AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 028/2021

O **BANCO DO ESTADO DO PARÁ S.A.** torna público que realizará nos termos da Lei n. 13.303/2016 e de seu Regulamento de Licitações e Contratos[1], licitação na modalidade Pregão Eletrônico para **contratação de Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework,** conforme especificações e condições exigidas no edital e demais anexos.

A sessão pública ocorrerá na seguinte data, horário e local:

DATA: 01/09/2021

HORÁRIO: 10h (Horário de Brasília)

SISTEMA DE LICITAÇÕES: www.gov.br/compras

UASG: 925803

O edital da licitação estará disponível a partir de **11/08/2021**, podendo ser obtido: (i) Gratuitamente no site do BANPARÁ (www.banpara.b.br) e sites www.gov.br/compras e www.compraspara.pa.gov.br; ou, (ii) Na sede do BANPARÁ (Av. Presidente Vargas, n. 251, Ed. BANPARÁ – 1º andar, Comércio, Belém/PA) mediante depósito identificado do valor de R$ 0,25 (vinte centavos) por folha (Conta Corrente nº 800.002-6, Agência nº 0011 do BANPARÁ), não reembolsável, relativos aos custos de reprodução.

Belém - Pará, 11 de agosto de 2021.

Fernanda Raia

Pregoeira

[1]https://www.banpara.b.br/media/277333/regulamento_de_licita__es_e_contratos_-_21.12.20.pdf

PREGÃO ELETRÔNICO Nº 028/2021
EDITAL

O **BANCO DO ESTADO DO PARÁ S.A.**, por intermédio do(a) pregoeiro(a) designado(a) pela **Portaria nº 217/2019** leva ao conhecimento dos interessados que, na forma da Lei n. 13.303/2016, do Regulamento de Licitações e Contratos do BANPARÁ (adiante denominado "Regulamento"), da Lei n. 10.520/2002 alterada pelas disposições do Decreto n. 10.024/2019, da Lei Complementar n. 123/2006 e da Lei Estadual n. 8.417/2016, do Decreto Estadual n. 2.121/2018, Lei n. 12.846/2013, e Código Civil Brasileiro, fará realizar licitação na modalidade Pregão Eletrônico, pelo critério de menor preço, conforme condições estabelecidas neste edital e seus anexos.

1. SUMÁRIO DA LICITAÇÃO

1.1. OBJETO: Constitui objeto da presente licitação a **contratação de Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework,** conforme especificações, exigências e condições estabelecidas no Edital e seus Anexos.

1.1.1. MODALIDADE: Pregão Eletrônico.
1.1.2. MODO DE DISPUTA: Aberto/Fechado.
1.1.3. CRITÉRIO DE JULGAMENTO: Menor preço, na forma estabelecida pelo artigo 51 do Regulamento.
1.1.4. CRITÉRIO DE VALORES: Valor máximo aceitável.
1.1.5. SESSÃO PÚBLICA: Designada para o dia 01/09/2021, às 10h (horário de Brasília) no sistema de licitações www.gov.br/compras.

1.2. A adjudicação será **GLOBAL.**

1.3. Havendo discordância entre as especificações deste objeto descritas no COMPRASNET-CATMAT e as especificações constantes do **ANEXO I – Termo de Referência** e seus adendos, prevalecerão as últimas.

1.4. Havendo contradições entre o edital e seus anexos OU entre os anexos do edital deverão prevalecer as regras contidas no item 4 do art. 34 do Regulamento.

1.5. Todas as referências de tempo neste edital, no aviso e durante a sessão pública, observarão obrigatoriamente o horário de Brasília/DF, salvo quando o edital e/ou o(a) pregoeiro(a), na sessão, informar o contrário.

1.6. No campo "descrição detalhada do objeto ofertado" do sistema www.gov.br/compras, obrigatoriamente, o licitante deverá descrever a síntese do objeto ofertado, **não sendo aceitável como descrição apenas o uso da expressão "conforme o edital" ou similares.**

1.7. Fica **vedado ao licitante qualquer tipo de identificação** quando do registro de sua proposta de preços no sistema do www.gov.br/compras, **inclusive sendo vedado indicar marca e fabricante no campo "descrição detalhada do objeto ofertado"**, sob pena de desclassificação do certame. A marca e o fabricante devem ser indicados em campo próprio no sistema do www.gov.br/compras, quando for o caso.

2. CONDIÇÕES DE PARTICIPAÇÃO E CONTRATAÇÃO

2.1. Poderão participar da presente licitação qualquer pessoa jurídica legalmente estabelecida no País e que atenda às exigências deste edital e seus anexos.

2.2. Não será admitida a participação, nesta licitação, de pessoas naturais ou jurídicas que estejam cumprindo penalidade de:

- **a)** Suspensão temporária de participação em licitação e impedimento de contratar, prevista no inciso III do artigo 87 da Lei nº 8.666/1993, aplicada pelo BANPARÁ;
- **b)** Impedimento de licitar e contratar, prevista no artigo 7º da Lei nº 10.520/2002 ou no artigo 47 da Lei nº 12.462/2011, aplicada por qualquer órgão ou entidade integrante da Administração Pública do Estado do Pará;
- **c)** Declaração de inidoneidade, prevista no inciso IV do artigo 87 da Lei nº 8.666/1993, aplicada por órgão ou entidade integrante da Administração Pública nacional, ou, a prevista no artigo 46 da Lei nº 8.443/1992, aplicada pelo Tribunal de Contas da União;
- **d)** Proibição de contratar com o Poder Público aplicada com fundamento no artigo 12 da Lei nº 8.429/1992, ou, proibição de participar de licitações e de contratar prevista no § 3º do artigo 81 da Lei nº 9.504/1997;
- **e)** Qualquer outra sanção que as impeçam de participar de licitações e contratar com o BANPARÁ.

2.2.1. Para os fins desta licitação, os impedimentos referidos neste edital serão verificados perante o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP) e outros sistemas cadastrais pertinentes que sejam desenvolvidos e estejam à disposição para consulta, conforme o caso.

2.3. Não será admitida a participação:

a) Das pessoas naturais ou jurídicas referidas no artigo 38 da Lei nº 13.303/2016. Os licitantes deverão apresentar declaração de conformidade ao referido dispositivo, conforme **ADENDO XI do Termo de Referência – Anexo I deste Edital**.

b) De cooperativas.

c) De empresas reunidas em consórcio.

d) De empresas que estejam sob falência.

2.4. O licitante poderá participar desta licitação por intermédio de sua matriz ou filial, desde que cumpra as condições exigidas para habilitação e credenciamento, em relação ao estabelecimento com o qual pretenda participar do certame.

2.4.1. O CNPJ do estabelecimento que participar do certame, matriz ou filial, deverá ser o mesmo a constar no contrato com o BANPARÁ e nas Notas Fiscais/Faturas emitidas, quando do fornecimento ou execução dos serviços contratados. Dessa forma, não será admitida a emissão de Notas Fiscais/Faturas por CNPJ de estabelecimento diverso daquele participante da licitação.

2.5. Esta licitação é de âmbito nacional.

2.6. Como requisito para participação neste PREGÃO ELETRÔNICO, o licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta de preços está em conformidade com as exigências deste instrumento convocatório e seus anexos.

3. PROCEDIMENTO DA LICITAÇÃO

3.1. A presente licitação será conduzida pelo(a) pregoeiro(a), que pode ser auxiliada por agente ou equipe de apoio técnica, observando o seguinte procedimento:

a) Publicação do edital:

I. O prazo de publicação do edital não poderá ser inferior a **15 dias úteis** tendo em vista o art. 39 do Regulamento Interno de Licitações e Contratos do Banco do Estado do Pará S/A (RILC).

b) Credenciamento no sistema de licitações:

I. O credenciamento no sistema de licitações ocorrerá conforme o item 4 do presente edital.

c) Eventual pedido de esclarecimento ou impugnação:

I. Pedidos de esclarecimento e/ou impugnações serão dispostas conforme o item 5 do edital.

d) Resposta motivada sobre o eventual pedido de esclarecimento ou impugnação:

I. Respostas aos pedidos de esclarecimento e/ou impugnações serão dispostas conforme o item 5 do edital.

e) Cadastramento da proposta no sistema de licitações:

I. O cadastramento da proposta no sistema de licitações obedecerá ao disposto no Decreto federal nº 10.024/2019, conforme abaixo:

i. O cadastramento da proposta no sistema de licitações deverá obedecer o tempo estipulado pelo prazo de publicação do edital tendo por data e horário limite o momento imediatamente anterior a abertura da licitação.

ii. Após a divulgação do edital no sítio eletrônico, todos licitantes terão a **obrigatoriedade** de encaminhar, **concomitantemente com a proposta de preço**, os **documentos de habilitação** exigidos no edital, **exclusivamente por meio do sistema.**

iii. Ficam dispensados de apresentar os documentos de habilitação que constem do SICAF.

Os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema, **até a abertura da sessão pública.** Durante a sessão pública e demais atos subsequentes que sejam necessários à comprovação da habilitação, o (a) pregoeiro (a) poderá solicitar aos licitantes inserção de documentos ainda não apresentados desde que os mesmos se refiram a circunstâncias anteriores à data da abertura da sessão para que se considere tempestiva a habilitação. O (a) pregoeiro (a) também poderá solicitar aos licitantes ajustes nos documentos já anexados, se necessário, conforme exemplificado no item i, VIII.

iv. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do(a) pregoeiro(a) e para acesso público após o encerramento do envio de lances.

f) Avaliação das condições de participação:

I. Após o início da sessão e antes da abertura dos itens para a fase de lances, serão verificadas, previamente:

i. As condições de participação da licitação previstas no item 2 do presente edital.

ii. O preenchimento da proposta preliminar com vedação de identificação do licitante e descrição correta do objeto nos termos do item 6 do edital.

g) Apresentação de lances:

I. A apresentação de lances no sistema de licitações obedecerá ao disposto no Decreto federal nº 10.024/2019, conforme abaixo:

i. A etapa de envio de lances na sessão pública durará **15** (**quinze) minutos** e, após isso, o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até dez minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada.

ii. Encerrado o prazo de dez minutos, aleatoriamente determinado, o sistema abrirá a oportunidade para que o autor da oferta de valor mais baixo e os autores das ofertas com valores até **dez por cento** superiores àquela possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento deste prazo.

iii. Na ausência de, no mínimo, três ofertas nas condições de que trata o item acima, os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, poderão oferecer um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento do prazo.

iv. Encerrados os prazos acima, o sistema ordenará os lances em ordem crescente de vantajosidade.

v. Na ausência de lance final e fechado classificado nos termos acima, haverá o reinício da etapa fechada para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento deste prazo, observado, após esta etapa, que o sistema ordenará os lances em ordem crescente de vantajosidade.

vi. Na hipótese de não haver licitante classificado na etapa de lance fechado que atenda às exigências para habilitação, o(a) pregoeiro(a) poderá, auxiliado pela equipe de apoio, mediante justificativa, admitir o reinício da etapa fechada.

h) Negociação:

I. Após a fase de lances, o licitante melhor colocado será chamado pelo(a) pregoeiro(a) a negociar.

i) Verificação de efetividade dos lances ou propostas:

I. A verificação dos lances ou propostas tem por objetivo impedir a contratação de bens e serviços com sobrepreço ou valores inexequíveis.

II. Nesse momento, o(a) pregoeiro(a) verificará a proposta ou lance final do licitante melhor colocado quanto à conformidade quanto ao critério de valores adotado para a licitação.

III. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

IV. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 2° do artigo 56 da Lei n° 13.303, de 2016 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

V. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

VI. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

VII. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata

VIII. O(a) Pregoeiro(a) poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de mínimo de 120 (cento e vinte) minutos, sob pena de não aceitação da proposta.

IX. O prazo poderá ser prorrogado pelo(a) Pregoeiro(a) por solicitação escrita e justificada do licitante e formalmente aceita pelo(a) Pregoeiro(a), formulada antes de findo o prazo.

X. Dentre os documentos passíveis de solicitação pelo(a) Pregoeiro(a), destacam-se as planilhas de custo, readequadas com o valor final ofertado.

XI. Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

XII. O(a) Pregoeiro(a) analisará a compatibilidade dos preços unitários apresentados na Planilha de Custos e Formação de Preços com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

XIII. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo(a) Pregoeiro(a), desde que não haja majoração do preço proposto.

j) Julgamento:

a) O critério de julgamento da presente licitação será o de **menor preço**.

k) Habilitação:

a) A habilitação, enviada previamente pelo licitante, será verificada após o julgamento da proposta vencedora da fase de lances e negociação com a finalidade de se obter o menor preço aceitável pelo Banco e será verificada sua conformidade com as instruções contidas no item 10 do edital.

l) Declaração de vencedor:

a) Ao licitante que após as análises se classificar melhor colocado e tiver seus documentos aprovados será declarado vencedor na ausência de intenção de recurso ou após resultado final de recurso.

m) Interposição de recurso:

a) Os procedimentos de interposição de recurso e julgamento serão definidos no item 11 do edital.

n) Adjudicação e homologação;

a) A adjudicação e homologação seguirão o rito definido pelo item 12 deste edital.

4. CREDENCIAMENTO E ACESSO AO SISTEMA DE LICITAÇÕES

4.1. Os interessados em participar deverão dispor de acesso no sistema de licitações www.gov.br/compras, no qual deverão realizar seu credenciamento e de representante capacitado e habilitado a praticar os atos e transações inerentes à licitação.

4.2. As empresas deverão ser registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do item 1 A do art. 42 do Regulamento. As que ainda não estejam cadastradas e tiverem interesse em participar do presente Pregão, deverão providenciar o seu cadastramento e sua habilitação através do endereço eletrônico do sistema de processamento eletrônico das informações cadastrais, ou seja, o site do SICAF referente ao SIASG/COMPRASNET, até o momento anterior à abertura da sessão.

4.3. O cadastro se dará após o acesso ao site: https://portal.brasilcidadao.gov.br/servicos-cidadao/acesso/#/primeiro-acesso e seguidas as devidas orientações de cadastro de fornecedores, os quais, deverão possuir, para operação do sistema SICAF digital o seu certificado digital no padrão ICP-Brasil conforme as exigências do sistema.

4.4. O credenciamento junto ao provedor do sistema implica na responsabilidade legal única e exclusiva do licitante ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes à licitação.

4.5. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao BANPARÁ responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

4.6. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, declarando e assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao BANPARÁ responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.7. O acesso ao sistema se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecido.

4.8. Caberá ao licitante acompanhar as operações no sistema, antes, durante e após a sessão pública de lances, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

4.9. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao Sistema Eletrônico, no site www.gov.br/compras. O credenciamento junto ao provedor do Sistema implica na responsabilidade legal, única e exclusiva do licitante, ou de seu representante legal, bem como na presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico e respectiva assunção das obrigações decorrentes da adjudicação e contratação.

4.10. A perda da senha ou a detecção de indícios que sugiram a quebra de sigilo devem ser imediatamente comunicadas ao provedor do sistema, com vistas à adoção das medidas cabíveis e imediato bloqueio de acesso.

5. CONSULTAS, ADITAMENTOS E IMPUGNAÇÕES

5.1. Qualquer cidadão ou agente econômico poderá pedir esclarecimentos e impugnar o edital, em requerimento escrito que deve ser apresentado, exclusivamente por meio eletrônico (internet), enviando para o e-mail cpl-1@banparanet.com.br.

5.1.1. Os pedidos de esclarecimentos e impugnações devem ser apresentados até às 16 horas (horário local) do **5º (quinto) dia útil** antes da data fixada para a ocorrência do certame, ou seja, até o dia **25/08/2021.**

5.1.2. Não serão conhecidos os requerimentos apresentados intempestivamente e/ou subscritos por pessoa não habilitada legalmente ou não identificada no processo para responder pela impugnante.

5.1.3. Ao receber os requerimentos, o(a) pregoeiro(a) deverá remetê-los, imediatamente, à área técnica competente, para que ofereça resposta motivada.

5.1.4. Os pedidos de esclarecimento deverão ser respondidos antes da sessão de abertura da licitação e os pedidos de impugnação, motivadamente, em até 03 dias úteis antes da abertura da sessão.

5.1.5. A decisão de eventual adiamento da abertura da licitação e a remarcação de sua abertura é de competência do(a) pregoeiro(a) e será publicada no sítio eletrônico do BANPARÁ e no site www.gov.br/compras, assim como, todos os avisos, pedidos de esclarecimentos, impugnações e suas respectivas respostas.

5.2. Somente terão validade os comunicados veiculados por intermédio do(a) pregoeiro(a) e disponibilizados na forma deste item.

5.3. O licitante, através de consulta permanente, deverá manter-se atualizado quanto a quaisquer alterações e esclarecimentos sobre o edital, não cabendo ao BANPARÁ a responsabilidade por desconhecimento de tais informações, em face de inobservância do licitante quanto ao procedimento apontado neste subitem.

5.4. Aplica-se, no que couber, quanto aos pedidos de esclarecimento e impugnação, o disposto no art. 40 do Regulamento.

6. APRESENTAÇÃO DA PROPOSTA NO SISTEMA DE LICITAÇÕES

6.1. O licitante deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

6.2. No ato de envio de sua proposta, o licitante deverá manifestar, em campo próprio do sistema de licitações, que:

6.2.1 Cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório.

6.2.2 Inexiste fato superveniente impeditivo para sua habilitação, ciente da obrigatoriedade de declarar ocorrências posteriores;

6.2.3 Não emprega menores em condições vedadas pela legislação trabalhista, nem possui empregados executando trabalhos degradantes ou forçados;

6.2.4 Sua proposta foi elaborada de forma independente:

i. As microempresas e empresas de pequeno porte (ME/EPP) deverão, por ocasião do envio da proposta, declarar em campo próprio do sistema, sob as penas da lei, que atendem os requisitos do art. 3º da Lei Complementar nº 123/2006, estando aptas a usufruir do tratamento favorecido.

ii. A falta da declaração a que se refere este item indicará que a microempresa ou empresa de pequeno porte (ME/EPP) optou por não utilizar os benefícios previstos na Lei Complementar nº 123/2006.

6.3. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta referente aos impedimentos e sobre a condição de microempresa e empresa de pequeno porte (ME/EPP) sujeitará a proponente às sanções previstas neste edital.

6.4. O licitante deverá encaminhar sua proposta preenchendo os campos específicos no sistema de licitações, observadas as seguintes condições:

6.4.1 O preenchimento da proposta, bem como a inclusão de seus anexos, no sistema de licitações é de exclusiva responsabilidade do licitante, não cabendo ao BANPARÁ qualquer responsabilidade.

