solicitem a remoção de perfis de acesso ou papéis dos seus subordinados diretos com fluxos de trabalho de aprovação.
16. Workflow
 - 16.1. A solução deve ter a capacidade de acionar automaticamente fluxos de trabalho específicos com base nos resultados obtidos através de suas funcionalidades de



pesquisa. Este acionamento deve ser configurável, permitindo a definição de parâmetros e condições que, quando atendidas pelos resultados da pesquisa, iniciem o fluxo de trabalho designado.

- 16.2. A solução deve disponibilizar fluxos pré-definidos para ações de remediação automática de acessos, caso indivíduos com combinações de acessos atípicas sejam detectados na organização.
- 16.3. A solução deve possuir uma interface para criação de fluxos de trabalho do tipo "drag and drop" para que seja possível a automatização de tarefas sem a necessidade de codificação.
- 16.4. A solução deve fornecer um mecanismo de fácil uso, no formato "drag and drop" para criação de formulários personalizáveis através de sua interface web de administração.
- 16.5. A solução deve permitir a configuração de regras de negócio que permitam, por exemplo, aplicar abordagens baseadas em riscos para concessão, revisão ou aprovação de acessos.
- 16.6. A solução deverá permitir a implementação de fluxos personalizáveis utilizando recursos no-code, capazes de acessar APIs para integração e consumo de dados internos e externos à plataforma, para automação de processos de negócio diversos, inerentes à administração de identidades e acessos, como por exemplo em fluxos de:

16.6.1. Admissão: Provisionar "kits básicos" de acessos inerentes ao tipo de colaborador, cargo, função, enviar notificações, entre outros.

16.6.2. Transferência: Remover e/ou revisar e conceder acessos inerentes à nova função, enviar notificações, entre outros.

16.6.3. Desligamento: Remover acessos, desabilitar e/ou excluir contas, enviar notificações, entre outros.

16.6.4. Afastamento/Férias: Remover/adicionar acessos, desabilitar/habilitar contas nos sistemas integrados, enviar notificações, permitir períodos de exceção mediante fluxo de aprovação do gestor, entre outros.

- 16.7. A solução deve oferecer suporte nativo à aprovação automática para itens de baixo risco, com base em classificação/tags, metadados e Inteligência Artificial (IA).
- 16.8. A solução deve oferecer suporte ao provisionamento e à integração com software de terceiros por meio do processo de fluxos de trabalho.

17. Módulo de Governança de Acessos em Provedores de Infraestrutura de Nuvem (CEM).

17.1. A solução de CIEM deve ser compatível com a solução de IGA ofertada.

17.2. A solução deverá permitir a integração de provisionamento com os principais provedores de plataformas de nuvem, como AWS, Microsoft Azure e Google Cloud Platform.



17.3. A solução deve oferecer suporte nativo à integração com o AWS Identity Center.

17.4. A solução deverá possuir integração nativa a provedores de identidade de terceiros, como por exemplo Azure AD (Microsoft Entra) para fornecer informações e contexto sobre os acessos federados, provendo a visibilidade completa entre os acessos federados ao IDP com os recursos de infraestrutura das plataformas de nuvem.

17.5. A solução deve disponibilizar um histórico de acessos aos recursos da nuvem ao qual ela está conectada e gerenciando.

17.6. A solução deve prover um relatório nativo, que traga visibilidade sobre informações dos últimos 90 dias das ações, direitos e os serviços não utilizados dos seus ambientes de infraestrutura de nuvem, tais como AWS, Azure e GCP.

17.7. A solução deverá fornecer informações sobre o acesso efetivo que uma pessoa tem aos recursos de infraestrutura de nuvem (tais como recursos computacionais, de armazenamento, de rede etc.).

17.8. A solução deverá fornecer visibilidade detalhada de como um acesso ao recurso de nuvem está sendo concedido, fornecendo informações sobre os caminhos do acesso que uma identidade possui vinculada aos recursos de infraestrutura de nuvem, permitindo identificar se o acesso é concedido de forma direta, por meio de associação a grupos locais ou grupos federados etc.

17.9. A solução deve possuir um relatório contendo informações do acesso aos recursos do provedor nuvem, permitindo identificar qual o nível de privilégio utilizado (ex. Leitura, escrita, administração etc.)

17.10. A solução deve prover um relatório para visualizar os serviços (por ex.: AWS EC2) e recursos (por ex.: máquina virtual de nome "SRV123") que as identidades podem acessar nos provedores de infraestrutura de nuvem, abrangendo provedores, no mínimo, AWS, Azure e GCP.

17.11. A solução deve fornecer contexto adicional de acessos sobre o item de revisão de acesso (por ex.: uma Role da Azure) quando o item estiver vinculado à recursos de infraestrutura de provedores de nuvem (AWS, GCP e Azure). Este contexto adicional deve incluir no mínimo:

17.11.1. o nome e tipo do recurso;

17.11.2. o nível de direitos de acesso (ex: leitura, escrita, administração);

17.11.3. datas de último acesso ao provedor de nuvem e uso do permissionamento do acesso;



17.11.4. tipo de privilégio utilizado na última atividade (ex: leitura, escrita, administração);

17.11.5. além de elementos gráficos que permitam o decisor compreender os possíveis caminhos de obtenção de acesso aos recursos de infraestrutura de nuvem relacionados ao item sendo revisado.

ANEXO V

NÍVEIS MÍNIMOS DE SERVIÇOS

De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos serviços gerenciados de segurança, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela contratada na execução do contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. O Nível Mínimo de Serviços deve ser considerado e entendido pela CONTRATADA como um compromisso de qualidade que assumirá junto ao BASA.

1. Disponibilidade Mensal dos Serviços

- 1.1.** A solução deverá estar acessível 24 horas por dia, 7 dias na semana através da internet e, durante esse período, a solução deverá atender, dentro do mês, o mínimo de 99,9% de disponibilidade.
- 1.2.** O cálculo do Percentual de Disponibilidade Mensal (PDM) deve ser calculado com a seguinte fórmula:

$$[PDM] _ = ([TM - [TI] _])/TM * 100$$

PDM = Percentual de Disponibilidade Mensal;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI = Tempo total mensal de indisponibilidade, em minutos, no mês de faturamento.

- 1.3.** Devem ser incluídos como Tempo de Indisponibilidade (TI):
 - 1.3.1.** Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;
 - 1.3.2.** Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;
 - 1.3.3.** Tempo decorrente entre ocorrências sucessivas de indisponibilidade dentro de um intervalo inferior a 24 (vinte e quatro) horas do surgimento da primeira. Tais períodos devem ser considerados de recorrência desde a primeira ocorrência de indisponibilidade. Assim, nesse caso, o tempo da indisponibilidade deve ser contado a partir do surgimento da indisponibilidade inicial até a recuperação da última indisponibilidade no intervalo;
- 1.4.** Não devem ser incluídos como Tempo de Indisponibilidade (TI):
 - 1.4.1.** Indisponibilidade da rede lógica do BASA;
 - 1.4.2.** Indisponibilidade do ambiente virtualizado do BASA;
- 1.5.** O Tempo de Indisponibilidade será calculado com base no período total de impacto aos serviços, desde o início da falha até a completa resolução e restauração das operações normais. Para cada ocorrência, serão registrados e documentados os detalhes do evento, o tempo de início e término da indisponibilidade, e as ações tomadas para resolver a situação.


CONTRATO Nº 2025/154-01
2. EXECUÇÃO DO SERVIÇO DE SUPORTE E OPERAÇÃO

2.1. Na tabela abaixo são especificados os tempos máximos de resolução que devem ser seguidos, sob pena de multa, considerando a contagem de tempo em modo 10 x 5.

Referência	Métrica	Descrição	Definição	NMS - Valores referência
NMS-01	Esclarecimento de dúvidas	Suporte para dúvidas e questões relacionadas a solução ou serviços contratados	Tempo decorrido entre a abertura do chamado até a resposta da solicitação.	24 horas
NMS-02	Implantação e configuração de conectores	Solicitações de inclusão e configuração de conectores	Tempo decorrido entre a abertura do chamado até que a configuração seja finalizada.	7 dias
NMS-03	Criação e manutenção de regras	Solicitações de criação/edição/exclusão de regras gerais da solução, incluindo políticas de SoD previamente mapeadas.	Tempo decorrido entre a abertura do chamado até a operacionalização da regra.	24 horas
NMS-04	Criação e manutenção de políticas de SoD	Solicitações de criação/edição/exclusão de políticas de SoD previamente mapeadas.	Tempo decorrido entre a abertura do chamado até a operacionalização da regra.	24 horas
NMS-05	Parametrização da solução	Solicitações de parametrização, melhorias e sugestões de parametrização da solução baseada em boas práticas.	Tempo decorrido entre a abertura do chamado até a operacionalização da regra.	48 horas
NMS-06	Configuração de identidades	Solicitações de criação/edição/exclusão de identidades sem base autoritativa	Tempo decorrido entre a abertura do chamado até que a implementação da solicitação.	2 horas
NMS-07	Configuração de campanhas de revisão de acesso	Solicitações de criação, acompanhamento e apoio aos gestores nas campanhas de revisão de acesso.	Tempo decorrido entre a abertura do chamado até a resposta da solicitação.	24 horas
NMS-08	Elaboração de Relatório	Elaboração ou edição de relatório executivos, gerenciais e operacionais.	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao relatório.	2 dias
NMS-09	Realização de buscas	Realização de buscas conforme escopo definido pelo BASA	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao relatório.	1 hora



NMS-10	Análise de alertas	Análise de alertas gerados pela solução de IGA incluindo sugestões de correção	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao relatório.	2 hora
NMS-11	Suporte da solução	Instalação, configuração, reinstalação e desinstalação de qualquer componente da solução.	Tempo decorrido entre a abertura do chamado até a implementação da solicitação.	24 horas
NMS-12	Atendimento de solicitações	Atendimento das demais atividades da CONTRATADA não abrangidas nos NMS anteriores.	Tempo decorrido entre a abertura do chamado até a implementação da solicitação.	48 horas
NMS-13	Implantação do CIEM	Implantação do módulo de CIEM	Tempo decorrido entre a abertura do chamado até a implementação da solicitação.	15 dias

2.2. CHAMADOS EMERGENCIAIS

2.2.1. Em casos emergenciais, quando houver a paralisação nas atividades do negócio ou uma demanda de nível superior, o BASA poderá abrir chamados emergenciais, com o NMS diferenciado, conforme a tabela abaixo. O BASA designará 2 pessoas que poderão abrir chamados emergenciais.