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

6.6 No sistema, **deverá ser cotado preço global**, contendo no máximo 02 (duas) casas decimais, sem arredondamentos. No preço cotado, deverão incluir todos os tributos, seguros, taxas e demais encargos que incidam ou venham a incidir sobre o contrato e sua execução, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho e outros.

6.7 O licitante microempresa ou empresa de pequeno porte (ME/EPP) optante do Simples Nacional deve indicar a alíquota de imposto incidente com base no faturamento acumulado dos últimos 12 (doze) meses anteriores.

6.8 Quando o objeto licitado estiver enquadrado em algumas das vedações previstas no art. 17 da Lei Complementar nº 123/2016, os licitantes microempresas ou empresas de

pequeno porte (ME/EPP) que forem optantes do Simples Nacional deverão formular suas propostas desconsiderando os benefícios tributários do regime a quem fazem jus.

6.9 O prazo de validade das propostas será de 120 (cento e vinte) dias, contados da data da sua apresentação, podendo vir a ser prorrogado mediante solicitação do BANPARÁ e aceitação do licitante.

6.9.1 O(a) pregoeiro(a) verificará as propostas de preços enviadas, antes da abertura da fase de lances, desclassificando, motivadamente, aquelas que, de pronto, não atenderem às exigências do presente edital e seus anexos, sejam omissas em relação às informações exigidas, apresentem irregularidades insanáveis ou defeitos capazes de dificultar o julgamento, ou, ainda, que não observem o disposto nos itens 1.6 e 1.7 deste edital.

6.9.2 A apresentação da proposta implicará a plena aceitação, por parte do licitante, das condições estabelecidas.

6.9.3 O BANPARÁ não aceitará qualquer cobrança posterior de quaisquer encargos financeiros adicionais, salvo se criados após a data de abertura desta licitação, desde que observem os requisitos e critérios relativos aos procedimentos de reequilíbrio econômico-financeiro da contratação, conforme definido neste edital, seus anexos e no Regulamento do BANPARÁ.

6.10 No momento da inserção da proposta deverão ser inseridos em anexo os documentos de habilitação previstos no item 10 e seus subitens do Termo de Referência – Anexo I deste Edital e item 10 deste Edital.

7 JULGAMENTO

7.1 A presente licitação será julgada pelo critério do **menor preço** e, nos termos do item 3 do art. 104 do Regulamento, seguirá as regras de apresentação de propostas e lances estabelecidos pelo sistema eletrônico utilizado, no caso, www.gov.br/compras. No horário designado, o(a) pregoeiro(a) fará realizar a sessão pública.

i. Se por algum motivo a sessão pública não puder ser realizada na data e horário previstos, os licitantes deverão ficar atentos à nova data e horário que serão disponibilizados no sistema eletrônico em que se realizará a sessão pública e no sítio eletrônico do BANPARÁ.

ii. No caso de desconexão do(a) pregoeiro(a), no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.
iii. Quando a desconexão do(a) pregoeiro(a) persistir por tempo superior a 10 (dez) minutos, a sessão da licitação eletrônica será suspensa e reiniciada somente após comunicação aos licitantes.

7.2 Os licitantes que atenderem as condições deste edital poderão apresentar lances, exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro do valor.

7.3 Os lances serão registrados no sistema, de forma sucessiva, em valores distintos e decrescentes.

7.4 O licitante somente poderá oferecer lances inferiores ao último por ele ofertado e registrado no sistema.

i. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes.
ii. Será permitida a apresentação de lances intermediários pelos licitantes, assim considerados os lances iguais ou superiores ao menor já ofertado, mas inferiores ao último lance dado pelo próprio licitante.
iii. Não serão aceitos lances iguais, prevalecendo aquele que for recebido e registrado primeiro.
iv. Durante a fase de lances, o(a) pregoeiro(a) poderá excluir, justificadamente, lance cujo valor for considerado inexequível.
v. Não será admitida a desistência do lance efetivado, sujeitando-se o licitante desistente às penalidades previstas neste edital e na legislação vigente.

7.5 Para efeito de ordenação das propostas de preços, a desistência em apresentar lance implicará exclusão do licitante da etapa de lances e na manutenção do último preço por ele apresentado.

8 DIREITO DE PREFERÊNCIA PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE (ME/EPP)

8.1 Encerrada a etapa de lances, o(a) pregoeiro(a) deverá verificar se ocorre o empate ficto em favor de microempresa ou empresa de pequeno porte (ME/EPP), assegurando, se for o caso, o direito de preferência, observando-se o seguinte:

i. O empate ficto ocorrerá quando as ofertas apresentadas pelas microempresas e empresas de pequeno porte (ME/EPP) sejam iguais ou até 5% (cinco por cento) superiores ao menor preço, quando este for de licitante que não se enquadre na condição de microempresa ou empresa de pequeno porte (ME/EPP);

ii. Ocorrendo o empate, a microempresa ou a empresa de pequeno porte melhor (ME/EPP) classificada, convocada pelo(a) pregoeiro(a), poderá, no prazo máximo de 5 (cinco) minutos, apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que deve ser adjudicado o objeto em seu favor;

iii. Se a microempresa ou empresa de pequeno porte (ME/EPP) melhor classificada não exercer o direito de preferência, deverão ser convocadas as remanescentes que porventura se enquadrem na situação de empate, na ordem classificatória, para o exercício do mesmo direito; e

iv. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte (ME/EPP) que se encontrem em situação de empate, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta. Não se aplica tal sorteio quando por sua natureza, o procedimento não admitir o empate real, como acontece na fase de lances do pregão, em que os lances equivalentes não são considerados iguais, sendo classificados conforme a ordem de apresentação pelos licitantes, conforme disposto art.8º §5º da Lei Estadual n. 8.417/2016.

8.2 Caso a microempresa ou empresa de pequeno porte (ME/EPP), classificada pelo exercício do direito de preferência, venha a ser desclassificada ou inabilitada por vícios em sua proposta ou documentação, o(a) pregoeiro(a) convocará, dentre as remanescentes que porventura se enquadrem na hipótese de empate ficto e respeitada a ordem classificatória, a próxima microempresa ou empresa de pequeno porte (ME/EPP) para o exercício do mesmo direito de preferência.

8.3 O procedimento previsto no subitem acima será adotado, sucessivamente, até a apuração de uma proposta que atenda ao edital ou até que não haja microempresa ou empresa de pequeno porte que se enquadre na hipótese de empate ficto.

8.4 Na hipótese da não-contratação nos termos previstos do item 8.2, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame, desde que atendas as exigências de efetividade e de habilitação.

9 VERIFICAÇÃO DA EFETIVIDADE DOS LANCES E PROPOSTAS

9.1 Encerrada a etapa de lances e após a verificação de possíveis preferências e empates, o(a) pregoeiro(a) examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.

9.1.1 Para o exame preliminar, o(a) pregoeiro(a) poderá exigir o imediato detalhamento da proposta. Quando exigido, a proponente deverá encaminhar, por meio do sistema eletrônico em que se realiza a licitação, www.gov.br/compras no prazo estipulado pelo(a) pregoeiro(a).

9.1.2 O(a) pregoeiro(a) irá conceder **prazo mínimo de 120 (cento e vinte) minutos** para que a empresa primeira colocada ajuste a Proposta de Preço com o último lance ofertado, caso a empresa oferte lances. A proposta ajustada deverá ser inserida no sistema Comprasnet.

9.1.3 A proposta inicial, assim como a proposta final, se for o caso, com o valor equalizado ao seu último lance ofertado, decomposta em planilha de preços, observado o modelo do **ADENDO II do Termo de Referência – Anexo I deste Edital**, deve constar conforme o caso:

i. Indicação dos quantitativos e dos custos unitários;
ii. Caso o licitante seja microempresa ou empresa de pequeno porte (ME/EPP) optante do Simples Nacional, deverá indicar a alíquota de imposto incidente com base no faturamento acumulado dos últimos 12 (doze) meses anteriores.
iii. Observar as exigências do Termo de Referência, ANEXO I deste edital.

9.2. O(a) pregoeiro(a) deverá avaliar se a proposta do licitante melhor classificado atende às especificações técnicas, demais documentos e formalidades exigidas no edital, podendo ser subsidiado pela área técnica no que se referir ao atendimento das questões técnicas relacionadas ao objeto da licitação ou de documentos com informações de ordem técnica que podem impactar a sua execução.

9.3. O(a) pregoeiro(a) deverá desclassificar as propostas que apresentem preços manifestamente inexequíveis, assim considerados aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida.

9.4. A inexequibilidade dos valores referentes a itens isolados da planilha de custos, desde que não contrariem instrumentos legais, não caracterizarão motivo suficiente para a desclassificação da proposta.

9.5. A análise de exequibilidade da proposta não deverá considerar materiais e instalações a serem fornecidos pelo licitante em relação aos quais ele renuncie à parcela ou à totalidade da remuneração, desde que a renúncia esteja expressa na proposta.

9.6. O(a) pregoeiro(a) poderá realizar diligências para aferir a exequibilidade ou qualquer outro aspecto da proposta.

9.6.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, o(a) pregoeiro(a) poderá exigir do licitante, sob pena de desclassificação, documentos que contenham as características dos bens ofertados (tais como marca, modelo, tipo, fabricante e procedência) e outras informações pertinentes (tais como catálogos, folhetos ou propostas de terceiros), que sejam capazes de demonstrar a exequibilidade da sua proposta.

9.6.2. Qualquer licitante poderá requerer motivadamente que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

9.7. O(a) pregoeiro(a) poderá negociar com o licitante autor da melhor proposta condições mais vantajosas, que poderão abranger os diversos aspectos da proposta, desde preço, prazos de pagamento e de entrega, sem que lhe caiba, a pretexto da negociação, relativizar ou atenuar as exigências e condições estabelecidas no edital e nos seus documentos anexos.

9.8. O(a) pregoeiro(a) poderá, de acordo com sua análise de conveniência e oportunidade, divulgar o orçamento do BANPARÁ para efeito de negociação.

9.9. O valor global da proposta, bem como os seus preços unitários, após a negociação, não poderão superar o orçamento estimado pelo BANPARÁ, sob pena de desclassificação do licitante.

9.10. O(a) pregoeiro(a) deverá desclassificar, em decisão motivada, apenas as propostas que contenham vícios insanáveis, observando-se o seguinte:

a) São vícios sanáveis, entre outros, os defeitos materiais atinentes à descrição do objeto da proposta e suas especificações técnicas, incluindo aspectos relacionados à execução do objeto, às formalidades, aos requisitos de representação, às planilhas de composição de preços, e, de modo geral, aos documentos de conteúdo declaratório sobre situações pré-existentes, desde que não alterem a substância da proposta;

b) O(a) pregoeiro(a) não deverá permitir o saneamento de defeitos em propostas apresentadas com má-fé ou intenção desonesta, como aqueles contaminados por falsidade material ou intelectual ou que tentem induzir o(a) pregoeiro(a) a erro;

c) O(a) pregoeiro(a) deverá conceder prazo adequado, recomendando-se 2 (dois) dias úteis, prorrogáveis por igual período, para que o licitante corrija os defeitos de sua proposta;

d) O(a) pregoeiro(a) deverá indicar expressamente quais aspectos da proposta ou documentos apresentados junto à proposta devem ser corrigidos;

e) A correção dos defeitos sanáveis não poderá importar alteração do valor final da proposta, exceto para oferecer preço mais vantajoso para o BANPARÁ;

f) Se a proposta não for corrigida de modo adequado, o(a) pregoeiro(a) poderá conceder novo prazo para novas correções.

9.11. Sendo aceitável a proposta, o(a) pregoeiro(a) deverá analisar a documentação de habilitação do licitante que a tiver formulado, para verificação de suas condições habilitatórias.

10 HABILITAÇÃO

10.1 O licitante autor da melhor proposta deve apresentar os documentos de habilitação exigidos neste item em formato digital por meio eletrônico, exclusivamente no sistema **www.gov.br/compras** no momento de inserção da proposta de participação do presente pregão eletrônico.

10.1.1 Os documentos de habilitação, bem como a proposta inicial de participação poderão ser inseridos, substituídos ou retirados do sistema até o momento imediatamente anterior da abertura da sessão.

10.2. O licitante deverá apresentar os seguintes documentos de **HABILITAÇÃO JURÍDICA**, que deverão estar acompanhados de todas as suas alterações ou da

respectiva consolidação, quando for o caso, e deles deverá constar, **entre os objetivos sociais**, **a execução de atividades da mesma natureza do objeto desta licitação**:

a) Inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, no caso de empresário individual;

b) Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documentos comprobatórios da eleição/nomeação de seus administradores, em se tratando de Sociedades Empresárias ou Empresa Individual de Responsabilidade Limitada (EIRELI);

c) Decreto de autorização, devidamente arquivado, quando se tratar de empresa ou sociedade estrangeira em funcionamento no País, com procurador residente domiciliado no País, conforme Parágrafo Único do artigo 16 do Decreto n. 3.555/2000, e ato de registro ou autorização para funcionamento, expedido pelo órgão competente, quando a atividade assim o exigir;

d) Inscrição do ato constitutivo em cartório de Registro Civil de Pessoas Jurídicas do local de sua sede, no caso de sociedades simples, acompanhada de prova da indicação de seus administradores.

10.3. QUALIFICAÇÃO TÉCNICA: o licitante deverá apresentar documentos de qualificação técnica conforme exigência dos **itens 10.1 e seus subitens** do Termo de Referência, **ANEXO I** deste edital.

10.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA: O licitante deverá apresentar os documentos relativos à capacidade econômico-financeira exigidos no **item 11 e seus subitens** e seus subitens do Termo de Referência, **ANEXO I** deste Edital.

10.5 REGULARIDADE FISCAL: O licitante deverá apresentar os seguintes documentos relativos à regularidade fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de regularidade com as fazendas públicas: **FEDERAL** (inclusive dívida ativa), **ESTADUAL** (se a sede da empresa for no Estado do Pará, a regularidade será comprovada por meio de duas certidões: tributária e não tributária) e **MUNICIPAL** (se a sede da empresa for no município de Belém, a regularidade será comprovada por meio de uma única certidão, em conformidade com o disposto na Instrução Normativa nº 06/2009 – GABS/SEFIN).

b.1) No que se refere à certidão de regularidade fiscal emitida pela **fazenda pública municipal ou estadual**, quando for o caso, que, por ocasião da

conferência da autenticidade online, ainda que dentro do prazo de validade, encontrar-se na situação "cassada", **o licitante poderá regularizá-la até o prazo final de análise dos documentos de habilitação.**

c) Prova de regularidade com o Instituto Nacional do Seguro Social – INSS;

d) Prova de regularidade com o Fundo de Garantia por Tempo de Serviço – FGTS;

e) Certidão Negativa de Débitos Trabalhistas – CNDT.

10.6 Microempresas e empresas de pequeno porte (ME/EPP) deverão atender a todas as exigências de habilitação previstas neste edital.

10.6.1. As microempresas e empresas de pequeno porte (ME/EPP) deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade **fiscal** e **trabalhista,** mesmo que esta apresente alguma restrição;

10.6.2. Havendo alguma restrição na comprovação da **regularidade fiscal ou trabalhista**, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, que é o momento imediatamente posterior à fase de habilitação, prorrogáveis por igual período pelo BANPARÁ, mediante requerimento do licitante, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa;

10.6.3. A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste edital, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

10.7 O licitante registrado no Sistema de Cadastramento Unificado de Fornecedores (SICAF), com cadastro vigente na data de vencimento da licitação, poderá apresentar o Certificado de Registro Cadastral em substituição às informações nele atestadas e que estejam dentro do prazo de validade.

10.7.1 Quando os documentos necessários à habilitação estiverem desatualizados no Sistema SICAF ou quando não estiverem nele contemplados, deverão ser anexados no sistema Comprasnet junto com a documentação, conforme **item 10.1** acima.

10.8 Se o licitante desatender às exigências habilitatórias, o(a) pregoeiro(a) examinará a proposta e documentação do licitante subsequente, e assim, sucessivamente, até a

apuração de documentação que atenda os termos do edital, cujo licitante será declarado vencedor.

10.9 O licitante será considerado habilitado se apresentar a documentação em conformidade com as exigências acima. Constatado o atendimento das exigências fixadas no edital, o licitante será declarado vencedor.

10.10 O(a) pregoeiro(a) somente deverá inabilitar o licitante autor da melhor proposta em razão de defeitos em seus documentos de habilitação que sejam insanáveis, aplicando-se os mesmos procedimentos e critérios prescritos neste edital para o saneamento de propostas, observando-se o seguinte:

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

b) O(a) pregoeiro(a) poderá realizar diligência para esclarecer o teor ou sanar defeitos constatados nos documentos de habilitação;

c) O(a) pregoeiro(a), se for o caso de diligência, deverá conceder prazo de 2 (dois) dias úteis, prorrogável por igual período, para que o licitante corrija os defeitos constatados nos seus documentos de habilitação, apresentando, se for o caso, nova documentação;

d) O(a) pregoeiro(a), se for o caso de diligência, deverá indicar expressamente quais documentos devem ser reapresentados ou quais informações devem ser corrigidas;

e) Se os defeitos não forem corrigidos de modo adequado, o(a) pregoeiro(a) poderá conceder novo prazo para novas correções.

10.11 Se todos os licitantes forem desclassificados ou inabilitados, dada a constatação de defeitos insanáveis em todas as propostas apresentadas, o(a) pregoeiro(a) deverá declarar a licitação fracassada.

10.12 O licitante que for declarado vencedor da presente licitação, não havendo interposição de recursos ou após decididos estes, **deverá enviar via física da proposta final, da documentação e das declarações para o BANPARÁ,** sito à Av. Presidente Vargas, nº 251 – Ed. BANPARÁ, 1º andar, Comércio, Belém/PA, CEP 66.010.000, no prazo máximo de 02 (dois) dias úteis.

10.12.1 O prazo estabelecido no subitem acima poderá ser prorrogado por decisão fundamentada do(a) pregoeiro(a), após análise de justificativa apresentada pelo licitante.

10.13 É de responsabilidade do licitante confirmar junto ao BANPARÁ o recebimento da proposta final e dos documentos de habilitação.

10.14 Todos os documentos integrantes da proposta e da documentação e a declaração deverão ser apresentados em original ou por qualquer processo de cópia autenticada por cartório competente ou ainda por servidor da Administração devidamente identificado ou publicação em órgão da imprensa oficial.