2.2.2. Em caso de indisponibilidade da solução de IGA, os chamados abertos para a contratada deverão ter um grau de severidade a ser definido pelo BASA. Para isso, o BASA irá avaliar a urgência e a criticidade da demanda. Nesse sentido, os níveis mínimos de serviços deverão ser aferidos conforme a severidade de cada chamado.

2.2.3. Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Referência	Severidade	Descrição	Prazo máximo para primeira resposta de atendimento remoto	Prazo máximo da solução remota
NMS-12	Urgente / Crítica Severidade 1	A Solução está totalmente parada ou inoperante;	Até 1 (uma) hora após a abertura do chamado.	Até 6 (seis) horas após abertura do chamado.
NMS-13	Alta Severidade 2	A Solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;	Até 2 (duas) horas após a abertura do chamado.	Até 12 (doze) horas após abertura do chamado.

BANCO DA AMAZÔNIA
CONTRATO Nº 2025/154-01

NMS-14	Normal Severidade 3	A Solução está operativa, mas suas funcionalidades são executadas com restrições;	Até 8 (oito) horas após a abertura do chamado.	Até 2 (dois) dias após abertura chamado.
NMS-15	Baixa Severidade 4	A Solução está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação	Até 12 (doze) horas após a abertura do chamado.	Até 6 (seis) dias após a abertura do chamado.

- 2.3.** Os NMS poderão ser revisados 1 (um) ano após a assinatura do contrato, caso o BASA entenda que os tempos aqui especificados não estão atendendo as suas necessidades, sujeito à aceitação da CONTRATADA.

3. DESCONTOS PELO NÃO CUMPRIMENTO DOS NMS:

- 3.1.** Ao final do mês, será computado o percentual de atendimento ao NMS.
- 3.2.** Para os serviços de implantação da solução de IGA a apuração dos níveis de serviço será realizada após a emissão do TAD (Termo de Aceitação Definitivo). Assim, em caso de atraso na implantação por responsabilidade única e exclusiva da CONTRATADA, esta será descontada em 1% (um por cento) por dia ou fração de dia de atraso do valor total do serviço.
- 3.3.** A análise dos resultados das avaliações, pelo BASA, poderá resultar em advertências, penalizações e redução na fatura, caso a CONTRATADA não cumpra os compromissos acordados em contrato.
- 3.4.** Os descontos pelo não atendimento do NMS serão aplicados na nota fiscal/fatura dos serviços conforme tabela abaixo:

Nível de atendimento do NMS	Desconto aplicado na nota fiscal/fatura
95% <= NMS < 98%	5%
90% <= NMS < 95%	10%
85% <= NMS < 90%	15%
80% <= NMS < 85%	20%
NMS < 80%	30%

- 3.5.** Ultrapassado este limite, a CONTRATADA fica sujeita à aplicação das penalidades descritas no item 15 do Termo de Referência – Sanções Administrativas.
- 3.6.** Em caso extremo de descumprimento dos níveis de serviço acordados, o BASA pode vir a encerrar o Contrato de acordo com o previsto na Lei 13.303/93.
- 3.7.** Pelo fechamento não autorizado de chamados técnicos:
- 3.7.1.** Os chamados abertos somente poderão ser fechados após autorização de empregado designado pelo BASA. Caso haja fechamento de chamados, por parte da contratada, que não tenha sido previamente autorizado pelo BASA, será cobrada uma multa de 0,5% (zero vírgula cinco por cento) no valor mensal do serviço, por chamado fechado sem autorização, cumulativamente.