10.15 Documentos em idioma estrangeiro deverão ser acompanhados de tradução por tradutor juramentado, em original ou cópia autenticada, devendo a respectiva autenticação ser realizada pelo consulado correspondente.

11 RECURSOS

11.1 Declarado o vencedor ou se a licitação for fracassada, durante a sessão qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido prazo de **3 (três) dias úteis** para apresentação das razões do recurso, ficando os demais licitantes desde logo intimados **para apresentar contrarrazões em igual número de dias**, que começam a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

11.2 A falta de manifestação imediata e motivada do licitante importará a decadência do direito de recurso e a adjudicação do objeto da licitação pelo(a) pregoeiro(a) ao vencedor.

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

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

11.4.1 As razões e contrarrazões de recursos, quando feitas, deverão ser enviadas em formato digital por meio eletrônico, exclusivamente em campo próprio do

Sistema Eletrônico, e excepcionalmente e por orientação do(a) pregoeiro(a), por e-mail para **cpl-1@banparanet.com.br**.

11.5 O(a) pregoeiro(a) poderá não conhecer o recurso já nesta fase em situação excepcional e restrita, acaso a manifestação referida no subitem acima seja apresentada fora do prazo ou se o motivo apontado não guardar relação de pertinência com a licitação. Será vedado o(a) pregoeiro(a) rejeitar o recurso de plano em razão de discordância de mérito com os motivos apresentados pelo licitante.

11.6 Apresentadas as razões e contrarrazões, o(a) pregoeiro(a) disporá de 5 (cinco) dias úteis, prorrogáveis por iguais períodos, para reavaliar sua decisão e dar os seguintes encaminhamentos, conforme o caso:

a) Se acolher as razões recursais, deverá retomar a sessão pública para dar prosseguimento à licitação, garantindo, depois de nova declaração de vencedor, o direito à interposição de recurso, inclusive por parte de licitante que tenha sido impedido de participar da licitação, desde que tenha apresentado lances, que teve sua proposta desclassificada ou que foi inabilitado;

b) Se não acolher as razões recursais, deverá produzir relatório e encaminhar o recurso para a autoridade competente, para decisão definitiva, que deve ser produzida em 5 (cinco) dias úteis, prorrogáveis por iguais períodos. Nesta última hipótese, a autoridade competente deverá tomar a decisão definitiva sobre o recurso.

11.7 No julgamento dos recursos, o(a) pregoeiro(a) ou autoridade competente poderão sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, atribuindo-lhes validade e eficácia, mediante despacho fundamentado, em observância ao princípio da motivação dos atos administrativos, sendo amplamente divulgado, em observância ao princípio da publicidade.

11.8 A decisão definitiva sobre o recurso deverá ser publicada no sítio eletrônico do BANPARÁ e no site **www.gov.br/compras**.

11.9 O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

11.10 Os autos do processo permanecerão com vista franqueada aos interessados, no BANCO DO ESTADO DO PARÁ S/A, localizado à Av. Presidente Vargas, nº 251 – 1º

andar – Bairro do Comércio – Belém/PA, CEP: 66.010-000, no horário de 9h as 16h (horário local).

11.11 Apenas serão recebidas e analisadas **as razões de recursos e contrarrazões apresentadas tempestivamente e, exclusivamente, através de campo próprio do Sistema Eletrônico Comprasnet,** salvo os anexos que, quando necessário, poderão ser encaminhados via e-mail, para: **cpl-1@banparanet.com.br**, o que deverá ser indicado pelo licitante em suas razões recursais, a fim de que o(a) pregoeiro(a) possa divulgá-los no site **www.banpara.b.br**.

12 ADJUDICAÇÃO E HOMOLOGAÇÃO

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

12.2 Na fase de homologação, a autoridade competente poderá:

a) Homologar a licitação;

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

c) Anular a licitação por ilegalidade, salvo as situações em que:

i. O vício de legalidade for convalidável; ou

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

iii. O vício de legalidade não contaminar a totalidade do processo de licitação, caso em que deve determinar ao(à) pregoeiro o refazimento do ato viciado e o prosseguimento da licitação.

12.2.1 O vício de legalidade será convalidável se o ato por ele contaminado puder ser repetido sem o referido vício, o que ocorre, dentre outros casos, com vícios de competência e tocantes às formalidades.

12.2.2 A revogação ou anulação da licitação, depois da fase de apresentação de lances ou propostas, dependerá da concessão de prazo de 5 (cinco) dias úteis para que os licitantes interessados ofereçam manifestação.

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

12.3 Se a adjudicação não puder ocorrer dentro do período de validade da proposta, e, havendo interesse do BANPARÁ, este poderá solicitar prorrogação geral da validade acima referida, por igual prazo, no mínimo.

12.4 Em conformidade com o art. 2º, do **Decreto Estadual nº 877/2008**, o pagamento decorrente da contratação a ser realizada com base no presente certame somente **será efetuado mediante crédito em conta corrente aberta no Banco do Estado do Pará S/A**. Assim, caso o licitante vencedor não possua conta corrente nesta Instituição Financeira, **deverá providenciar a abertura desta no prazo de até 05 (cinco) dias úteis, a partir da assinatura do Contrato**, cabendo-lhe, ainda, apresentar os dados relativos aos números da Agência e Conta para o fiscal da contratação ou área gestora.

13 CONTRATAÇÃO

13.1 No prazo de até 15 (quinze) dias úteis após a homologação, o BANPARÁ convocará o licitante adjudicado para assinar o contrato e seus adendos, conforme minuta que integra o presente Edital – **ANEXO II.**

13.1.1 A convocação para assinatura do contrato deverá ser atendida pelo licitante adjudicado no prazo de 5 (cinco) dias úteis, prorrogável uma única vez a critério do BANPARÁ, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas.

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

13.2 Na ocasião da assinatura do contrato, será exigido do licitante adjudicado:

a) A apresentação do **termo de compromisso de política anticorrupção**, conforme adendo à minuta de contrato – Adendo 4 do Contrato;

b) Indicação da modalidade de **garantia de execução** que será prestada;

13.3 A recusa injustificada do licitante vencedor em assinar o instrumento contratual, dentro do prazo e condições estabelecidos, caracterizará o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas.

13.3.1 Ocorrendo o previsto no subitem acima, é facultado ao BANPARÁ rescindir o contrato por inadimplência, convocar os licitantes remanescentes, na ordem de classificação, para negociação e possível adjudicação ou revogar a licitação.

13.4 Todas as disposições sobre o contrato estão previstas na minuta do contrato, documento anexado ao edital - **ANEXO II.**

14 SANÇÕES ADMINISTRATIVAS

14.1. Com fundamento no Art. 98 do Regulamento, o licitante será sancionado com a suspensão temporária de participação em licitação no BANPARA, por prazo não superior a 2 (dois) anos, além das demais cominações legais cabíveis, nos seguintes casos:

a) Deixar de entregar a documentação exigida no certame;

b) Não mantiver a proposta de preços; incidindo também nesta hipótese a não apresentação das amostras ou realização de prova de conceito, salvo se em decorrência de fato superveniente;

c) Não assinar o contrato ou retirar a nota de empenho no prazo estabelecido.

d) Apresentar documentação falsa ou prestar declaração falsa;

e) Cometer ato fraudulento e/ou praticar atos ilícitos visando frustrar aos objetivos da licitação;

f) Cometer fraude fiscal ou comportar-se com má fé;

g) Comportar-se de modo inidôneo (Reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93, que se aplicam à Lei nº 13.303/2016 por força do disposto em seu art. 41).

14.2. Verificado o descumprimento ao presente Edital, o processo administrativo deverá ser instaurado por decisão do Presidente da Comissão de Licitação – CPL, nos termos do art. 99 do Regulamento, ocasião em que designará pregoeiro ou outro funcionário da área de licitações, para a adoção dos seguintes procedimentos:

a) Conduzir o processo administrativo;

b) Descrever os fatos e as faltas imputadas ao licitante;

c) Indicar a penalidade a que ele estará sujeito;

d) Determinar a notificação do licitante para apresentar a defesa, no prazo de até 10 (dez) dias, cuja intimação, assim como a defesa deverão ser realizadas por e-mail (art. 77 do Regulamento);

e) Analisar eventual pedido de produção de provas, podendo mediante decisão fundamentada, recusar as provas quando sejam ilícitas, impertinentes, desnecessárias, protelatórias;

f) Comunicar o licitante com antecedência mínima de três dias úteis, sobre o direito de acompanhar e participar de produção de provas, diligências, avaliações ou oitivas de testemunhas, se for o caso.

g) Conceder prazo de 10 (dez) dias para que o licitante apresente as alegações finais, no caso de ter havido produção de provas no processo.

14.3. Encerrado o referido prazo, com apresentação ou não das razões da empresa, o(a) pregoeiro(a) designado submeterá o processo à Diretoria Administrativa para decisão final, devidamente motivada, ouvido o NUJUR por meio de Parecer Jurídico.

14.4. Da decisão, o licitante será notificado por e-mail e mediante publicação no site www.banpara.b.br, podendo interpor recurso no prazo de 10 dias, sem efeito suspensivo, salvo se excepcionalmente concedido pela Diretoria Administrativa, por meio de decisão devidamente motivada e publicada nos meios pertinentes.

14.5. As penalidades referentes à inexecução do contrato estão estabelecidas na minuta do contrato - **ANEXO II** deste edital.

15. RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANPARÁ

15.1. Com fundamento no artigo 5º da Lei nº 12.846/2013, constituem atos lesivos ao BANPARÁ as seguintes práticas:

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

b) Impedir, perturbar ou fraudar a realização de qualquer ato do procedimento licitatório;

c) Afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) Fraudar a licitação ou contrato dela decorrente;

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

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

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

15.2. A prática, pelo licitante, de atos lesivos ao BANPARÁ, o 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.

15.3 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).

15.4 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.

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

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

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

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

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

15.7 A prática de atos lesivos ao BANPARÁ será apurada em Processo Administrativo de Responsabilização (PAR), instaurado pelo Diretor Presidente do BANPARÁ e conduzido por comissão composta por 2 (dois) funcionários designados.

15.8 Na apuração do ato lesivo e na dosimetria da sanção eventualmente aplicada, o BANPARÁ deve levar em consideração os critérios estabelecidos no art. 7º e seus incisos da Lei n. 12.846/201.

15.9 Caso os atos lesivos apurados envolvam infrações administrativas à Lei n.8.666/1993, ao Regulamento ou 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.

15.10 A decisão administrativa proferida pela autoridade julgadora ao final do PAR será publicada no Diário Oficial do Estado do Pará.

15.11 O processamento do PAR não interferirá na instauração e seguimento de processo administrativo específicos para apuração da ocorrência de danos e prejuízos ao BANPARÁ resultantes de ato lesivo cometido pelo licitante, com ou sem a participação de agente público.

15.12 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 n. 8.420/2015.

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

15.14 As disposições deste item se aplicam quando o licitante se enquadrar na definição legal do parágrafo único do art. 1º da Lei n. 12.846/2013.

16. DISPOSIÇÕES FINAIS

16.1. Os licitantes deverão observar os mais altos padrões éticos de probidade e boa-fé durante o processo licitatório e respectiva contratação, estando sujeitos às sanções previstas na legislação brasileira e nas normas internas do BANPARÁ.

16.2. Os licitantes serão responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados, em qualquer época. A apresentação de informações ou declarações com falsidade material ou intelectual sujeitará o licitante à aplicação da sanção de suspensão temporária do direito de participar de licitação, de acordo com os critérios do art. 98 do Regulamento, além das demais cominações legais.

16.3. As normas que disciplinam esta licitação serão sempre interpretadas em favor da ampliação da disputa entre os licitantes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

16.4. Os atos, comunicados, decisões e quaisquer documentos referentes a este processo licitatório serão sempre publicados no sítio eletrônico do BANPARÁ e, adicionalmente, no site **www.gov.br/compras**, poderão ser veiculados por e-mail aos licitantes e/ou mediante publicação no Diário Oficial do Estado do Pará.

16.5. A presente licitação poderá ter sua abertura adiada ou transferida para outra data, mediante aviso prévio, publicado de acordo com o disposto no Regulamento.

16.6. No intuito de dar celeridade ao processo licitatório, o BANPARÁ recomenda às interessadas em participar deste procedimento de licitação que providenciem a sua inclusão/atualização no Sistema de Cadastramento Unificado de Fornecedores (SICAF) para o(s) objeto(s) da presente licitação.

16.7. O processo de licitação, bem como todos os documentos a ele pertinentes, estão disponíveis para a realização de vistas. Para tanto, é necessário prévio agendamento junto ao(à) pregoeiro(a), por solicitação pelo e-mail **cpl-1@banparanet.com.br.**

16.8. Os licitantes são responsáveis por todos os custos de preparação e apresentação de suas propostas, documentos e amostras/protótipos, realização de prova de conceito, participação em visitas técnicas obrigatórias ou facultativas, não cabendo ao BANPARÁ qualquer responsabilidade por tais custos, independentemente da condução ou do resultado do processo licitatório.

16.9. Nenhuma indenização ou ressarcimento serão devidos aos licitantes pela elaboração de proposta ou apresentação de documentos ou, ainda, quando for o caso, apresentação de amostras/protótipos, realização de prova de conceito, participação em visitas técnicas obrigatórias ou facultativas, relativa a esta licitação.

16.10. Da sessão será lavrada ata eletrônica com a relação das licitantes e todas as ocorrências que interessarem ao certame, como a indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão Eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

16.11. O(a) pregoeiro(a) ou a Autoridade Superior poderão promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação, visando a obtenção da melhor proposta para a Administração.

16.12. A homologação do resultado desta licitação não implicará direito à contratação do objeto pelo BANPARÁ.

16.13. Para fins de aplicação das sanções administrativas constantes no presente edital, o lance é considerado proposta de preços.

16.14. O(a) pregoeiro(a) não desclassificará ou inabilitará qualquer licitante por falta de rubrica, erros ou omissões que não prejudiquem o curso do processo, cujas exigências possam ser satisfeitas no curso da sessão.

16.15. O licitante, através de consulta permanente, deverá manter-se atualizado quanto a quaisquer alterações e esclarecimentos sobre o edital, não cabendo ao BANPARÁ a responsabilidade por desconhecimento de tais informações, em face de inobservância do licitante quanto ao procedimento apontado neste subitem.

16.16. Esta licitação será regida pela Lei n. 13.303/2016, Regulamento de Licitações e Contratos do BANPARÁ, Lei n. 10.520/2002, Decreto n. 10.024/2019, da Lei Complementar n. 123/2006 e da Lei Estadual nº 8417/2016, do Decreto Estadual nº 2121/2018, da Lei nº 12.846/2013, e do Código Civil Brasileiro.

16.17. O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o local da realização do certame, considerado aquele a que está vinculado o(a) pregoeiro(a).

16.18. Fazem parte integrante deste edital os seguintes anexos:

ANEXO I – TERMO DE REFERÊNCIA
ANEXO II – MINUTA DE CONTRATO

Belém-Pará, 11 de agosto de 2021.

Fernanda Raia
Pregoeira

ANEXO I - TERMO DE REFERÊNCIA – TESTE DE INTRUSÃO

1 Objeto

Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework.

1.1 Parcelamento do objeto

Não haverá parcelamento do objeto, pois considerando que o serviço a ser adquirido possui a mesma natureza, e, em face da inviabilidade técnica de divisibilidade do fornecimento a ser contratado.

2 JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1 Razão da necessidade da contratação:

O Programa de Segurança do Cliente é um programa que a SWIFT criou para ajudar a comunidade de usuários da SWIFT a melhorar a segurança cibernética e facilitar a avaliação de riscos de segurança cibernética diretamente, e entre os usuários e inclui iniciativas como as definidas na Estrutura de controles de segurança do cliente SWIFT (CSCF – Costumer Security Crontrol Framework), na Política de controles de segurança do cliente SWIFT (CSCP) ou no SWIFT ISAC.

Para realizar negócios na rede SWIFT, os usuários (bancos) precisam ter um contato/relacionamento com outros usuários SWIFT. Os usuários devem estabelecer tais relacionamentos levando em consideração vários critérios. Além de considerações comerciais óbvias, esses critérios normalmente se relacionam à conformidade com KYC e sanções / ALM (Aint Laundry Money – Anti – lavagem de dinheiro), risco operacional, segurança cibernética e fraude.

A segurança da informação é de alta relevância no estabelecimento de relações comerciais entre os usuários do SWIFT. Como com os outros critérios, requer avaliação pelo usuário de todos os seus negócios homólogos. Cada usuário é, portanto, responsável por aplicar sua própria avaliação de risco e contra seu próprio apetite ao risco e, normalmente, usa várias fontes e categorias de informações para fazer isso. A SWIFT, como uma cooperativa de propriedade dos membros, desenvolveu várias iniciativas sob o

SWIFT Customer Security Program para o benefício coletivo de sua comunidade de usuários, conforme estabelecido no SWIFT Customer Security Controls Framework (CSCF) e na Política de controles de segurança do cliente SWIFT (CSCP) ou o SWIFT ISAC, projetados para ajudar a comunidade de usuários SWIFT a melhorar a segurança cibernética.

As funções e responsabilidades da SWIFT por essas iniciativas são separadas da função e responsabilidades como fornecedor de serviços e produtos SWIFT. No contexto do CSCF e CSCP, que fazem parte do SWIFT Customer Security Program, o SWIFT está atuando como facilitador de padrões e transparência em relação ao status de conformidade de segurança cibernética os usuários. Nos termos do CSCP, os usuários devem atestar-se contra os controles de segurança estabelecidos no CSCF. Embora a SWIFT se reserve o direito de relatar falhas em seu cumprimento, cada usuário permanece única e exclusivamente responsável por qualquer confiança e, mais geralmente, qualquer decisão de trocar (ou parar ou suspender a troca) de mensagens ou arquivos com outro usuário e definir e implementar controles de suporte apropriados e outros arranjos.

A partir de 2020, todos os usuários (bancos) da SWIFT, por demanda da rede SWIFT, serão obrigados a realizar uma avaliação independente ao serem atestados. Isso pode ser feito através de Avaliação externa realizada por uma organização externa independente com experiência em avaliação de segurança cibernética e avaliadores individuais que possuem certificação relevante no setor de segurança.

No mínimo, as avaliações independentes devem abranger todos os controles obrigatórios na versão mais recente da Estrutura de controles de segurança do cliente (CSCF) aplicáveis a partir do seu tipo de arquitetura e infraestrutura de CSP.