4. DISPOSIÇÕES GERAIS SOBRE OS NMS:



- 4.1.** O momento de início da medição do nível de serviço de cada atendimento/atividade solicitada à CONTRATADA será definido pela data e hora da abertura do chamado.
- 4.1.1.** No caso dos serviços agendados, os tempos serão contados a partir do início da data e hora agendada para o referido atendimento.
- 4.2.** A critério exclusivo do BASA, a contagem de tempo somente pode ser interrompida:
 - 4.2.1.** caso a CONTRATADA apresente, tempestivamente, razões que comprovem a ocorrência de fatos que fogem do seu controle, aceitas pelo BASA;
 - 4.2.2.** quando ações necessárias para a resolução de chamados tenham sido agendadas pela CONTRATADA em conjunto com o BASA; e
 - 4.2.3.** quando forem necessárias ações do BASA.
- 4.3.** Para quaisquer indicadores de nível de serviço influenciados negativamente por eventos comprovadamente causados pelo BASA não serão considerados os efeitos de tais eventos no cômputo do indicador de nível de serviço.
- 4.4.** Em qualquer mudança na situação de chamados, deve ser encaminhada uma notificação ao BASA, contendo as informações de registro do chamado, para endereço eletrônico de e-mail, inclusive quando houver mudança de status interrompendo a contagem de NMS.
- 4.5.** Em qualquer mudança na situação de chamados quando houver necessidade de agir por parte da CONTRATADA, a contagem de tempo para fins de NMS será iniciada automaticamente, mesmo que o chamado tenha sido negociado sem nível mínimo de serviço.
- 4.6.** O momento de fim da medição do nível de serviço de cada atendimento/atividade do Catálogo solicitada à CONTRATADA será definido pela data e hora da resposta da equipe da CONTRATADA pelo mesmo meio que foi registrado o atendimento.
- 4.7.** O BASA analisará a correteza da resolução do atendimento para então aprovar ou recusar o fechamento dele. Para efeitos de apuração do tempo gasto pela CONTRATADA para a apuração do NMS, serão desconsiderados os períodos em que o BASA estiver responsável por executar ações necessárias para a análise e atendimento da solicitação. Os chamados abertos somente podem ser concluídos e fechados após autorização do BASA.
- 4.8.** Para que um chamado seja considerado concluído, os serviços executados devem ser adequadamente documentados, evidenciados e arquivados no sistema de controle de chamados. A documentação entregue deve ser simplificada para esclarecer os procedimentos executados e permitir que servidores do BASA possam repetir as ações tomadas posteriormente.
- 4.9.** Caso seja necessária a elaboração de uma documentação detalhada dos procedimentos executados, incluindo justificativas técnicas, esclarecimentos e gráficos, o BASA pode solicitar sua elaboração por meio de registro de uma solicitação.
- 4.10.** Considerar-se-á como tempo de resolução, o período líquido compreendido entre o momento de início e a finalização do atendimento, descontado o tempo em que ele ficou pendente de execução por outras equipes do BASA.



- 4.11.** A frequência de aferição e avaliação dos serviços deve ser mensal, devendo a CONTRATADA elaborar Relatório de Serviços Prestados (RSP) até o 5º (quinto) dia útil do mês subsequente.
- 4.12.** O Relatório de Serviços Prestados (RSP) deve conter níveis de serviço acordados e alcançados, resultados obtidos e custos despendidos, estatísticas de disponibilidade de serviços e de desempenho de chamados, além de informações históricas sobre os dados coletados.
- 4.13.** O relatório deverá ser emitido em arquivo eletrônico em formato de planilha e enviada e/ou armazenada em condições a serem definidas pelo BASA.
- 4.14.** O Relatório de Serviços Prestados (RSP) deve conter, no mínimo:
- a.** Resumo Financeiro detalhado, contendo valores por serviço e por quantidades, contendo, no mínimo:
 - i. Valor mensal consolidado do serviço;
 - ii. Violações contratuais individualizadas.
 - iii. Descontos Pelo Não Cumprimento Dos NMS;
 - iv. Valor final faturado.
 - b.** Relatório Consolidado - Desempenho de Serviço (RDS), discriminado tipo de solicitação e de incidente, contendo, no mínimo:
 - i. Quantitativo de chamados abertos no período;
 - ii. Quantitativo de chamados que extrapolaram o tempo de conclusão de atendimento;
 - iii. Quantitativo de chamados que extrapolaram o tempo de registro de atendimento;
 - iv. Quantitativo de chamados que extrapolaram o tempo de início de atendimento;
 - v. Somatório de tempo de chamados que extrapolaram o tempo de conclusão de atendimento;
 - vi. Somatório de tempo de chamados que extrapolaram o tempo de registro de atendimento;
 - vii. Somatório de tempo de chamados que extrapolaram o tempo de início de atendimento;
 - c.** Relatório Analítico – Desempenho de Serviço (RDS), discriminado tipo de solicitação e de incidente, contendo, no mínimo:
 - i. Status do chamado;
 - ii. Tipo;
 - iii. Atividade;
 - iv. Solicitante;
 - v. Item de serviço;
 - vi. Número do ticket;
 - vii. Número do ticket associado ao sistema de chamados do BASA, se for o caso;
 - viii. Responsável pelo atendimento;
 - ix. Data-hora de ocorrência do evento, se aplicável (T0);
 - x. Data-hora de registro do chamado (T1);
 - xi. Data-hora de início do atendimento do chamado (T2);
 - xii. Data-hora de conclusão do atendimento do chamado (T3);