2.2 A demanda do BANPARÁ tem como base as seguintes informações e histórico de necessidades:

O presente Projeto Básico visa fornecer um conjunto de especificações técnicas com intuito subsidiar processo de licitação para contratação de auditoria em Segurança da Informação para avaliação da estrutura interna cibernética, a fim de atender a demanda da SWIFT.

3 Modalidade da Licitação

Pregão Eletrônico.

3.1 Da Justificativa da Modalidade

O objeto caracterizado por este Termo de Referência tem padrões de qualidade e desempenho definidos objetivamente, além de tratar-se de objeto plenamente disponível no mercado. Desse modo consoante previsão do art. 1º da lei nº 10.520/02 c/c art. 2º do Dec. Fed. Nº 5.450/05.

3.2 Das Restrições de competição previstas em Lei

Não será permitida a subcontratação, no todo ou em parte, do objeto deste certame licitatório sem a prévia anuência do contratante desde que não se refira a parcela sobre a qual o Banpará exigiu atestado de capacidade técnica durante o processo licitatório.

3.3 Condições de Participação:

Não será permitida a participação de empresas reunidas em consórcio ou cooperativa uma vez que os serviços prestados em cada um dos itens exigem elevada especialização técnica e controle uníssono para fiscalização do contrato.

4 Modo de Disputa

Aberto e Fechado.

4.1 Critério de julgamento

Menor Preço

5 Critério de valor

Valor máximo aceitável

6. Da Especificação do Item

Item	Objeto	Descrição
1	Serviço de Auditoria em Segurança da Informação	Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISSO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework, conforme descritas nos termos do Edital, Termo de Referência e seus anexos

6.1 Detalhamento do Item

6.1.1 Trata-se de um objeto diferenciado da maioria dos serviços de auditoria fornecido no mercado, haja vista a necessidade do conhecimento extremamente técnico e especializado do executor contratado, e que seja capaz de realizar uma entrega de serviço em conformidade com o necessitado pelo Banpará em consonância com o exigido pela SWIFT.

Com isso tem-se clara a singularidade do objeto, no qual se faz necessária a contratação de empresa com equipe comprovadamente especializada e, portanto, com experiência comprovada em estudos semelhantes, dada a especialidade da análise a ser implementada.

6.1.2 É relevante explicitar que o produto deve ser havido como singular quando nele interferir um componente, estilo, capacidade ou qualidade de quem o produz. É o que ocorre quando os conhecimentos científicos, tecnológicos, organizacionais e experiência do produtor influem diretamente no produto, impregnando sua específica individualidade e habilitação pessoal, como é o caso desta auditoria.

7. Serviços

7.1 Escopo de Avaliação

7.1.1 A avaliação deve cobrir todos os controles obrigatórios estabelecidos na versão mais recente do Customer Security Controls Framework (CSCF), que são aplicáveis a esse usuário em consonância com seu tipo de arquitetura e infraestrutura. Essa avaliação será acompanhada por um auditor interno do Banpará.

7.1.2 A avaliação inclui todos os componentes no escopo da infraestrutura relacionada ao SWIFT do usuário, conforme documentado no CSCF. Estes incluem os seguintes sistemas básicos, operadores e dispositivos, quando relevante:

7.1.2.1 Camada de troca de dados

7.1.2.2 Middleware Server é aconselhado para consideração, embora não seja obrigatório

7.1.2.3 Infraestrutura SWIFT local

7.1.2.4 Zona segura

7.1.2.5 Interface de mensagens

7.1.2.6 Interface de Comunicação

7.1.2.7 Link SWIFTNet (SNL)

7.1.2.8 Conector

7.1.2.9 Módulos de segurança de hardware SWIFT (HSMs)

7.1.2.10 Firewalls, roteadores e switches dentro ou ao redor da infraestrutura SWIFT

7.1.2.11 Interface gráfica do usuário (GUI)

7.1.2.12 Jump Server

7.1.2.13 Plataforma de Virtualização

7.1.2.14 PC operador dedicado

7.1.2.15 Operadores e seus PCs de Operador Geral

7.1.3 A avaliação deve confirmar o tipo de arquitetura selecionado e abranger todos os ambientes de produção, recuperação de desastres (DR) e/ou backup (conforme aplicável) que abrigam qualquer um dos sistemas, operadores ou dispositivos acima.

7.1.4 O SWIFT recomenda que os usuários definam completa e precisamente o escopo da avaliação com seu (s) avaliador (es) em potencial durante o processo de aquisição do fornecedor. Isso pode ajudar a evitar mal-entendidos e mitigar substancialmente quaisquer riscos associados ao excesso ou falta de abrangência da iniciativa de avaliação.

7.1.5 Uma vez estabelecido o escopo, o tempo pode ser determinado para garantir que o relatório será entregue a tempo de permitir que o usuário envie seu Attestation KYC-SA associado para KYC-SA dentro da janela de atestado normal - de 1 de julho até o prazo final do ano de 10 de dezembro. Como tal, o planejamento deve incluir o tempo necessário para que o assessor documente os achados associados a todos os controles no escopo, para elaborar os relatórios e revisar outros resultados devidos ao usuário na conclusão da avaliação para abordar possíveis exceções identificadas, a fim de concluir alguma conformidade final.

7.2 Abordagem Baseada em Risco

7.2.1 Os avaliadores devem usar uma abordagem baseada em risco para avaliar a conformidade do usuário com os objetivos de controle de CSP; ou seja, avaliar a meta de segurança, independentemente do método de implementação usado (sejam as diretrizes de implementação sugeridas ou alternativas).

7.2.2 Para cumprir um controle CSP, os usuários devem implementar uma solução que:

7.2.2.1 Atende ao objetivo de controle declarado,

7.2.2.2 Aborda os riscos, e

7.2.2.3 Abrange os componentes documentados dentro do escopo relevantes para a arquitetura do usuário.

7.2.3 A ‘Declaração de Controle’ é um meio sugerido para cumprir o objetivo de controle e as diretrizes de implementação são métodos comuns para cumprir o objetivo. Mesmo que as diretrizes possam ser uma boa maneira de iniciar uma avaliação, a seção de orientação de implementação nunca deve ser considerada uma "lista de verificação de auditoria", pois a implementação de cada usuário pode variar. Portanto, no caso de alguns elementos não estarem presentes ou parcialmente cobertos, as mitigações, bem como as especificidades ambientais particulares devem ser levadas em consideração para avaliar adequadamente a conformidade geral e o nível de adesão (novamente, de acordo com as diretrizes sugeridas ou conforme alternativas). O uso de diretrizes sugeridas ou métodos alternativos é considerado equivalente do ponto de vista do risco.

7.3 Recursos de Avaliação Disponíveis

7.3.1 Os avaliadores externos ou usuários devem possuir registro no SWIFT (normalmente no Programa de Parceiros SWIFT) para que tenham acesso direto ao treinamento e outros materiais de avaliação.

7.4 Orientação de segurança e documentação

7.4.1.1 SWIFT fornece documentos de orientação de segurança específicos do produto. Estes estabelecem as recomendações relacionadas à segurança da SWIFT para clientes que usam produtos SWIFT, como: Alliance Web Platform Server-Embedded, Alliance Access / Entry, Alliance Gateway e SWIFTNet Link, Alliance Lite2, AGI, bem como todas as versões do Alliance Messaging Hub (AMH) O mapeamento entre os controles CSCF e a Orientação de Segurança da Aliança é registrado em um documento separado; para AMH, esse mapeamento está incluído no próprio documento de Orientação de Segurança AMH.

7.4.1.2 Os usuários e avaliadores do SWIFT são fortemente encorajados a ler os documentos de orientação de segurança relevantes e verificar a implementação em sua configuração SWIFT local.

7.5 Modelos e formulários de avaliação

7.5.1.1 Para conveniência dos usuários e para garantir uma abordagem consistente para o processo de avaliação, o SWIFT fornece aos usuários modelos e formulários padronizados. Esses incluem:

a) Uma 'carta de confirmação de solicitação de avaliação', que uma instituição usará para responder a uma solicitação de avaliação obrigatória SWIFT

b) Uma carta de 'Notificação de Seleção de Avaliador Externo' que uma instituição usará para avaliações obrigatórias SWIFT

c) Modelos de avaliação de controles obrigatórios e consultivos baseados em Excel para todos os tipos de avaliações

d) Um documento Word de 'Carta de Conclusão da Avaliação' ou todos os tipos de avaliações

7.5.2 O SWIFT fornece esses modelos para capturar os detalhes e resultados das avaliações para os avaliadores. Existem modelos separados disponíveis para controles obrigatórios e consultivos no CSCF.

7.5.3 O uso desses modelos é recomendado, mas não obrigatório para avaliações Community-Standard ou SWIFT Mandated. Esses modelos, no entanto, fornecem um meio consistente para os avaliadores documentarem e relatarem os resultados da avaliação

7.5.4 Os avaliadores que aparecem no diretório de provedores de avaliação CSP são registrados no Programa de Parceria SWIFT

7.5.5 Os modelos de avaliação estão diretamente relacionados ao CSCF e destacam quais controles do CSCF são aplicáveis ao tipo de arquitetura do usuário. Para cada controle aplicável, o modelo relevante define o objetivo do controle e qualquer princípio (s) -chave subjacente. Usando o modelo, o avaliador pode então confirmar se aqueles que são aplicáveis ao usuário são alcançados, seja por meio da orientação de implementação do SWIFT ou, para instituições tipicamente grandes ou complexas, por meio de um método de implementação alternativo.

7.5.6 O usuário pode encontrar os materiais de avaliação mais atualizados online por meio do portal swift.com. A SWIFT recomenda que os usuários verifiquem rotineiramente este portal para garantir que eles e seus avaliadores estejam usando as versões mais recentes dos formulários e modelos disponíveis para a comunidade SWIFT.

7.5.7 Os avaliadores podem preencher os modelos de avaliação do Excel usando seu idioma nativo; a carta de conclusão deve, no entanto, ser preenchida em inglês.

7.6 Material de Treinamento

7.6.1 Para usuários ou avaliadores com acesso direto ao portal swift.com, recursos de treinamento SWIFTSmart estão disponíveis em tópicos relacionados a CSP e CSCF.

7.6.2 Todos os avaliadores selecionados para executar o processo de avaliação do CSCF devem ser devidamente qualificados e conduzir a avaliação de forma independente.

7.7 Resultados da Avaliação

7.7.1 A seção a seguir descreve os resultados recomendados (opcionais) e obrigatórios para os avaliadores.

7.8 Relatório de Avaliação

7.8.1.1 Os avaliadores devem fornecer aos usuários

a) um relatório formal descrevendo a confirmação do avaliador de conformidade para cada controle, juntamente com a documentação dos defeitos de implementação observados e

b) uma carta de conclusão confirmando que o trabalho foi realizado com a objetividade e independência exigidas e com escrutínio suficiente.

7.8.1.2 Para avaliações obrigatórias do SWIFT e padrão da comunidade, os avaliadores devem garantir que o relatório reflita o resultado documentado nos modelos de avaliação. A SWIFT também recomenda que os avaliadores incluam um relatório de nível executivo em qualquer avaliação CSCF. Além disso, para uso em instruções à administração da empresa, esses relatórios podem ajudar a rastrear os resultados da avaliação anual. O relatório de avaliação não deve ser enviado proativamente à SWIFT.

7.8.1.3 Espera-se que todos os usuários rastreiem devidamente a resolução da não conformidade e, quando tratada a critério do avaliador, atualize seu status no KYC-SA conforme a próxima seção.

7.8.1.4 Para avaliações obrigatórias de SWIFT e padrão da comunidade, uma carta de conclusão de avaliação formal também deve ser preparada utilizando o modelo fornecido, conforme apropriado. Embora não deva ser enviado para o SWIFT de forma proativa, deve ser disponibilizado mediante solicitação. Portanto, espera-se que os usuários garantam que a carta de conclusão seja mantida com segurança durante o período em que a avaliação sustentar seu atestado.

8. Níveis Mínimos de Serviço/ Indicadores de Desempenho Esperados

8.1 A determinação dos níveis de serviço, ou SLA tem por finalidade garantir a qualidade na prestação dos serviços pela contratada para execução dos serviços descritos no objeto deste termo de referência e seus anexos;

8.2 A contratada deverá consignar os resultados das auditorias em relatórios circunstanciados, elaborados com 30 dias de antecedência ao prazo estipulado pela Swift. Nos quais constarão descrição dos exames efetuados e as observações e recomendações quando necessárias, devendo ser entregues:

8.2.1 Dentro do prazo necessário, definido antecipadamente pela administração do Banco, para atender os órgãos reguladores (Swift) e as aprovações internas (Conselho Fiscal e Conselho de Administração), os relatórios de auditoria semestral e anual;

8.2.2 Em 20 (vinte) dias uteis, após o termino das auditorias, relatório circunstanciado de revisão de critérios adotados pelo BANPARÁ quanto a classificação nos níveis de risco;

8.2.3 Com antecedência de 15 (quinze) dias, contados do início dos trabalhos, Plano de Auditoria e Cronograma das Atividades a serem desenvolvidas com vistas a atender o objeto do contrato, para cada visita.

8.2.4 A não observância dos níveis de SLA mínimos definidos, desde que tenha havido culpa exclusiva e comprovada da contratada, será passível de aplicação das penalidades convencionadas e genéricas conforme definido em contrato.

9. Das Definições do Acordo de Nível de Serviços (SLA).

9.1 A contratada deverá manter a qualidade e os níveis mínimos determinados pelo BANPARÁ na prestação dos serviços contratados, obedecendo às referências determinadas pelo contratante;

9.2 A contratada deverá manter, medir e relatar os níveis de serviços contratados gerenciando os processos e conduzindo projetos de forma a manter os níveis estabelecidos neste módulo.

9.3 A contratada deverá efetuar mensalmente apresentação consolidada e explicativa da medição dos níveis de serviços, sendo que esta deverá relatar e detalhar as ocorrências adversas, bem como planos de ação para normalizar as desconformidades nos níveis de serviços;

9.4 O contratante se resguarda o direito de verificar os níveis de serviço, inclusive com o direito de realizar verificações in loco.

10. Dos Requisitos de Habilitação

10.1 Requisitos de Qualificação Técnica

10.1.1 A empresa licitante deverá apresentar experiência recente e relevante através de carta de circularização para executar uma avaliação operacional orientada para segurança cibernética para um padrão da indústria, como PCI DSS, NIST SP 800-53, a NIST Cybersecurity Framework ou simplesmente CSP/CSCF nos 12 meses anteriores a licitação deste edital com comprovação. Estas obrigações dar-se-ão devido a orientação da SWIFT, através do Customer Security Programme, sendo assim é necessário termos empresas qualificadas para a execução do objeto deste Termo de Referência.

10.1.2 O(s) atestado(s)/certidão(ões)/declaração(ões) deverá(ão) ser apresentado(s) em papel timbrado da pessoa jurídica, contendo a identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico, para contato e deve(m) indicar as características, quantidades e prazos das atividades executadas ou em execução pela licitante vencedora.

10.1.3 Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da CONTRATADA.

10.1.4 O(s) atestado(s)/certidão(ões)/declaração(ões) apresentado poderá ser objeto de diligência a critério do Banpará, para verificação da autenticidade de seu conteúdo. Encontrada qualquer divergência entre a informação apresentada pela CONTRATADA e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviço assinado entre o emissor e a LICITANTE, além da desclassificação sumária do Pleito, a empresa fica sujeita às penalidades cabíveis e aplicáveis.

10.1.5 Certidão Negativa de Licitante Inidôneo do Tribunal de Contas do Estado do Pará e do Tribunal de Contas da União.

10.2 PERFIS PROFISSIOGRÁFICOS

10.2.1 A seguir estão relacionadas exigências de perfis dos profissionais que executarão os serviços dos itens 1 e 2 do objeto dessa contratação. A comprovação se dará através da apresentação tempestiva de currículos detalhados, diplomas, e documentação das certificações (dentro do período de validade), exigidas na data da assinatura do contrato.

10.2.2 O CONTRATANTE se reserva o direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

10.2.3 A CONTRATADA deve retirar dos serviços qualquer empregado que, a critério do BANPARÁ, seja julgado inconveniente ao bom andamento dos trabalhos;

10.2.4 Comprovação de possuir no seu quadro permanente no ato da contratação, no mínimo, em conjunto de profissionais com os certificados abaixo:

10.2.5 No momento da assinatura do contrato a CONTRATADA deverá apresentar a lista de profissionais, com suas devidas certificações, que poderão atuar nos testes.

10.2.6 A prestação do Serviço deverá ser realizada por equipe de profissionais que possua, pelo menos uma das seguintes certificações relevantes para o setor, pois para a SWIFT, através do Customer Security Programme, é necessário que o profissional possua certificação para executar a avaliação:

Item	Certificação
1	**PCI Qualified Security Assessor (QSA)**

2	**Certified Information Systems Security Professional (CISSP)**
3	**Certified Information Systems Auditor (CISA)**
4	**Certified Information Security Manager (CISM)**
5	**ISO 27001 Lead Auditor**
6	**System Administration, Networking, and Security Institute (SANS)**

10.2.7 CONTRATADA deverá apresentar, também na assinatura do contrato, alista dos profissionais, com seus currículos e a comprovação da exigência de certificação acima, suas responsabilidades em cada etapa (testes externos, testes internos, análise de aplicações web), quais atuarão on site (no Banpará) e quais atuarão remotamente e, por fim, a comprovação de seu vínculo empregatício com a CONTRATADA.

10.2.8 Caso a CONTRATANTE considere necessário, o responsável Técnico deverá, durante as análises e testes internos, estar presente, dependências do CONTRATANTE para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE;

10.3 Dos Documentos Comprobatórios aos Critérios de Sustentabilidade

10.3.1 A contratada se compromete, sob pena de infração e rescisão contratual, a:

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

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

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

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

10.3.6 Buscar a incorporação em sua gestão dos Princípios do Pacto Global, disponível em http:http://www.pactoglobal.org.br/artigo/56/Os-10-principios, bem como o alinhamento com as diretrizes da Política de Responsabilidade Socioambiental do Banpará disponível em http://www.banpara.b.br/media/187386/prsa.pdf;

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

10.3.8 Desenvolver suas atividades respeitando a legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como os demais dispositivos legais relacionados proteção dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se:

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

10.3.9 A CONTRATANTE poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o Contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia defesa, caso se comprove que a CONTRATADA, subcontratados ou fornecedores utilizem-se de trabalho em desconformidade com as condições referidas nas cláusulas supracitadas.

10.3.10 Plano de Gerenciamento de Resíduos Sólidos ou Declaração de Sustentabilidade Ambiental;

10.3.11 Certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências do edital.

11. Requisitos de Qualificação Econômico Financeira:

11.1 Na habilitação econômico-financeira, a Licitante deverá apresentar os seguintes documentos:

11.1.1 Certidão negativa de feitos sobre falência, expedida pelo cartório distribuidor da comarca da sede da pessoa jurídica, somente será aceita com o prazo máximo de 90 (noventa) dias, contados da data de sua emissão.

a) Agente econômico em recuperação judicial ou extrajudicial pode participar de licitação, desde que atenda às condições para comprovação da capacidade econômica e financeira previstas no edital.

11.1.2 Balanço patrimonial e demais demonstrações contábeis do último exercício social, já exigível e apresentado na forma da lei:

a) Para Sociedades Anônimas, cópia autenticada da publicação do Balanço Patrimonial em diário oficial ou jornal de grande circulação da sede da empresa Licitante;

b) Para as Sociedades Limitadas e demais empresas, cópias legíveis e autenticadas das páginas do livro diário, onde foram transcritos o Balanço Patrimonial e a Demonstração do Resultado do último exercício social, com os respectivos termos de abertura e de encerramento registrados na Junta Comercial; OU no caso de empresas com obrigatoriedade por lei de Registro de suas demonstrações em outros órgãos, deverá apresentar tais demonstrações registradas em tais órgãos.

c) Demonstrações Contábeis elaboradas via escrituração contábil digital, através do Sistema Público de Escrituração Digital – SPED. **Os tipos societários obrigados e/ou optantes pela Escrituração Contábil Digital – ECD, consoante disposições contidas no Decreto nº 6.022/2007, regulamentado através da IN nº 1420/2013 da RFB e alterações, apresentarão documentos extraído do Sistema Público de Escrituração Digital – SPED na seguinte forma:**

I. Recibo de Entrega de Livro Digital transmitido através do Sistema Público de Escrituração Digital – Sped, nos termos do decreto 8.683/2016, desde que não haja indeferimento ou solicitação de providências;

II. Termos de Abertura e Encerramento do Livro Diário Digital extraídos do Sistema Público de Escrituração Digital – Sped;

III. Balanço e Demonstração do Resultado do Exercício extraídos do Sistema Público de Escrituração Digital – Sped.

11.1.2.1 As empresas com menos de 01 (um) ano de existência, que ainda não tenham balanço de final de exercício, deverão apresentar demonstrações contábeis envolvendo seus direitos, obrigações e patrimônio líquido, relativos ao período de sua existência, bem como, balanço de abertura ou documento equivalente, devidamente assinado por contador e arquivado no órgão competente;

11.1.3 Índices de Liquidez Corrente (**LC**), de Liquidez Geral (**LG**) e de Solvência Geral (**SG**) **≥ 1.0 (maior ou igual a um).**

a) Os índices descritos no subitem acima, deverão ser apurados com base no Balanço Patrimonial e demais demonstrações contábeis do último exercício social e apresentados de acordo com as seguintes fórmulas:

$$\mathbf{LC} = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

$$\mathbf{LG} = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$\mathbf{SG} = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

b. As empresas que apresentarem quaisquer dos índices calculados na alínea anterior **inferiores a um (<1)** deverão comprovar Capital Social ou Patrimônio Líquido de valor não inferior a 10% (dez por cento) do valor cotado na sessão.

c. As microempresas ou empresas de pequeno porte devem atender a todas as exigências para comprovação da capacidade econômica e financeira previstas no edital.

12. Da Visita Técnica

Não haverá necessidade de Visita Técnica visto o objeto deste Termo de Referência.

13. Da Adjudicação do Objeto

Global.

14. Das Condições de Contratação

14.1 A empresa licitante deverá demonstrar qualificação técnica necessária à prestação dos serviços apresentando material que comprove a posse de portfólio de serviços de auditoria em segurança da informação sendo uma condição de contratação.

14.2 A empresa deve apresentar currículo assinado pelo próprio profissional, de pelo menos um dos profissionais que participarão das avaliações, que contemple ao menos um dos seguintes certificados:

Item	Certificação
1	**PCI Qualified Security Assessor (QSA)**
2	**Certified Information Systems Security Professional (CISSP)**
3	**Certified Information Systems Auditor (CISA)**
4	**Certified Information Security Manager (CISM)**
5	**ISO 27001 Lead Auditor**
6	**System Administration, Networking, and Security Institute (SANS)**

14.2.1 As certificações apresentadas no item anterior garantem que a empresa vencedora executará com excelência o objeto do certame, uma vez que são certificações solicitadas pela SWIFT através do Customer Security Programme, reconhecidas nacional e internacionalmente.

15. Da Garantia

15.1 Da Garantia Contratual

15.1.1 A **CONTRATADA** deverá apresentar à Administração do **CONTRATANTE**, no prazo máximo de 10 (dez) dias úteis, contados da data do protocolo de entrega, ou de Aviso de Recebimento (AR), caso o envio se dê pelos Correios, da via do contrato assinada, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor anual atualizado do contrato, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

15.1.2 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

f) Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

g) Prejuízos causados à administração ou à terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

h) As multas moratórias e punitivas aplicadas pela Administração à **CONTRATADA**;

i) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela **CONTRATADA**.

15.1.3 Não serão aceitas garantias na modalidade seguro-garantia em cujos termos não constem expressamente os eventos indicados nas letras “a” a “d” desta cláusula.

15.1.4 A garantia em dinheiro deverá ser efetuada na Agência Empresarial do Banpará, em conta Poupança específica com correção monetária, aberta em favor da **CONTRATADA** e que ficará bloqueada para movimentações e saques pelo período em que viger o contrato.

15.1.5 A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento).

15.1.6 O garantidor deverá declarar expressamente que tem plena ciência dos termos do Edital e das cláusulas contratuais.

15.1.7 O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Banpará com o objetivo de apurar prejuízos e/ou aplicar sanções à **CONTRATADA**.

15.1.8 Será considerada extinta a garantia:

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 da Administração, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do contrato;

b) Com a extinção do contrato.

15.1.9 Isenção de responsabilidade da garantia:

15.1.10 O Banpará não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

a) Caso fortuito ou força maior;

b) Alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;

c) Descumprimento das obrigações pela **CONTRATADA** decorrentes de atos ou fatos praticados pela Administração;

d) Atos ilícitos dolosos praticados por servidores da Administração.

15.1.11 Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.

15.1.12 Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pelo **CONTRATANTE** à **CONTRATADA** e/ou à Instituição Garantidora, no prazo de até 90 (noventa) dias após o término de vigência do contrato.

15.2 Da Garantia do Objeto

15.2.1 A contratada assumirá integral responsabilidade pela boa execução e eficiência dos serviços que efetuar de acordo com as especificações e demais documentos técnicos fornecidos.

15.2.2 Todos os bens licitados devem atender às recomendações da Associação Brasileira de Normas Técnicas - ABNT (Lei n.º 4.150 de 21.11.62), no que couber e, principalmente no que diz respeito aos requisitos mínimos de qualidade, utilidade, resistência e segurança.

16. Características e Condições da Execução do Contrato

16.1 A execução do contrato será iniciada a partir da assinatura do mesmo.

16.2 Da validade

16.2.1 O prazo de vigência do contrato será de 12 (doze) meses, contados da assinatura do mesmo, podendo ser prorrogado a critério do Banpará, conforme legislação vigente.

16.3 Do Recebimento do Objeto

16.3.1 Concluída a realização dos serviços solicitados, a CONTRATADA deverá comunicar este fato formalmente a CONTRATANTE. O BANPARÁ emitirá o documento de aceite que deverá conter as informações relacionadas a execução e ser assinado por responsáveis da CONTRATADA e pelo Gestor Técnico do BANPARÁ.

16.4 Obrigações da Contratada

16.4.1 Adicionalmente às responsabilidades estabelecidas nos demais tópicos constantes deste documento, incumbe à contratada observar os seguintes requisitos:

16.4.2 Cumprir os prazos e obrigações estabelecidas no Edital.

16.4.3 Prestar os serviços no prazo, quantidade e especificações solicitadas conforme as características descritas na sua proposta e no edital.

16.4.4 Observar as normas e procedimentos internos do CONTRATANTE no que se refere à segurança (Política de Segurança cibernética – ADENDO V) e sigilo dos dados manuseados, bem como no que é pertinente à documentação (Termo de Confidencialidade, Acordo de Confidencialidade da Informação e Responsabilidade – ADENDO IV, sobre os quais se obriga a dar ciência a seus funcionários, que tiverem acesso às dependências do CONTRATANTE, e aos que possuírem acesso remoto);

16.4.5 Alocar profissionais necessários à realização dos serviços, de acordo com a experiência profissional e qualificação técnica exigida, apresentando a documentação que comprove a qualificação.

16.4.6 Dar conhecimento a todos os profissionais que venham a prestar serviços relacionados ao objeto contratado, os processos de trabalho, políticas e normas internas do CONTRATANTE, bem como zelar pela observância de tais instrumentos.

16.4.7 Informar imediatamente ao CONTRATANTE a ocorrência de transferência, remanejamento, promoção ou demissão de profissional sob sua responsabilidade, para providências de revisão, modificação ou revogação de privilégios de acesso a sistemas, informações e recursos do CONTRATANTE.

16.4.8 Prestar os serviços no prazo, quantidade e especificações solicitadas conforme as características descritas na sua proposta e no edital;

16.4.9 Colocar, nos prazos contratados, os profissionais à disposição do CONTRATANTE para execução dos serviços;

16.4.10 Responsabilizar–se pelos encargos fiscais e comerciais resultantes desta contratação e ainda pelos encargos trabalhistas, previdenciários, securitários, tributos e contribuições sociais em vigor, obrigando-se a saldá-los nas épocas próprias, haja vista que os empregados da CONTRATADA não manterão qualquer vínculo empregatício com a CONTRATANTE;

16.4.11 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

16.4.12 Responsabilizar-se pelos danos causados direta ou indiretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo quando do fornecimento dos produtos contratados, não excluindo ou reduzindo essa responsabilidade em caso de fiscalização e/ou acompanhamento pelo CONTRATANTE;

16.4.13 Manter garantia contra defeitos de hardware e software, inclusive atualização de versões dos programas utilizados para objeto deste Edital;

16.5 Obrigações da Contratante

16.5.1 Fiscalizar o fornecimento do objeto deste Edital, podendo sustar, recusar, mandar fazer ou desfazer qualquer fornecimento dos produtos/serviços que não estejam de acordo com as normas, especificações e técnicas usuais;

16.5.2 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA sobre os produtos objeto desta licitação;

16.5.3 Acompanhar e atestar nas Notas-Fiscais/Faturas a efetiva entrega do produto/serviço do objeto deste Edital;

16.5.4 Aplicar à CONTRATADA as penalidades regulamentares e contratuais, previstas em lei e neste Edital;

16.5.5 Comunicar à CONTRATADA, quaisquer irregularidades observadas no objeto deste Edital.

16.5.6 Verificar a regularidade da situação fiscal da CONTRATADA, antes de efetuar o pagamento devido.

16.5.7 Proceder às advertências, descontos e demais cominações legais pelo descumprimento das obrigações assumidas pela CONTRATADA.

16.5.8 Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado, pelas demais empresas fornecedoras, de forma a garantir que continuem a serem os mais vantajosos para a Administração.

17. Das Sanções Administrativas

17.1 A CONTRATADA, em caso de inadimplemento de suas obrigações, garantido o contraditório e ampla defesa anteriormente a sua aplicação definitiva, ficará sujeita às seguintes sanções previstas no Regulamento de Licitações e Contratos do BANPARÁ - RLC disponível no endereço https://www.banpara.b.br/media/233274/regulamento_de_licita__es_e_contratos.pdf e na Lei nº 13.303, de 2016:

a) advertência;

b) multa moratória;

c) multa compensatória;

d) multa rescisória, para os casos de rescisão unilateral, por descumprimento contratual;

e) suspensão do direito de participar de licitação e impedimento de contratar com o BANPARÁ , por até 02 (dois) anos.

17.2 As sanções previstas nos incisos “a” e “e” poderão ser aplicadas com as dos incisos “b”, “c” e “d”.

17.3 O contratado que cometer qualquer das infrações elencadas artigos 98 e 99 da RLC, dentre outras apuradas pela fiscalização do contrato durante a sua execução, ficará sujeito, sem prejuízo da responsabilidade civil e criminal, as sanções previstas neste item.

17.4 A aplicação das penalidades previstas neste item realizar-se-á no processo administrativo da contratação assegurado a ampla defesa e o contraditório à Contratada.

17.5 A aplicação de sanção administrativa e o seu cumprimento não eximem o infrator da obrigação de corrigir as irregularidades que deram origem à sanção.

17.6 A multa, aplicada após regular processo administrativo, será descontada da garantia do respectivo contratado. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Conab ou ainda, quando for o caso, cobrada judicialmente.

17.7 Da sanção de advertência:

17.7.1 A sanção de advertência é cabível sempre que o ato praticado não seja suficiente para acarretar prejuízo ao BANPARA, suas instalações, pessoas, imagem, meio ambiente, ou a terceiros.

17.7.2 A aplicação da sanção do subitem anterior importa na comunicação da advertência à contratada, devendo ocorrer o seu registro junto ao SICAF.

17.8 Da sanção de multa:

17.8.1 A multa poderá ser aplicada nos seguintes casos:

a) em decorrência da não regularização da documentação de habilitação, nos termos do art. 43, § 1° da Lei Complementar n° 123, de 2006, deverá ser aplicada multa correspondente a 5% (cinco por cento) sobre o valor estimado para a licitação em questão;
b) em decorrência da prática por parte do licitante/adjudicatário das condutas elencadas artigos 98 e 99 da RLC deverá ser aplicada multa correspondente a 5% (cinco por cento) sobre o valor estimado para a licitação em questão;
c) pela recusa em assinar o Contrato dentro do prazo estabelecido pelo instrumento convocatório, deverá ser aplicada multa correspondente a 5 % (cinco por cento) sobre o valor homologado para a licitação em questão;
d) multa moratória por atraso injustificado na entrega da garantia contratual, conforme item 15.1.5 do Termo de Referência;
e) multa moratória de 0,2 % (dois décimos por cento) sobre o valor anual do contrato, por dia de atraso na execução dos serviços até o limite de 15 (quinze) dias;
f) multa moratória de 0,3% (três décimos por cento) sobre o valor anual do contrato, por dia de atraso na execução dos serviços, por período superior ao previsto na letra b, até o limite de 15 (quinze) dias.
g) Esgotado o prazo limite a que se refere a letra “c” poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução parcial ou total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
h) no caso de inexecução parcial, incidirá multa compensatória no percentual de 4% (quatro por cento) sobre o valor anual do contrato.
i) multa compensatória de 5% (cinco por cento) sobre o valor total do Contrato, no caso de inexecução total do Contrato;
j) multa rescisória de 4,6 % (quatro vírgula seis por cento) sobre o valor total do Contrato, no caso de rescisão contratual unilateral do Contrato;
k) Multa moratória de 0,5% sobre o valor total da contratação, por dia de atraso injustificado no início ou na conclusão dos testes ou por recusa de correção de todos os defeitos, falhas e quaisquer outras irregularidades causadas pelos testes, limitada sua aplicação até o máximo de 10 dias, situação que poderá caracterizar inexecução parcial do contrato

- Pela caracterização de inexecução parcial do objeto contratado, será aplicada multa de até 5% do valor global do contrato

l) Após o 20º dia de atraso, os serviços poderão, a critério do CONTRATANTE, não mais ser aceitos, configurando-se a inexecução total do Contrato, com as consequências previstas em lei e neste instrumento

- Pela caracterização de inexecução total do objeto contratado, será aplicada multa de até 5% do valor total do contrato

m) Todas as ocorrências contratuais serão registradas pelo CONTRANTE, que notificará a CONTRATADA dos registros. Serão atribuídos níveis para as ocorrências, conforme ofensividade, conforme tabelas abaixo:

INFRAÇÃO		
Item	**Descrição**	**Nível**
1	Transferir a outrem, no todo ou em parte, o objeto do contrato sem prévia e expresso acordo do CONTRATANTE.	6
2	Caucionar ou utilizar o contrato para quaisquer operações financeiras.	6
3	Reproduzir, divulgar ou utilizar, em benefício próprio ou de terceiros, quaisquer informações de que tenha tomado ciência em razão do cumprimento de suas obrigações sem o consentimento prévio e por escrito do CONTRATANTE	6

4	Utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos.	5
5	Deixar de relacionar-se com o CONTRATANTE, exclusivamente, por meio do fiscal do Contrato	3
6	Deixar de se sujeitar à fiscalização do CONTRATANTE, que inclui o atendimento às orientações do fiscal do contrato e a prestação dos esclarecimentos formulados.	4
7	Deixar de responsabilizar-se pelos produtos e materiais entregues, assim como deixar de substituir imediatamente qualquer material ou objeto que não atenda aos critérios especificados neste termo.	6
8	Deixar de responsabilizar-se pelos encargos trabalhistas, fiscais e comerciais, pelos seguros de acidente e quaisquer outros encargos resultantes da prestação do serviço.	6
9	Deixar de manter, durante todo o período de vigência contratual, todas as condições de habilitação e qualificação que permitiram sua contratação	6
10	Deixar de disponibilizar e manter atualizados conta de *e-mail,* endereço e telefones comerciais para fins de comunicação formal entre as partes.	2

11	Deixar de responsabilizar-se pela idoneidade e pelo comportamento de seus prestadores de serviço e por quaisquer prejuízos que sejam causados à CONTRATANTE e a terceiros.	6
12	Deixar de encaminhar documentos fiscais e todas documentações previstas no contrato, como relatórios, vídeos, dentre outras, para efeitos de atestar a entrega dos bens e comprovar regularizações.	6
13	Deixar de resguardar que seus funcionários cumpram as normas internas do CONTRATANTE e impedir que os que cometerem faltas a partir da classificação de natureza grave continuem na prestação dos serviços.	3
14	Deixar de relatar ao CONTRATANTE toda e quaisquer irregularidades ocorridas, que impeça, altere ou retarde a execução do Contrato, efetuando o registro da ocorrência com todos os dados e circunstâncias necessárias a seu esclarecimento.	5
15	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, a execução do objeto.	5
16	Recusar fornecimento determinado pela fiscalização sem motivo justificado.	3
17	Retirar das dependências do CONTRATANTE quaisquer equipamentos ou materiais de consumo sem autorização prévia.	6

18	Destruir ou danificar documentos por culpa ou dolo de seus agentes.	6
19	Recusa de correção de todos os defeitos, falhas e quaisquer outras irregularidades causadas pelos testes	6
20	Fraudar, manipular ou descaracterizar indicadores/metas de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	6
21	Deixar de entregar produtos resultantes dos serviços de uma OS dentro do prazo previsto , para cada produto e por dia de atraso.	1
22	Substituir empregado que se conduza de modo inconveniente ou não atenda as necessidades, por empregado e por dia.	1
23	Deixar de cumprir quaisquer dos itens do edital e de seus anexos não previstos nesta tabela de multas, por ocorrência.	1

Tabela 1: Infrações e correspondentes níveis

NÍVEL	CORRESPONDÊNCIA (percentual da multa, por ocorrência, sobre o valor global da contratação)
1 (menor ofensividade)	0,5%.
2 (leve)	0,8%.
3 (médio)	1,5%.
4 (grave)	4,0%.
5 (muito grave)	4,5%.
6 (gravíssimo)	5,0%.