- xiii. Diferença de tempo entre o registro e a conclusão do atendimento do chamado, discriminando o tempo total de atendimento do chamado, tempo total de parada de contagem de NMS e o tempo extrapolado;
 - xiv. Breve descrição do ticket.
 - d. Backlog, contendo, no mínimo, as seguintes informações do corrente mês e respectiva série histórica anual:
 - i. Quantitativo de tickets em backlog;
 - ii. Quantitativo de tickets em backlog encerrados;
 - iii. Quantitativo de tickets em backlog cancelados;
 - iv. Descrição do ticket contendo, no mínimo: número do ticket, data de abertura, tipo (incidente ou solicitação), atividade e descrição sumária.
- 4.14.1.** A entrega do relatório é condição para o pagamento. Durante a vigência do contrato, o BASA pode solicitar reuniões avaliação dos níveis de serviço, ajustes na prestação do serviço e esclarecimentos julgados necessários.
- 4.15.** O Relatório de Serviços Prestados (RSP) deve ser avaliado e homologado pelo BASA até o 5º (quinto) dia útil subsequente à entrega pela CONTRATADA, subtraídos eventuais ajustes existentes.
- 4.16.** O relatório mensal de serviços poderá sofrer alterações no decorrer do contrato para melhor se adequar aos processos internos do BASA.
- 4.17.** Semestralmente a CONTRATADA deverá entregar e apresentar um Relatório Positivo destacando os aspectos de sucesso e melhorias implementadas, assim como recomendações para sustentar e potencializar o sucesso identificado. O objetivo é fornecer uma visão estratégica e otimista sobre o desempenho, enfatizando as conquistas e o valor agregado para a organização.

ANEXO VI

PROVA DE CONCEITO

1 DESCRIÇÃO

1.1 Visando aferir os requisitos funcionais e as condições de operação a licitante classificada em primeiro lugar deverá realizar Prova de Conceito (PoC) da solução de IGA ofertada.

1.2 A PoC representa a execução de um conjunto pré-definido de verificações sobre o software de IGA oferecido, com o objetivo de determinar se a solução está de acordo com a descrição do objeto deste Termo de Referência.

1.3 A PoC deverá ser realizada de forma remota, por meio de videoconferência a ser realizada na plataforma Microsoft Teams do Banco da Amazônia. A reunião será convocada pelo BASA e será gravada para compor o dossiê do processo.

1.4 A PoC deverá ser realizada em até 5 (cinco) dias úteis após a convocação e o término em até 2 (dois) dias úteis. Estes prazos devem ser contados a partir da solicitação formal pelo BASA.

1.5 Se os produtos apresentados não forem aprovados, a proposta da licitante será desclassificada e a autora da segunda melhor proposta classificada será submetida à PoC, e assim sucessivamente, até a apuração de uma proposta que atenda às especificações deste edital e seus anexos.

1.6 Poderão participar como observadores da Prova de Conceito, sem direito a manifestação durante a sua realização, 1 (um) representante de cada licitante interessada, sendo necessária a apresentação de procuração específica da licitante em nome do representante para a participação como observador na Prova de Conceito.

2 REQUISITOS E MÉTODOS DA POC

2.1 O software deverá ser executado em um ambiente da licitante. Para isso, durante a videoconferência, o representante da licitante deverá compartilhar a tela de sua estação de trabalho visando demonstrar o atendimento de cada uma das funcionalidades solicitadas no presente Anexo.

2.2 A Prova de Conceito da solução ofertada deverá ser realizada sem custo para o BASA.

2.3 O licitante que for reprovado na prova de conceito não terá direito a qualquer indenização.



2.4 A verificação de conformidade às características obrigatórias estabelecidas neste Termo de Referência será feita por meio dos seguintes testes:

2.4.1 Verificação se a solução é ofertada na modalidade SaaS baseada em microsserviços, garantindo escalabilidade e alta disponibilidade automatizados.

2.4.2 Verificação da capacidade da Inteligência Artificial Generativa para auxiliar na codificação de conectores e integrações, incluindo sugestões de melhor utilização das APIs da plataforma, sugestões de como criar um workflow de integração para melhor alinhar a necessidade de negócio com as capacidades da plataforma e sugestões de criação de conectores customizados para integração com sistemas legados.

2.4.3 Verificação da capacidade da solução de aplicar algoritmos de IA avançados (LLM) para gerar sugestões de descrições dos acessos do catálogo de direitos, abrangendo todos os direitos descobertos pela solução dos sistemas integrados.

2.4.4 Verificação da capacidade de fornecimento de recomendações baseadas em inteligência artificial sobre regras de correlação entre contas e identidades.

2.4.5 Verificação da capacidade de fluxo de autosserviço para que as pessoas chave (como por exemplo os responsáveis pelos direitos de acesso) possam revisar (acatar ou ajustar) as descrições geradas por IA melhorando a qualidade dos dados e enriquecendo os acessos do ambiente.

2.4.6 Verificação da capacidade de criação de perfis funcionais (mapeadas para um cargo/função ou estrutura organizacional) e perfis de acesso (pacotes ou conjuntos de direitos).

2.4.7 Verificação da capacidade de criação de perfis funcionais e perfil de acesso no modelo RBAC.

2.4.8 Verificação da capacidade de permitir que perfis de negócio possuam uma regra de associação automática, e que tais regras possam ser baseadas em atributos da identidade, atributos da conta ou ainda baseada em algum acesso específico da aplicação (por exemplo, um grupo LDAP).