Tabela 2: Classificação das infrações e multas

n) Em caso de registro de infração na qual a CONTRATADA apresente justificativa razoável e aceita pelo fiscal do contrato, o nível da infração poderá ser desconsiderado ou inserido em uma categoria de menor gravidade.

17.8.2 **A inexecução parcial ou total do contrato** será configurada, entre outras hipóteses, na ocorrência de, pelo menos, uma das seguintes situações:

NÍVEL	QUANTIDADE DE INFRAÇÕES	
	Inexecução Parcial	Inexecução Total
1	7 a 11	12
2	6 a 10	11 ou mais
3	5 a 9	10 ou mais
4	4 a 6	7 ou mais
5	3 a 4	5 ou mais
6	2	3 ou mais

Tabela 3: Qualificação da inexecução contratual

17.9 Da sanção de suspensão:

17.9.1 Cabe a sanção de suspensão do direito de participar de licitação e impedimento de contratar com o BANPARÁ em razão de ação ou omissão capaz de causar, ou que tenha causado, prejuízo ao BANPARÁ, suas instalações, pessoas, imagem, meio ambiente ou, ainda, em decorrência de determinação legal.

17.9.2 A aplicação da sanção de suspensão do direito de participar de licitação e impedimento de contratar com o BANPARÁ, por até 02 (dois) anos, será aplicada de acordo com os arts. 98 a 99 do RLC e registrada no SICAF e no Cadastro de Empresas Inidôneas - CEIS de que trata o artigo 23 da Lei n° 12.846, de 2013.

17.9.3 Em decorrência da prática por parte do licitante/adjudicatário das condutas elencadas nos artigos 98 e 99 do RLC, poderá ser aplicada a sanção de suspensão do direito de participar de licitação e impedimento de contratar com o BANPARÁ.

17.9.4 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

17.10 Do cometimento de falta grave:

17.10.1 Comete falta grave, podendo ensejar a rescisão unilateral da avença, sem prejuízo da aplicação da penalidade de multa e da suspensão do direito de participar de licitação e impedimento de contratar com o BANPARÁ por até 02 (dois) anos, nos termos do art. 98 do RLC, aquele que:

17.10.2 não promover o recolhimento das contribuições relativas ao FGTS e à Previdência Social exigíveis até o momento da apresentação da fatura, após o prazo de 05(cinco) dias úteis da notificação do BANPARÁ, podendo o prazo ser prorrogado mediante justificativa acatada pelo BANPARÁ;

18. Do Faturamento

18.1 O valor será faturado em 01 parcela um mês após entrega do relatório de conclusão.

19. Do Pagamento

19.1 O pagamento será efetuado à CONTRATADA mediante apresentação da nota fiscal com demonstrativo financeiro, via crédito em conta corrente a ser aberta pela empresa vencedora em uma das Agências do BANPARÁ, a qual deverá ser indicada na nota fiscal/fatura, conforme dispõe o Decreto do Estado do Pará nº 877/2008;

19.2 O pagamento será feito pela CONTRATANTE no mês subsequente da prestação do serviço, devendo a Nota Fiscal/Fatura ser apresentada a CONTRATANTE com antecedência mínima de 10 dias do vencimento, ficando este isento de responsabilidade por atrasos na apresentação das faturas por parte da CONTRATADA.

19.3 No preço apresentado pela CONTRATADA já estarão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscal e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguros de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do Banco por eventuais autuações.

19.4 Nenhum pagamento será efetivado enquanto estiver pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidades ou inadimplência contratual.

19.5 Havendo necessidade de realização de serviços por profissionais residentes ou não residentes em Belém-PA, as despesas com passagens aéreas, deslocamentos, estadias e refeições, serão arcadas pela CONTRATADA.

19.6 A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer cláusulas contratuais.

19.7 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário e órgão administrativos, atribuídos ao CONTRATANTE, oriundos de problemas na execução do contrato por parte da CONTRATADA serão repassados a esta e deduzidos do pagamento realizado pelo Banco, independente de comunicação ou interpelação judicial ou extrajudicial.

19.8 De acordo com a legislação tributária e fiscal em vigor será efetuada a retenção na fonte dos tributos e contribuições incidentes no objeto contratado.

19.9 É permitido ao BANPARÁ descontar dos créditos da CONTRATADA qualquer valor relativo à multa, ressarcimento a e indenizações, sempre observado o contraditório e ampla defesa.

19.10 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o judiciário e órgãos administrativos, atribuídos ao CONTRATANTE, oriundos de problemas na execução do contrato por ato da CONTRATADA, serão repassados a esta e deduzidos do pagamento realizado pelo Banco, independente de comunicação ou interpelação judicial ou extrajudicial.

19.11 A CONTRATADA deverá enviar a documentação de cobrança diretamente a área gestora do contrato SUROP/GESEI, junto com os documentos válidos informados no item abaixo, dentro do horário comercial.

19.12 Documentos:

a) Certidão Negativa de débito em dívida ativa
b) Certidão Negativa de débitos na Secretaria de Estado de Fazenda
c) Certidão Negativa de débito Trabalhista
d) Certificado de Regularidade do FGTS-CRF
e) Certidão Negativa Federal e Municipal

20. Fiscalização do Contrato

20.1 A gestão e fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste.

20.2 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.

20.3 A fiscalização da execução do contrato consiste na verificação do cumprimento das obrigações contratuais por parte do contratado, com a alocação dos recursos, pessoal qualificado, técnicas e materiais necessários.

20.4 Fiscalização Técnica

20.4.1 A Fiscalização Técnica do fornecimento do objeto será exercida pelo Gerente ou um funcionário da SUCEX – Superintendência de Câmbio e Comércio Exterior em conjunto com o Gerente ou um funcionário da SUROP – Superintendência de Risco Operacional, a serem nomeados pelo BANPARA;

20.4.2 Ao BANPARA reserva-se o direito de rejeitar, no todo ou em partes os itens fornecidos em desacordo com o estabelecido;

20.4.3 A fiscalização exercida pelo BANPARA não excluirá ou reduzirá a responsabilidade da CONTRATADA pela completa e perfeita execução dos itens deste Termo de Referência.

20.5 Fiscalização Administrativa

20.5.1 A fiscalização administrativa deve avaliar o cumprimento de obrigações do contratado relacionadas a aspectos de gestão, especialmente nos contratos de terceirização e tocante aos empregados que põe à disposição do BANPARÁ, de modo a exigir o cumprimento das obrigações trabalhistas e sociais, com a apresentação dos documentos previstos nos contratos e que sejam pertinentes, nos termos da legislação e deste Regulamento, devendo determinar a correção de falhas ou faltas por parte do contratado, bem como informar ao gestor do contrato sobre providências que importem disposição sobre o contrato, com as respectivas justificativas.

20.5.2 A Fiscalização Administrativa do fornecimento do objeto será exercida Pela Gerencia ou por um funcionário da SUCEX – Superintendência de Câmbio e Comércio Exterior, a ser nomeado pelo BANPARA;

20.6 A fiscalização da execução do contrato abrange as seguintes rotinas:

20.6.1 **Fiscalização Técnica:**

a) acompanhar e fiscalizar a execução de todas as atividades decorrentes do serviço contratado a fim de atender as condições definidas neste termo;
b) intermediar a comunicação e interação entre o BANPARA e a CONTRATADA;
c) convocar reuniões, quando necessárias;
d) manter registro de todas as atas de reuniões, ocorrências, relatórios e documentação referentes ao serviço;
e) efetuar a abertura de chamados técnicos para a correção de problemas ou dúvidas;
f) sugerir a aplicação de sanções administrativas;
g) enviar a nota fiscal, com anuência da área gestora, para pagamento respeitando os prazos deste termo;
h) promover as ações necessárias a fim de garantir a continuidade dos serviços;

20.6.2 **Fiscalização Administrativa:**

a) Acompanhar administrativamente a execução do contrato, supervisionando sua execução orçamentária;

b) Emitir as certidões de regularidade fiscal e trabalhista do fornecedor, antes do envio da fatura para pagamento;
c) Atestar que a documentação de cobrança apresentada se encontra na forma estabelecida no contrato, conferindo a nota fiscal do serviço emitida quanto às obrigações previdenciárias, fiscais, trabalhistas e FGTS;
d) Efetuar a instrução processual para fins de pagamento, na forma convencionada no instrumento contratual;
e) Fiscalizar, por amostragem, os registros dos empregados da contratada locados nos serviços, para verificar a regularidade trabalhista;
f) Oficiar a contratada sobre a necessidade de atualização documental para manutenção das condições de habilitação ou atendimento de exigências legais supervenientes;
g) Prestar orientações técnicas à unidade demandante e à Contratada, relativas à observância das condições pactuadas, no que diz respeito aos prazos de execução, faturamento e pagamento e outros esclarecimentos que venham a ser solicitados;
h) Recusar, com a devida justificativa, qualquer documento ou Nota Fiscal encaminhados pelo fiscal do contrato que se encontre em desacordo com as condições estabelecidas no contrato;
i) Realizar toda e qualquer ação pertinente à alteração contratual.

ADENDO I

PLANILHA DE PREÇOS

ITEM	**DESCRIÇÃO**	**VALOR TOTAL**
1	Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISSO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework, conforme descritas nos termos do Edital, Termo de Referência e seus anexos	

ADENDO II

MODELO PARA PROPOSTA

CARTA DE APRESENTAÇÃO DE PROPOSTA

Ao BANCO DO ESTADO DO PARÁ S.A.
Av. Presidente Vargas, nº 251, Ed. BANPARÁ – 1º andar
Comércio, Belém/PA, CEP 66.010-000

Ref: Edital de Licitação nº ...../.....
Objeto:.....

Prezados senhores,

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

1. Propõe-se o Valor Total de R$ .....(.....), conforme quadro abaixo:

ITEM	**DESCRIÇÃO**	**VALOR TOTAL**
1	Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISSO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework, conforme descritas nos termos do Edital, Termo de Referência e seus anexos	

2. No valor total proposto estão englobados todos os custos e despesas previstos no edital nº ...../....., tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucros e outros necessários ao cumprimento integral do objeto.

3. Junta-se detalhamento da proposta acima.

4. Que, em relação às prerrogativas da Lei Complementar nº 123/2016, o proponente:

( ) Enquadra-se como microempresa, empresa de pequeno porte ou equivalente legal, nos termos previsto no Decreto nº 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 (doze) meses.

( ) Não é optante do Simples Nacional.

5. Essa proposta é válida por 120 (cento e vinte) dias, contados da data prevista para abertura da sessão.

6. Até que o contrato seja assinado ou recebida a Nota de Empenho conforme o caso, esta proposta constituirá um compromisso da ....., observadas as condições do edital. Caso esta proposta não venha a ser aceita para contratação, o BANPARÁ fica desobrigado de qualquer responsabilidade referente a presente proposta.

6. Os pagamentos serão efetuados em conformidade com as condições estabelecidas no Termo de Referência e Nota de Empenho.

7. "**ATENÇÃO: Caso não sejam informadas abaixo a agência e a respectiva conta aberta no Banco do Estado do Pará S.A., em cumprimento ao art. 2º do Decreto Estadual n.º 877/2008 de 31/03/2008, o licitante deverá apresentar a seguinte declaração:**

"COMPROMETEMO-NOS A REALIZAR A REFERIDA ABERTURA DA CONTA NO PRAZO MÁXIMO DE ATÉ 05 (CINCO) DIAS CONSECUTIVOS CONTADOS DA ASSINATURA DO CONTRATO."

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

BANCO: 037 .....
AGÊNCIA: .....
CONTA CORRENTE: .....
PRAÇA DE PAGAMENTO: .....

9. Por fim, declara conhecer e aceitar as condições constantes do edital nº ...../..... e de seus anexos.

.....
(Local e Data)

.....
(Representante legal)

ADENDO III

ATESTADO DE CAPACIDADE TÉCNICA

(Modelo)

Atestamos para os devidos fins que a empresa **[Razão Social da Empresa licitante]**, inscrita no CNPJ sob o Nº. **[da Empresa Licitante]**, estabelecida na **[endereço da Empresa Licitante]**, prestou ou presta serviços para esta empresa/Entidade **[Razão Social da Empresa Emitente do atestado]**, inscrita no CNPJ sob o Nº. **[CNPJ da Empresa Emitente do atestado]**, situada no **[endereço da Empresa Emitente do atestado]**, conforme descriminado abaixo:, no período de (__/__/__ a __/__/__):

1 SERVIÇO PRESTADO:

2 **VALOR GLOBAL** (R$):.....

Declaramos ainda que os compromissos assumidos foram executados satisfatoriamente, não constando em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

_____
Local e Data

_____
[Nome do Representante da Empresa Emitente]
Cargo / Telefone/Email/ Contatos:

OBSERVAÇÃO: EMITIR EM PAPEL TIMBRADO DA EMPRESA/ ENTIDADE OU IDENTIFICÁ-LA LOGO ABAIXO OU ACIMA DO TEXTO, COM NOME, CNPJ, ENDEREÇO, TELEFONES, FAX E E-MAIL.

ADENDO IV
ACORDO DE CONFIDENCIALIDADE DA INFORMAÇÃO E RESPONSABILIDADE

O Banco do Estado do Pará, com sede na Av. Presidente Vargas, nº 251, Bairro Campina, Belém/PA, inscrito no CNPJ/MF sob o nº 04.911.713/0001-08, doravante denominado CONTRATANTE, neste ato representado por seu Diretor Presidente, XXXXXXXX, CPF nº <**CPF**>, residente e domiciliado nesta Capital, no uso das atribuições que lhe são conferidas e <**EMPRESA CONTRATADA**>, inscrita no CNPJ/MF nº <**CNPJ**>, com endereço na <**endereço completo**>, doravante denominada CONTRATADA, neste ato representada por seu sócio <**ou diretor ou procurador**>, Sr. <**nome do representante**>, <**nacionalidade**>, CPF nº <**CPF**>, residente e domiciliado na <**localidade de domicílio**>, firmam o presente ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÃO E RESPONSABILIDADE, decorrente da realização do Contrato nº <**número do contrato**>, que entra em vigor neste dia ____ de _____ de 20__ e é regido mediante as cláusulas e condições seguintes:

1. DA INFORMAÇÃO CONFIDENCIAL

Para fins do presente Acordo, são consideradas INFORMAÇÕES SIGILOSAS, os documentos e informações transmitidos pela CONTRATANTE e recebidos pela CONTRATADA através de seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes. Tais documentos e informações não se limitam, mas poderão constar de dados digitais, desenhos, relatórios, estudos, materiais, produtos, tecnologia, programas de computador, especificações, manuais, planos de negócio, informações financeiras, e outras informações submetidas oralmente, por escrito ou qualquer outro tipo de mídia. Adicionalmente, a expressão INFORMAÇÕES SIGILOSAS inclui toda informação que CONTRATADA possa obter através da simples visita às instalações da CONTRATANTE.

2. DOS LIMITES DA CONFIDENCIALIDADE DAS INFORMAÇÕES

Para fins do presente Acordo, não serão consideradas INFORMAÇÕES SIGILOSAS as que:

2.1 São ou tornaram-se públicas sem ter havido a violação deste Acordo pela CONTRATADA;

2.2 Eram conhecidas pela CONTRATADA, comprovadas por registros escritos em posse da mesma, antes do recebimento delas pela CONTRATANTE;

2.3 Foram desenvolvidas pela CONTRATADA sem o uso de quaisquer INFORMAÇÕES SIGILOSAS;

2.4 Venham a ser reveladas pela CONTRATADA quando obrigada por qualquer entidade governamental jurisdicionalmente competente;

2.4.1 Tão logo inquirida a revelar as informações, a CONTRATADA deverá informar imediatamente, por escrito, à CONTRATANTE, para que este requera medida cautelar ou outro recurso legal apropriado;

2.4.2 A CONTRATADA deverá revelar tão somente as informações que forem legalmente exigidas;

3. DAS OBRIGAÇÕES DA CONTRATADA

Consiste nas obrigações da CONTRATADA:

3.1 Garantir que as Informações Confidenciais serão utilizadas apenas para os propósitos do contrato nº <**número do contrato**>, e que serão divulgadas apenas para seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes, respeitando o princípio do privilégio mínimo com devida classificação de informação conforme ABNT NBR ISO IEC 27002:2005;

3.2 Não divulgar, publicar, ou de qualquer forma revelar qualquer INFORMAÇÃO SIGILOSA recebida através da CONTRATANTE para qualquer pessoa física ou jurídica, de direito público ou privado, sem prévia autorização escrita da CONTRATANTE;

3.3 Garantir que qualquer INFORMAÇÃO SIGILOSA fornecida por meio tangível não deve ser duplicada pela CONTRATADA exceto para os propósitos descritos neste acordo;

3.4 A pedido da CONTRATANTE, retornar a ele todas as INFORMAÇÕES SIGILOSAS recebidas de forma escrita ou tangível, incluindo cópias, reproduções ou outra mídia contendo tais informações, dentro de um período máximo de 10 (dez) dias após o pedido;

3.4.1 Como opção para CONTRATADA, em comum acordo com a CONTRATANTE, quaisquer documentos ou outras mídias possuídas pela CONTRATADA contendo INFORMAÇÕES SIGILOSAS podem ser destruídas por ela;

3.4.1.1 A destruição de documentos em papel deverá seguir recomendação da norma DIN 32757-1: **4**, ou seja, destruição do papel em partículas de, no mínimo, 2 x 15mm;

3.4.1.2 A destruição de documentos em formato digital deverá seguir a norma DoD 5220.22-M (ECE) ou o método descrito por Peter Gutmman no artigo “Secure Deletion of Data From Magnetic and Solid-State Memory” ou através da utilização de desmagnetizadores (degausser);

3.4.1.3 A destruição das INFORMAÇÕES SIGILOSAS que não estiverem nos formatos descritos nos itens 3.4.1.1 e 3.4.1.2 deverá ser previamente acordada entre a CONTRATANTE e a CONTRATADA;

3.4.1.4 A CONTRATADA deverá fornecer à CONTRATANTE certificado com respeito à destruição, confirmando quais as informações que foram destruídas e os métodos utilizados, dentro de um prazo máximo de 10 (dez) dias;

3.5 A CONTRATADA deverá dar ciência deste acordo a todos seus sócios, empregados, prestadores de serviço, prepostos ou quaisquer representantes que participarão da execução dos serviços objetos do contrato vierem a ter acesso a quaisquer dados e informações confidenciais cumpram as obrigações constantes deste Acordo e que será responsável solidariamente por eventuais descumprimentos das cláusulas aqui descritas;

4. DA PROPRIEDADE DAS INFORMAÇÕES SIGILOSAS

4.1 A CONTRATADA concorda que todas as INFORMAÇÕES SIGILOSAS permanecem como propriedade da CONTRATANTE e que este pode utilizá-las para qualquer propósito sem nenhuma obrigação com ela;

4.2 A CONTRATADA concorda ter ciência de que este acordo ou qualquer INFORMAÇÕES SIGILOSAS entregues pela CONTRATANTE a ela, não poderá ser interpretado como concessão a qualquer direito ou licença relativa à propriedade intelectual (marcas, patentes, copyrights e segredos profissionais) à CONTRATADA;
4.3 A CONTRATADA concorda que todos os resultados dos trabalhos prestados por ela à CONTRATANTE, inclusive os decorrentes de especificações técnicas, desenhos, criações ou aspectos particulares dos serviços prestados, são reconhecidos, irrestritamente, neste ato, como de exclusiva propriedade do CONTRATANTE, não podendo a CONTRATADA reivindicar qualquer direito inerente à propriedade intelectual;
4.4. Utilizar os bens de informação disponibilizados por força de contrato celebrado com o BANPARÁ exclusivamente para fins da adequada prestação dos serviços contratados, estritamente em observância aos interesses do BANPARÁ.
4.5. Respeitar a propriedade do BANPARÁ ou de terceiros, sobre os bens de informação disponibilizados, zelando pela integridade dos mesmos, não os corrompendo ou os divulgando a pessoas não autorizadas;
4.6. Manter, a qualquer tempo e sob as penas de lei, total e absoluto sigilo sobre os bens de informação do BANPARÁ, utilizando-os exclusivamente para os fins de interesse deste, estritamente no desempenho das atividades inerentes a prestação dos serviços contratados, não os revelando ou divulgando a terceiros, em hipótese alguma, sem o prévio e expresso consentimento do BANPARÁ;
4.7. Instalar e utilizar nos ambientes computacionais disponibilizados pelo BANPARÁ somente softwares desenvolvidos ou adquiridos pelo BANPARÁ;
4.8. Permitir ao BANPARÁ a fiscalização, a qualquer tempo, de todos os dados manejados através dos meios fornecidos pelo BANPARÁ em razão da prestação de serviços contratados, pelo que autorizo o BANPARÁ a monitorar todos os dados manejados nos meios de propriedade do contratante, não configurando o referido monitoramento qualquer quebra de sigilo ou invasão de privacidade.
4.9. Não utilizar o ambiente de internet disponibilizado pelo BANPARÁ para uso pessoal, ilícito, ilegal, imoral ou para quaisquer outros fins senão os de estrita prestação dos serviços contratados.

5. DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO DA CONTRATANTE

5.1 A CONTRATADA declara que recebeu cópia e está ciente da Política de Segurança da Informação da CONTRATANTE, definida pelo Conselho de Administração em Reunião Ordinária realizada em 13 de julho de 2016, e de todos os seus documentos acessórios já criados;
5.2 A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de segurança da informação definidos e/ou seguidos pela CONTRATANTE;
5.3. A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de continuidade definidos e/ou seguidos pela CONTRATANTE;
5.4. Seguir os Manuais de Normas e Procedimentos da área de Gestão de Riscos Operacionais, Manual de Boas Práticas de Segurança da Informação

6. DO PRAZO DE VALIDADE DO ACORDO

As obrigações tratadas neste acordo subsistirão permanentemente, mesmo após a conclusão dos serviços ou até que a CONTRATANTE comunique expressa e inequivocadamente, por escrito, à CONTRATADA, que as informações já não são mais sigilosas.

7. DAS PENALIDADES

Qualquer divulgação de dados, materiais, desenhos ou informações, obtidos em razão dos serviços por CONTRATADA, ou prepostos e seus funcionários, sem a respectiva autorização prévia, expressa e escrita da CONTRATANTE, implicará na obrigatoriedade de CONTRATADA ressarcir as perdas e danos experimentados pela CONTRATANTE, sem prejuízo das penalidades civis e criminais previstas em lei.

8. DO FORO

Fica eleito o foro da Justiça Estadual, Seção Judiciária de Belém, na cidade do Belém, para dirimir dúvidas decorrentes do presente Acordo.
E, por estarem assim justas e contratadas, firmam o presente instrumento, em 3 (três) vias de igual teor e forma, para que se produzam os necessários efeitos legais.

Belém, de de 20

_____

XXXXXXXXXXXXXXX
Diretor Presidente
Banco do Estado do Pará SA
CONTRATANTE

_____

XXXXXXXXXXXXXXX
Representante
CONTRATADA

ADENDO V
POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética do Banpará tem os seguintes objetivos:

1.1. Proteger o valor e a reputação da empresa;

1.2. Proteger as informações do Banpará, bem como as de clientes e de terceiros por ele custodiadas, garantindo a confidencialidade, integridade e disponibilidade;

1.3. Identificar violações de segurança cibernética, estabelecendo ações sistemáticas de prevenção, detecção e resposta a incidentes;

1.4. Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos relacionados ao risco cibernético;

1.5. Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;

1.6. Estabelecer e melhorar continuamente o processo de Gestão de Riscos de Segurança Cibernética;

RESPONSABILIDADES

O cumprimento da Política Corporativa de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às diretrizes nela elencadas.

ADENDO VI

MODELO DO TERMO DE ACEITE PARA PAGAMENTO

CONTRATADA:

CONTRATO:

OBJETO:

ATESTAMOS, para os devidos fins, que a empresa <nome da empresa> , procedeu com <apontar o serviço executado>, discriminados na Nota Fiscal/Fatura n.º <numero da nota fiscal> , emitida em __ / __ / 20____, referente a OS Nº <inserir o numero da OS> , não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

Belém, ____ de _____ de 20__.

NOME DO GERENTE / GESTOR
Cargo e nome da área – SIGLA

NOME DO RESP. PELA EMISSÃO
Cargo e nome da área – SIGLA

ADENDO VII
MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO – Nº

PRESTAÇÃO DE SERVIÇOS DE CONSULTORIA EM SEGURANÇA CIBERNÉTICA SWIF

CONTRATO Nº

A presente ordem de serviço é celebrada em conformidade com o procedimento para PRESTAÇÃO DE SERVIÇOS DE CONSULTORIA EM SEGURANÇA CIBERNÉTICA SWIF, previstos no Contrato Nº....., firmado entre o Banco do Estado do Pará SA - BANPARÁ e a CONTRATADA, em vigor desde ___ de _____ de _____, sendo incorporada ao mesmo por referência.

Quantidade de Horas	Período de Atividade da OS		Valor Total
	Início	Fim	
		TOTAL GERAL	

Descrição das atividades:

1) Planejamento

2) Descoberta;

3) Ataque (exploração);

4) Relatório Teste de Invasão;

5) Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste

6) Reavaliação, novo teste pós-remediação

7) Relatório final do teste de invasão

Para efeito do cumprimento desta ORDEM DE SERVIÇO a CONTRATANTE e CONTRATADA indicam os seguintes responsáveis:

CONTATOS DA CONTRATANTE		
Nome:		
Gerencia:	Unidade:	Matrícula:

Telefones de Contato:		

CONTATOS DA CONTRATADA		
Nome:		
Gerencia:	Unidade:	Matrícula:
Telefones de Contato:		

Belém, _____ de _____ de 20__

CONTRATANTE CONTRATADA

ADENDO VIII

RECOMENDAÇÕES E PADRÕES DE SEGURANÇA TECNOLÓGICA MÍNIMA

A CONTRATADA deve apresentar, sempre que solicitado pela BANPARÁ, evidências de que o ambiente de realização dos serviços contratados possui o grau de segurança necessário para garantir o sigilo das informações a ela confiadas.
Os produtos gerados pela CONTRATADA deverão respeitar todos os padrões de segurança estabelecidos pela BANPARÁ.
A CONTRATADA deverá prover todos os equipamentos de rede necessários à prestação dos serviços, a serem instalados nas suas dependências, conforme abaixo:

1. ROTEADORES:

a) Utilização de filtros nos roteadores de borda.

2. FIREWALL:

a) Solução de firewall em todas as regiões de fronteira das redes de comunicação TCP/IP relacionadas às aplicações onde sejam implementados pontos de conexão externa da CONTRATADA (Internet e Extranet); nestes pontos são executadas interfaces de comunicação, transmissão e transferência de dados;
b) Evidência de disponibilidade dos firewalls de 99,99% mensurados e demonstrados mensalmente;
c) Distribuição de carga, em casos de falha de um dos componentes da solução de firewall, de forma a estabilizar no máximo de 80% (oitenta por cento) da carga máxima possível entre os componentes remanescentes;
d) Disponibilizar equipamento dedicado de firewall para provimento de controle de acesso aos serviços fornecidos pela CONTRATADA através dos servidores.
e) Deve haver soluções de *firewall* em todas as regiões de fronteira das redes de comunicação TCP/IP relacionadas aos serviços fornecidos pela CONTRATADA.

- Nestes pontos são executadas interfaces de comunicação, transmissão e transferência de dados, em conformidade com a norma NBR ISO/IEC 27002:2007, item 11.4.5.
- A BANPARÁ deverá ter acesso *on-line* às ferramentas de *firewall* utilizadas na solução, restrito à operação de leitura, através de suas consoles a qualquer momento, para fins de auditoria.
  - As soluções de *firewall* a serem implementadas devem prover, no mínimo:

- Bloqueio de acesso por portas;
- Bloqueio de acesso por IPs;
- Controle *Stateful* de fluxo;
- Registro de acessos negados;
- Controle de aplicações complexas (FTP e aplicações multiporta), caracterizada por aquelas aplicações que utilizam fluxos não comuns e tráfego de redes, como o uso de protocolos com várias portas no lado servidor e múltiplos protocolos de transporte.
- Controle *antispoofing*;
- Resistência a ataques de DDOS;
- Resistência a ARP *Poisoning*;
- Resistência a SYN *Flooding;*
- Resistência a SMURF *Attack*;
- Controle de fluxo UDP *Stateful;*
- Controle de fluxo ICMP;
- Suporte a implementação de NAT.

f) Relativo à configuração dos firewall deverá ser observado:
- Princípio restritivo, em que todo o tráfego é bloqueado, à exceção daquele expressamente configurado como permitido;
- Manter documentação formal de todas as configurações relacionadas aos recursos e regras das soluções de firewall;
- Geração de “log” administrativos do próprio produto e também do tráfego por ele inspecionado;
- Equipamento de serviço de firewall deverá ter somente a configuração mínima necessária, sendo desabilitados os recursos adicionais do sistema operacional que não sejam estritamente necessários o seu funcionamento.

g) Os sistemas de *firewall* devem necessariamente se basear no princípio restritivo, em que todo o tráfego é bloqueado, à exceção daquele expressamente configurado como permitido.

h) Todas as configurações de regras e recursos de todas as soluções de *firewall* devem ser informadas ao corpo técnico do BANPARÁ.

i) Tais especificações devem ser entregues ao BANPARÁ dentro de um prazo máximo de 30 (trinta) dias a contar da assinatura do contrato.

j) Caso exista alguma discordância por parte do corpo técnico da BANPARÁ as adequações deverão estar corrigidas nos documentos e implementadas num prazo inferior a 30 (trinta) dias.

k) Todas as configurações relacionadas aos recursos e regras das soluções de *firewall* devem ser rigorosa e formalmente documentadas, atualizadas e repassadas ao BANPARÁ.

l) O período de tempo para aplicação das regras e alterações não suspenderá a contagem de tempo de indisponibilidade.

m)A solução de f*irewall* deverá gerar *logs* administrativos do próprio produto e também do tráfego por ele inspecionado, que devem ser fornecidos ao corpo técnico do BANPARÁ quando por ele solicitado.

n) O sistema operacional deverá utilizar configuração mínima necessária ao funcionamento do serviço de *firewall*.

o) A BANPARÁ poderá, a qualquer momento, auditar a configuração da solução de *firewall*.

3. IDS – Sistemas de Detecção de Intrusão:

a) Soluções de IDS – Sistema de Detecção de Intrusão em todas as regiões de fronteira das redes de comunicação TCP/IP relacionadas às aplicações onde sejam implementados pontos de conexão externa da CONTRATADA.
Nestes pontos são executadas interfaces de comunicação, transmissão e transferência de dados;
b) Devem ter funcionalidades que permitam a criação automática de regras de defesa, quando sob ataque, no dispositivo responsável pela autorização de tráfego;
c) Integração automática com a solução de firewall em níveis de bloqueio, proteção, alertas e geração de log;
d) Demonstrar a disponibilidade de funcionamento à taxa de 99,99% mensurada mensalmente.
e) A solução deve contemplar sensores de rede e de servidores, para os servidores envolvidos na infra-estrutura da CONTRATADA.

f) Um gráfico descrevendo a topologia dos pontos de aplicação dos sensores deve ser especificado e entregue ao BANPARÁ num período máximo de 30 (trinta) dias a contar da assinatura do contrato.
g) Entenda-se como topologia um desenho ou imagem descritiva, na qual estejam representadas as disposições das redes e seus respectivos ativos envolvidos, bem como os sensores de IDS.
h) O BANPARÁ deve ter acesso on line à configuração destes equipamentos através de sua console a qualquer momento.
i) Este acesso deverá ser seguro (autenticidade, integridade e confidencialidade dos dados) e restrito à operação de leitura.
j) A solução de IDS deve prover, no mínimo:
a. Detecção de ataques ou comportamentos anômalos baseado em "assinaturas" e/ou comportamental;
b. Permitir reset de conexão para ataques selecionados;
c. Envio de alarmes para console de gerenciamento própria com níveis de severidade de acordo com o tipo do ataque;
d. Permitir análise de segmentos de rede no modo "promíscuo";
e. Alarme por presença de strings e/ou assinaturas customizadas;
f. Criptografia dos dados entre a console administrativa e o dispositivo coletor de dados.
k) Garantia de disponibilidade de funcionamento à taxa de 99,9% medida e relatada mensalmente.

Quando da ocorrência de atividades suspeitas, sem falso positivo, todas as configurações relacionadas à análise de tráfego, verificações realizadas, ocorrências de atividades suspeitas, registros em log, respostas e contramedidas das soluções de IDS devem ser rigorosa e formalmente documentadas, atualizadas e repassadas ao BANPARÁ.

4. ANTIVÍRUS:

a) A CONTRATADA deverá garantir que todo dado transmitido à BANPARÁ esteja livre de vírus de computador;

b) Recursos de antivírus para proteção das informações administradas, no mínimo, capaz de;

- Detectar e remover vírus, Cavalos de Tróia, *worms* e ameaças correlatas, para a solução a ser utilizada no ambiente da CONTRATADA;

c) Fornecer proteção contra vírus em tempo real para correio eletrônico SMTP e tráfego FTP e HTTP.
d) A solução de antivírus a ser utilizada no ambiente da CONTRATADA deve ser capaz de detectar e remover vírus, cavalos de tróia, *worms* e ameaças correlatas, em conformidade com a norma NBR ISO/IEC 27002:2007 item 10.4.
e) As atualizações das vacinas ou versões dos programas de antivírus devem ocorrer automaticamente para todos os servidores e estações da solução a ser contratada sempre que disponibilizadas pelo fabricante.
f) Os documentos dessa política devem ser entregues ao BANPARÁ dentro de um prazo máximo de 30 (trinta) dias a contar da assinatura do contrato.
g) Caso exista alguma discordância por parte do corpo técnico do BANPARÁ as adequações deverão estar corrigidas nos documentos e implementadas num prazo inferior a 30 (trinta) dias.
h) O tratamento das mensagens de correio efetuado pela solução de antivírus deve:

- fornecer proteção contra vírus em tempo real para correio eletrônico SMTP;
- detectar vírus e bloquear códigos *Java e ActiveX* maliciosos;
- rastrear, detectar e remover vírus de arquivos compactados com os algoritmos de compactação padrões de mercado, cujas extensões de arquivos são zip, lha, cab, gz, tar, jar, arc, arj, lzh, rar, dentre outras;
- implementar filtro de *spam*, de forma a bloquear mensagens indesejadas de correio eletrônico;

Ter como opção limpar os arquivos infectados antes de enviá-los aos destinatários sem a interrupção da entrega da mensagem.

5. POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÕES

A CONTRATADA deve definir e implementar política para classificação de documentos em quaisquer mídias que venham a ser utilizadas para armazenamento e transporte de dados pertinentes ao processo a ser contratado e sistemas computacionais a ela correlacionados, em conformidade com a norma NBR ISO/IEC 27002:2007, item 7.2.
A política deve considerar que os dados pertinentes ao processo a ser contratado e sistemas computacionais a ele correlacionados serão classificados como confidenciais, isto é, de acesso restrito à CONTRATADA no exercício de suas funções.
Os documentos dessas políticas devem ser entregues ao BANPARÁ dentro de um prazo máximo de 30 (trinta) dias a contar da assinatura do contrato.
Caso exista alguma discordância por parte do corpo técnico do BANPARÁ as adequações deverão estar corrigidas nos documentos e implementadas num prazo inferior a 30 (trinta) dias.