2.4.9 Verificação da capacidade em permitir que novos acessos incluídos num perfil sejam provisionados automaticamente para as identidades que possuem o perfil previamente atribuído.

2.4.10 Verificação da capacidade de criação de novos atributos de uma identidade por meio de sua interface gráfica de administração.

2.4.11 Verificação da capacidade da solução de fornecer uma maneira configurável de identificar o conjunto de atributos que irão vincular automaticamente as contas dos sistemas conectados às identidades conhecidas pela plataforma.



2.4.12 Verificação da capacidade de utilizar informações de qualquer atributo da identidade para geração do identificador único.

2.4.13 Verificação da capacidade de efetuar a leitura de contas de usuários e permissões de acessos (direitos) dos aplicativos integrados e consolidar em um catálogo centralizado de governança.

2.4.14 Verificação da capacidade de solicitações de acessos a direitos individuais (grupos, telas, funcionalidades), conjuntos de direitos/grupos de direitos (perfis de acessos) e/ou perfis funcionais.

2.4.15 Verificação da capacidade de verificação das solicitações de papéis e acesso de forma self-service, integrada a um fluxo de trabalho de aprovação para gerenciamento e controle de concessões de acesso.

2.4.16 Verificação da capacidade de gerenciamento de senhas entre vários tipos de sistemas, como por exemplo Active Directory, incluindo a possibilidade de sincronizar a alteração destas senhas, conforme política configurada.

2.4.17 Verificação da capacidade de interceptação de senha para domínios Microsoft Active Directory visando o sincronismo da senha entre a solução e as demais aplicações integradas quando a senha é alterada diretamente no controlador de domínio ou através de Desktops.

2.4.18 Verificação da capacidade em permitir que usuários com perfis de helpdesk possam enviar um link de acesso para que usuários redefinam suas senhas.

2.4.19 Verificação da capacidade em gerenciar os acessos nos sistemas conectados, de acordo com informações organizacionais dos sistemas autoritativos, ou com base no estado do ciclo de vida de uma identidade, como por exemplo: ativo, licença, em férias, desligado etc.

2.4.20 Verificação da capacidade de acionar automaticamente fluxos de trabalho como Admissão, Transferência, Desligamento e Afastamento/Férias.

2.4.21 Verificação da capacidade de configuração de regras para o provisionamento com base no tipo de usuário (ex. Funcionário, terceiro, parceiro etc.).

2.4.22 Verificação da capacidade em oferecer suporte a desligamento de contas de forma unificada e imediata.

2.4.23 Verificação da capacidade em suportar processos flexíveis para cenários de desligamento com base nas aplicações, como por exemplo: desativar conta, excluir conta, mover conta de estrutura organizacional etc.



2.4.24 Verificação da capacidade de pesquisas complexas em toda a sua base de dados, incluindo mecanismo de pesquisa em linguagem natural para explorar os dados dentro do sistema.

2.4.25 Verificação da capacidade criação de revisão de acessos dos perfis, bem como campanhas de certificação sob demanda.

2.4.26 Verificação da capacidade de criação e aplicação de regras de segregação de funções entre diferentes tipos de aplicação.

2.4.27 Verificação da capacidade de criação de políticas para manter dos dados das identidades organizados.

2.4.28 Verificação da capacidade criação de gatilhos de eventos para fornecer atualizações sobre mudanças nas identidades.

2.4.29 Verificação da capacidade em efetuar reconciliações com os sistemas integrados e detectar de forma nativa quaisquer alterações a nível de contas gerenciadas, tais como mudanças de atributo, concessão ou remoção de acessos feitas fora da plataforma/processo de governança. Ao detectar tais alterações, a solução deve permitir ainda a configuração de fluxos de trabalho automatizados para análise e auto remediação do evento de mudança não autorizado.

2.4.30 Verificação da capacidade de identificação de contas órfãs (contas de sistemas que não possuem uma identidade relacionada) de forma automática e oferecer opções para lidar com essas contas, como por exemplo, revisar os seus acessos.

2.4.31 Verificação da capacidade em descobrir novas contas em sistemas gerenciados, que foram criadas fora da solução de governança.

2.4.32 Verificação da capacidade auxílio no processo de evolução de perfis, utilizando inteligência artificial, para sugerir automaticamente novas permissões (direitos) a serem adicionadas nos perfis existentes.

2.4.33 Verificação da capacidade exportação de relatório em formato CSV, XLSX e PDF.

2.5 A solução ofertada será rejeitada se não atender a qualquer dos requisitos listados no item 2.4 e seus subitens deste Anexo.

2.6 Após a realização da PoC, será emitido relatório resumido de análise, descrevendo as atividades realizadas e contendo a aprovação ou não da Proposta.



Ao BANCO DA AMAZÔNIA S.A.

Ref: Edital de Licitação n.90002/2025

Objeto: Solução de Governança e Administração de Identidade.

Prezados senhores,

A QOS TECNOLOGIA E SERVIÇOS LTDA, inscrita no CNPJ sob o n. 05.012.577/0001-37, sediada em Av. Rio Branco, nº 243, Sala 401, Edifício São Paulo, no bairro de Recife, Recife-PE com o telefone para contato n. (81) 3194.2000 e e-mail: comercial@qostecnologia.com.br, por intermédio do seu representante legal o Sr. Walter Fernandes Pinto Neto, CEO, portador da Carteira de Identidade n. 5.251.836 SSP/PE e do CPF n. 025.596.954-64, residente e domiciliado no Av. Rio Branco, nº 243, Sala 401, Edifício São Paulo, no bairro de Recife, Recife-PE, 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\$ 12.048.544,00 (doze milhões quarenta e oito mil quinhentos e quarenta e quatro reais), sendo somatória dos custos estimados para os 36 meses para a execução dos serviços objeto desta licitação.

GRUPO 1					
Item	Descrição	Unidade de medida	Quantidade	Preço Unitário (R\$)	Preço Total (R\$)
1	Serviço de subscrição anual da solução de IGA	Identidade	5000	1.698,90	8.494.500,00
2	Serviço de subscrição anual do módulo de CIEM	Identidade	200	1.041,40	208.280,00
3	Serviço de implantação da solução de IGA	-	1	1.201.118,00	1.201.118,00
4	Serviço de suporte e operação da solução	Mês	36	36.376,20	1.309.543,20
5	Serviço de capacitação na solução de IGA	Turma	1	30.002,80	30.002,80
6	Serviços técnicos especializados	UST	5000	161,02	805.100,00
VALOR GLOBAL: R\$12.048.544,00					

2. No valor total proposto estão englobados todos os custos e despesas previstos no Edital n. 90002/2025, 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.

QOS TECNOLOGIA E SERVIÇOS LTDA

CNPJ: 05.012.577/0001-37

Av. Rio Branco, 243 Edf. São Paulo - Sala 401 - Bairro do Recife - Recife/PE - CEP 50.030-310

Telefone: +55 81 3194.2000 - Fax 81 3194.2022

www.qostecnologia.com.br



3. Junta-se a planilha de composição de preços:

3.1. Juntamente com a Proposta de Preço, o licitante deverá encaminhar planilha de composição de custo e documentação técnica das soluções ofertadas, acrescida de Planilha de Atendimento aos Requisitos Técnicos indicando para cada item (exigência), o documento ou manual e o número da página, na documentação técnica fornecida, que permita a verificação das características técnicas obrigatórias, observado que o licitante deverá fornecer todas as informações que sejam solicitadas pela equipe do BANCO, visando completa validação de atendimento às características técnicas;

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

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

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

() Não é optante do Simples Nacional.

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

5. Essa proposta é válida por 60 (sessenta) dias, contados da data prevista para abertura dos envelopes.

6. Até que o contrato seja assinado, esta proposta constituirá um compromisso da QOS TECNOLOGIA E SERVIÇOS LTDA, observadas as condições do Edital. Caso esta proposta não venha a ser aceita para contratação, a BANCO DA AMAZÔNIA S.A. fica desobrigada de qualquer responsabilidade referente à presente proposta.

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

8. Não será admitido valor global do item superior ao estimado pelo Banco, pois caso algum dos itens estiver acima do valor orçado, o licitante será convocado a negociar, de maneira que a proposta para o item não ultrapasse o estimado.

9. 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: 001

AGÊNCIA: 7-8

CONTA CORRENTE: 48403-2

PRAÇA DE PAGAMENTO: Recife /PE

10. Por fim, declara conhecer e aceitar as condições constantes do Edital n. 90002/2025 e de seus Anexos.

QOS TECNOLOGIA E SERVIÇOS LTDA

CNPJ: 05.012.577/0001-37

Av. Rio Branco, 243 Edf. São Paulo - Sala 401 - Bairro do Recife - Recife/PE - CEP 50.030-310

Telefone: +55 81 3194.2000 - Fax 81 3194.2022

www.qostecnologia.com.br



Eng.º Walter Fernandes Pinto Neto
CEO

CPF n.º 025.596.954-64

R.G: 5.251.836 – SSP/PE

**WALTER
FERNANDES
PINTO
NETO:02559695464**

Assinado digitalmente por WALTER
FERNANDES PINTO NETO:02559695464
ND: C=BR, O=ICP-Brasil, OU=videoconferencia,
OU=33683111000107, OU=Secretaria da
Receita Federal do Brasil - RFB, OU=
ARSEP/PRO, OU=RFB e-CPF A3, CN=WALTER
FERNANDES PINTO NETO:02559695464
Razão: Eu estou aprovando este documento
Localização:
Data: 2025.05.07 12:08:20-03'00'
Foxit PDF Reader Versão: 2024.4.0



QOS TECNOLOGIA E SERVIÇOS LTDA
CNPJ: 05.012.577/0001-37

Av. Rio Branco, 243 Edf. São Paulo - Sala 401 - Bairro do Recife - Recife/PE - CEP 50.030-310

Telefone: +55 81 3194.2000 - Fax 81 3194.2022

www.qostecnologia.com.br

Certificado de Conclusão

Identificação de envelope: 911E2CCC-6ECB-423F-9B39-C4FD5D1CB702

Status: Concluído

Assunto: BASA-Docusign: Assinatura do Contrato 2025-154-01 - QOS TECNOLOGIA E SERVIÇOS LTDA.pdf

Envelope fonte:

Documentar páginas: 112

Assinaturas: 6

Remetente do envelope:

Certificar páginas: 5

Rubrica: 0

assinatura.contratos@basa.com.br

Assinatura guiada: Ativado

Rua Santo Antonio, N.17 - Sala F - Centro

Selo com Envelopeld (ID do envelope): Ativado

Eusebio, CE 61760000

Fuso horário: (UTC-03:00) Brasília

assinatura.contratos@basa.com.br

Endereço IP: 201.90.109.142

Rastreamento de registros

Status: Original

Portador: assinatura.contratos@basa.com.br

Local: DocuSign

22/07/2025 11:02:07

assinatura.contratos@basa.com.br

Eventos do signatário

Walter Fernandes Pinto Neto

walter@qostecnologia.com.br

Nível de segurança: E-mail, Autenticação da conta (Nenhuma)

Assinatura

DocuSigned by:

2B86AD1FAF4946E...

Adoção de assinatura: Imagem de assinatura carregada

Usando endereço IP:

2804:14d:72bc:81a9:f132:6d9a:391b:ea5a

Registro de hora e data

Enviado: 22/07/2025 11:26:51

Visualizado: 22/07/2025 15:27:00

Assinado: 23/07/2025 11:34:32

Termos de Assinatura e Registro Eletrônico:

Aceito: 22/07/2025 15:27:00

ID: 0b2747f8-b6a2-413b-8084-88eb28486aac

Diego Santos Lima

diego.lima@basa.com.br

Nível de segurança: E-mail, Autenticação da conta (Nenhuma)

DocuSigned by:

2E980EF2D4F4483...

Adoção de assinatura: Estilo pré-selecionado

Usando endereço IP: 201.90.109.142

Enviado: 23/07/2025 11:34:34

Reenviado: 28/07/2025 11:47:36

Visualizado: 28/07/2025 14:14:02

Assinado: 28/07/2025 14:14:19

Termos de Assinatura e Registro Eletrônico:

Aceito: 28/07/2025 14:14:02

ID: 0f5cedde-0052-49c7-8e54-3bfa754ebf5

Eventos do signatário presencial

Assinatura

Registro de hora e data

Eventos de entrega do editor

Status

Registro de hora e data

Evento de entrega do agente

Status

Registro de hora e data

Eventos de entrega intermediários

Status

Registro de hora e data

Eventos de entrega certificados

Status

Registro de hora e data

Eventos de cópia

Status

Registro de hora e data

Michelle Bastos Magalhães

michelle.bastos@basa.com.br

COORDENADORA

BANCO DA AMAZONIA

Nível de segurança: E-mail, Autenticação da conta (Nenhuma)

Copiado

Enviado: 28/07/2025 14:14:20

Eventos de cópia	Status	Registro de hora e data
Termos de Assinatura e Registro Eletrônico: Não oferecido através da DocuSign		
assinatura.contratos@basa.com.br assinatura.contratos@basa.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Copiado	Enviado: 28/07/2025 14:14:21 Reenviado: 28/07/2025 14:14:25
Termos de Assinatura e Registro Eletrônico: Não oferecido através da DocuSign		
Phelipe Erik Tozzi Silva phelipe.silva@basa.com.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Copiado	Enviado: 28/07/2025 14:14:22
Termos de Assinatura e Registro Eletrônico: Não oferecido através da DocuSign		
Eventos com testemunhas	Assinatura	Registro de hora e data
Eventos do tabelião	Assinatura	Registro de hora e data
Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	22/07/2025 11:26:51
Envelope atualizado	Segurança verificada	22/07/2025 11:41:13
Envelope atualizado	Segurança verificada	22/07/2025 11:41:13
Envelope atualizado	Segurança verificada	22/07/2025 11:41:13
Envelope atualizado	Segurança verificada	25/07/2025 15:32:43
Entrega certificada	Segurança verificada	28/07/2025 14:14:02
Assinatura concluída	Segurança verificada	28/07/2025 14:14:19
Concluído	Segurança verificada	28/07/2025 14:14:22
Eventos de pagamento	Status	Carimbo de data/hora
Termos de Assinatura e Registro Eletrônico		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, HCITIS ISV OBO BASA BANCO DA AMAZONIA (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact HCITIS ISV OBO BASA BANCO DA AMAZONIA:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: jonatas.nobre@basa.com.br

To advise HCITIS ISV OBO BASA BANCO DA AMAZONIA of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at jonatas.nobre@basa.com.br and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from HCITIS ISV OBO BASA BANCO DA AMAZONIA

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with HCITIS ISV OBO BASA BANCO DA AMAZONIA

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify HCITIS ISV OBO BASA BANCO DA AMAZONIA as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by HCITIS ISV OBO BASA BANCO DA AMAZONIA during the course of your relationship with HCITIS ISV OBO BASA BANCO DA AMAZONIA.