6. SEGURANÇA FÍSICA E LÓGICA

O acesso físico e lógico ao ambiente controlado da BANPARÁ somente será disponibilizado aos funcionários da CONTRATADA mediante o cumprimento das condições de segurança estabelecidas neste Termo de Referência e no Contrato.
Como padrão de segurança será adotada criptografia para as senhas pessoais dos usuários e para o tráfego de dados em rede, para Extranet ou Internet.
O Gestor do CONTRATO irá especificar quais dados serão armazenados no Banco de Dados e nos backups de forma criptografada.
Os dados que trafegarem pela Extranet ou Internet deverão ser criptografados podendo utilizar em sua última versão e com chave de 128 bits, um dos padrões a seguir:
a) S.S.L. - *Secure Sockets Layer*;
b) T.L.S - *Transport Layer Security.*
A CONTRATADA deverá possuir, em suas instalações, padrões mínimos necessários de segurança, objetivando garantir a segurança contra ataques externos e tentativas de invasão.
Os empregados da CONTRATADA podem ter acesso ao ambiente do BANPARÁ, exceto partições de homologação/produção e de suporte técnico, respeitados os padrões de Controle de Acesso Lógico a Sistemas Computacionais.
O acesso às bases de dados internas dos clientes do BANPARÁ, e/ou eventual armazenamento destes dados por parte da CONTRATADA dar-se-á conforme os padrões do BANPARÁ.
A CONTRATADA e seus empregados bem como a eventual subcontratada e seus empregados devem manter, sob as penas da lei, o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais dos materiais do BANPARÁ, de que venham a tomar conhecimento ou ter acesso, ou que venham a ser ele confiados, sejam relacionados ou não com o fornecimento objeto do contrato.

7. POLÍTICA DE ACESSO LÓGICO

Os documentos que constituem a política de acesso lógico a ser utilizada em todas as instâncias da infra-estrutura de rede e dos sistemas computacionais da CONTRATADA, correlatos ao processo a ser contratado, devem ser entregues ao BANPARÁ dentro de um prazo máximo de 30 (trinta) dias a contar da assinatura do contrato.
Essa política deve estar em conformidade com a norma NBR ISO/IEC 27002:2007, itens 11.1, 11.2, 11.3 e 11.4.
Caso exista alguma discordância por parte do corpo técnico do BANPARÁ as adequações deverão estar corrigidas nos documentos e implementadas num prazo inferior a 10 (dez) dias.

8. ARQUITETURA DA SISTEMA - PLATAFORMA

Deverá utilizar o conceito das três camadas no desenvolvimento da Solução: aplicação, dados e apresentação.
Deverá possuir mecanismos automáticos e manuais de manutenção das bases de dados (exemplo: reorganização de base, reindexação de tabelas), sendo todas as ações registradas em *log*.
Deverá seguir o padrão J2EE, MVC2 e W3C para a camada de apresentação *web*_.
Deverá ser desenvolvida como sendo uma coleção de módulos funcionais, onde cada módulo deverá corresponder a uma unidade de execução de uma seqüência de

tarefas que compreende um determinado serviço bem delineado como, por exemplo, autorização, fraude, cobrança, fatura.

9. SEGURANÇA - ADMINISTRAÇÃO E OPERAÇÃO

Deverá suportar a segregação das funções de administração de sistemas e a administração de segurança para propiciar separação de responsabilidades no sistema.
Deverá realizar validação de entrada de dados na camada *Web* a fim de evitar ataques como SQL *Injection, Cross Site Scripting* e *Cookie Poisoing.*

10. SEGURANÇA - GERENCIAMENTO DE SESSÃO

Deverá possuir mecanismo com capacidade de forçar revogação e bloqueio imediato de um usuário e/ou da sessão de um usuário quando requisitado pelo administrador.

11. ATENDIMENTO A RESOLUÇÃO 4658/2018 DO BANCO CENTRAL

O contrato desse serviço deve atender a resolução n. 4658/2018 a qual informa que o terceiro precisa:

11.1. Segundo art. 12 assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;
b) o acesso da CONTRATANTE aos dados e às informações a serem processados ou armazenados pelo prestador de serviço (CONTRATADA);
c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço (CONTRATADA);
d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
e) o acesso da CONTRATANTE aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço (CONTRATADA), relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
f) A CONTRATADA deve fornecer o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
g) a identificação e a segregação dos dados dos clientes da CONTRATANTE por meio de controles físicos ou lógicos; e
h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da CONTRATANTE.

11.1.1. Segundo art. 17 precisa prever:

a) Adoção de medidas de segurança para transmissão e armazenamento dos dados conforme normativos de segurança da CONTRATANTE
b) Manutenção da segregação dos dados para controle de acesso para proteção das informações dos clientes da CONTRATANTE.
c) Garantir que exista procedimentos de continuidade dos serviços que estão em nuvem.

ADENDO IX

NORMA DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS

1 NORMAS DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS

1.1 – OBJETIVOS

Y. Controlar e identificar os dados para legados antigos, analisando a aderência destes quanto aos requisitos de segurança e necessidade de integração ao SGA, sendo que todos devem ser integrados ao sistema de RH.

Z. Autenticar somente as pessoas que podem utilizar os sistemas corporativos da instituição;

AA. Garantir a utilização de informações sensíveis e confidenciais, somente por pessoas autorizadas, de acordo com o seu perfil funcional;

BB. Registrar as ações realizadas por todos os usuários nos sistemas corporativos.

1.2 - JUSTIFICATIVA

As normas de segurança NBR ISO / IEC 27001 e 27002 recomendam como requisitos de segurança da informação a criação de: Controles de Acesso e Auditoria de Logs nos sistemas corporativos. A cada usuário é permitido visualizar e executar somente as transações autorizadas a determinados sistemas de acordo com o seu perfil funcional, mitigando assim as vulnerabilidades existentes nos sistemas corporativos da instituição. Além disso, é necessária a fiscalização das ações executadas por estes usuários, de modo claro e preciso, através da existência de logs de auditoria nos sistemas monitorados. Deve-se também levar em consideração a viabilidade de disponibilidade do SGA e do serviço deste para os sistemas clientes, que são os sistemas integrados ao mesmo. Assim, a severidade de eventos que possam comprometer a disponibilidade, a confidencialidade, a autenticidade, o não-repúdio e a integridade das informações torna-se mínima para o sistema que gere vários outros sistemas, incluindo acessos externos ao Banpará

1.3 – NORMAS GERAIS

Com base nas recomendações de normas de segurança NBR ISO / IEC 27001 e 27002, visando à Segurança da Informação quanto aos requisitos necessários de segurança dos sistemas corporativos estes serão categorizados em “Críticos” e “Não críticos”.

São considerados sistemas “**críticos**” todo e qualquer sistema que apresente pelo ao menos uma das características a seguir:

- Realiza movimentação financeira em contas de clientes (PF/PJ/Governo/Prefeitura);
- Realiza movimentação financeira em contas da instituição financeira (Banpará);
- Realiza movimentação de dados de clientes (PF/PJ/Governo/Prefeitura);
- Sistemas com acesso externo ou integrado a um sistema externo;
- Possui integração com órgãos/entidades regulamentadoras;
- Possui integração com órgãos/entidades de apoio ao sistema financeiro nacional;
- Possui integração com sistema que realize movimentação financeira, seja da instituição ou cliente independente da sua natureza;
- Possui integração com parceiros de negócio;
- Gera arquivos de natureza legal;
- Sistema integrado ao SGA;

São considerados sistemas "**não críticos**" todos os demais sistemas que não estejam enquadrados em pelo ao menos uma das características acima.

1.3.1 - A partir da categorização dos sistemas bancários serão validados os requisitos de segurança e os procedimentos que devem ser efetuados para a integração dos sistemas corporativos ao Sistema de Gestão de Acesso (SGA) (novos e críticos/legado e crítico a partir da avaliação de disponibilidade/criticidade do sistema bancário) ou permanecer com módulo próprio com requisitos de segurança para sistemas críticos ou não críticos do BANPARÁ:

1.3.1.1 - O SGA é um sistema de gerenciamento de identidade que consiste em um ambiente centralizado para controle de privilégios de usuários e grupos de usuários, no seu próprio universo e no universo dos Sistemas Clientes (sistemas corporativos do Banpará) à ele integrados, fazendo-se uso de *login único* em aplicações, além de possuir integração ao sistema de RH, com informações atualizadas de perfis por função de cada funcionário do Banco.

1.3.1.2 - Consideram-se os sistemas legados como os sistemas pré-existentes à implantação do SGA. As possíveis modificações de versões nos sistemas de acesso centralizados dos fornecedores ou dos módulos de segurança de cada sistema novo devem ocorrer para uma efetiva integração ao SGA.

1.3.1.3 - Para os sistemas legados deverão ser avaliados pela área de Segurança da Informação, a integração ao SGA ou permanência de módulo de segurança próprio, contanto que atenda aos requisitos de segurança para sistemas críticos/não críticos, de acordo com disponibilidade/criticidade do mesmo.

1.3.1.4 - Consideram-se novos sistemas como sistemas sob a responsabilidade da SUATI/SUINS/SUDEM, geridos e executados através dos Gerentes de Projetos e fornecedores, sob adequação de funcionalidades para atender especificidades do ambiente do BANPARÁ. Estes sistemas deverão entrar em produção após a homologação desse e de seu módulo de segurança integrado ao SGA ou controle de acesso próprio que atenda a todos os requisitos de segurança para sistemas críticos/não críticos.

1.3.2 - A base de dados utilizada para autenticação e autorização de acesso dos usuários aos sistemas corporativos será do SGA ou do sistema legado que módulo próprio de gestão de acesso, disponibilizadas no momento em que o usuário efetivar o Login a partir destes sistemas.

1.3.2.1 - A base de dados para controle de autenticação no caso do sistema possuir sistema de segurança e acesso próprio deverá centralizar de forma parametrizável gestão de: usuário, senha, perfis, tela, perfil temporário, log transacional e de segurança; para sistemas críticos (Anexo III / IV / V / VI) e para sistemas não críticos (Anexo VII) é imprescindível possuir gestão de: usuário, senha, perfis, perfil temporário, log transacional e de segurança; e multisessão.

1.3.3 - A base de dados utilizada para armazenamento dos Logs de Auditoria nos sistemas clientes será de responsabilidade destes e disponibilizadas mediante consultas efetivadas a partir do SGA ou do sistema legado que possui controle de acesso próprio. Para sistema legado a base de dados para armazenamento dos Logs de auditoria é de responsabilidade do próprio legado.

1.3.4 - Os registros dos Logs de Auditoria e os registros dos Logs de Eventos deverão ser armazenados em banco de dados por um período definido através de parâmetro determinado pelo SGA, e sob a responsabilidade do fornecedor do sistema e anuência do Gerente de Projeto do Banpará, ou do sistema legado que possui módulo próprio de gestão de acesso.

1.3.5 Usar ferramentas de teste, como o OWASP Zed Attack Proxy Project, que analisa o comportamento da aplicação e aponta possíveis vulnerabilidades de segurança. A gravidade de risco da aplicação para o teste supracitado deve ser mínima, caso seja maior deve ser submetida a área de T.I e segurança da informação da CONTRATANTE para avaliação e verificação das fragilidades.

1.4 - ESPECIFICAÇÕES DE INTEROPERABILIDADE PARA CONTROLE DE ACESSO

1.4.1 – A tecnologia utilizada para a comunicação entre os Sistemas (SGA e Clientes) será WebService, a qual possibilita interoperabilidade entre aplicações distribuídas e heterogêneas quanto a suas particularidades de implementação.

1.4.2 – A integração e as trocas de mensagens entre os sistemas clientes e o SGA deverão seguir as recomendações contidas no Manual Técnico Web Services a ser disponibilizado pelo BANPARÁ.

1.4.3 Deverá suportar identificação e validação de estações.

1.4.4 Deverá permitir que os usuários identifiquem-se e autentiquem-se perante o sistema, a partir de base de dados externas como LDAP, utilizando protocolos de autenticação seguros (TLS/SSL).

1.4.5 Deverá permitir a implementação de política de formação de senhas.

1.4.6 Deverá permitir a implementação de política de troca de senhas.

1.4.7 Deverá prover armazenamento seguro das senhas através de criptografia.

1.4.8 Cada fornecedor deverá adequar os Sistemas Clientes sob sua responsabilidade (legados e/ou novos), a fim de que os mesmos possam ter administração concentrada pelo SGA ou no módulo próprio de gestão de acesso que contenha:

a) Dos acessos dos sistemas que serão gerenciados e suas transações;
b) Dos perfis dos usuários;
c) Das contas dos usuários com um dos status abaixo:

- Ativo: o usuário está habilitado a utilizar o sistema;
- Suspenso: o usuário tentou logar no sistema e errou uma certa quantidade de vezes a sua respectiva senha, a citada quantidade é parametrizável nos sistemas novos e integrados ao SGA assim como para sistema legado que possua módulo de acesso próprio. Caso o usuário esteja de folga, férias ou licença seu acesso deve ser bloqueado até reiniciar o trabalho, sendo que o controle de acesso deve ser integrado ao sistema de RH.
- Desativado: o usuário está desabilitado a utilizar o sistema. Pode ocorrer de forma automática via integração com sistema de RH, ou manualmente, pelos analistas de controle de acesso. A opção “Data de desativação” possibilita especificar uma data para desativação do usuário automaticamente. Neste momento, o usuário não deve mais conseguir acessar o sistema.

d) Da definição e consulta de logs dos sistemas.

1.4.9 – Os critérios de acesso para Autenticação e Autorização deverão atender aos seguintes requisitos:

a) O acesso a um sistema corporativo deverá ser autenticado pelo SGA, devendo ser repassado para validação: a matrícula do sistema, login e senha do usuário, conforme definido no MTWS (Manual Técnico de WebService). Ou pelo sistema legado que módulo próprio de gestão de acesso.
b) O SGA deverá identificar o sistema cliente solicitante, e validar os dados de usuário e senha além de registrar os dados repassados no log. Caso o sistema legado possua controle de acesso próprio deve validar dados do usuário e registrar log de acesso.
c) Após a validação dos dados o SGA repassará ao sistema solicitante os dados de autenticação, assim como todas as permissões definidas pelo perfil funcional do usuário. Caso o sistema legado possua controle de acesso próprio deve repassar permissões definidas para perfil funcional do usuário para o sistema integrado a ele e registrar log de acesso.
d) Caso o parâmetro *status* do usuário esteja inativo, o SGA repassará as informações referentes à inatividade, inserindo-os nos parâmetros de retorno e enviando-os ao sistema solicitante para tratamento e apresentação ao usuário. Caso o sistema legado possua controle de acesso próprio deve repassar informação de inatividade para o sistema integrado a ele e apresentar mensagem ao usuário.

e) No caso em que o usuário inserir os parâmetros de autenticação (senha ou login) errados, após tentativas sem sucesso, o sistema cliente deverá informar ao usuário o bloqueio do seu acesso, indicando providências para a normalização. O número de tentativas sem sucesso serão definidas conforme políticas de segurança parametrizáveis no SGA ou no controle de acesso próprio do legado.
f) Os sistemas clientes (integrados) ao SGA não devem permitir multisessão por usuário.
g) Os sistemas legados com controle de acesso próprio ou integrados ao SGA não devem permitir multisessão por usuário. Sendo considerado multisessão sessões em navegadores diferentes ou guias diferentes para sistemas web, para todos os demais sistemas categorizado como crítico ao tentar fazer login na segunda sessão deve ser questionado ao usuário se deseja continuar com sessão que está ativa ou iniciar nova.

h) O sistema categorizado como crítico deve possuir bloqueio das telas por um período parametrizável (semelhante ao bloqueio de descanso de tela do Windows), e desbloqueio com a senha do usuário que está logado no sistema.

1.4.10 – Os critérios parametrizáveis de Troca de Senha deverão atender aos seguintes requisitos:

a) Na troca de senha, através do sistema gerenciado, o mesmo deverá repassar ao SGA as informações necessárias para o registro da última manutenção de usuário conforme definido no MTWS (Manual Técnico de WebService).
b) Se o sistema possuir controle de acesso próprio deverá validar parâmetros de senha sendo: alteração de senha no primeiro login, alteração de senha, caracteres válidos para senha (parametrizável), tamanho mínimo da senha (parametrizável), não permitir cadastro de senha anterior (parametrizável em n senhas anteriores), expiração da senha (parametrizável) e bloqueio da senha (parametrizável). É desejável que haja tela para alterar os parâmetros para senha para sistemas categorizados como críticos, mas caso o legado categorizado como não crítico não tenha disponibilizado a tela parametrizável que faça validação desses quesitos.
c) Durante a autenticação, se o parâmetro de alteração de senha no logon estiver selecionado, o sistema gerenciado deverá solicitar a troca da senha do usuário, repassando os dados para validação do SGA, quanto aos requisitos de segurança da senha (tamanho mínimo, complexidade, repetição e etc) serão definidos através de parâmetros do SGA. Para sistema legado que possui controle de acesso próprio durante autenticação deve validar se parâmetro para alteração de senha no próximo logon estiver marcado deve solicitar troca de senha do usuário repassando os dados para sistema que faz gestão de acesso o qual o mesmo está integrado.
d) Caso o parâmetro de expiração de senha vier selecionado, o sistema gerenciado deverá informar o usuário, dando-lhe a opção de realizar a alteração da mesma.

d) Ao se realizar a troca da senha através do sistema categorizado como crítico e integrado ao SGA, o mesmo deverá repassar os dados necessários (definidos no

MTWS) para o registro da alteração no SGA. e) Na interface de login também deverá conter a funcionalidade “Esqueci minha senha” para sistemas críticos e integrados ao SGA assim como o sistema legado que possui gestão de acesso próprio, possibilitando que o usuário possa recuperar sua senha a qualquer momento. Podendo ocorrer exceções devido às especificidades de negócio ou de sistema.

1.4.11 – Os critérios de Permissões e Grupos de acesso deverão atender aos seguintes requisitos para sistemas integrados ao SGA:

a) As permissões liberadas, específicas de cada sistema, serão liberadas para o Grupo de Acesso e repassadas no momento da autenticação através dos parâmetros definidos no MTWS.

b) Os usuários serão vinculados ao(s) Grupo(s) de Acesso, podendo ser definido período para o(s) mesmo(s).

1.4.12 - Os critérios de Permissões e Perfil de acesso deverão atender aos seguintes requisitos para sistemas legados com/integrados módulo de acesso próprio:

a) As permissões liberadas, específicas de cada sistema, serão liberadas para o Perfil de Acesso e repassadas no momento da autenticação através de integração com módulo próprio de acesso do sistema legado.

b) Os usuários serão vinculados ao(s) Perfil(s) de Acesso, podendo ser definido período para o(s) mesmo(s) como perfil temporário.

1.4.13 Para versão web deve protocolo https e usar SSL (TSL 1.2) no servidor e também rodar o certificado SSL para comunicação.

1.4.14 Não permitir que senha copiada ou que esteja na área de transferência seja colada no campo senha para fazer login.

1.4.15 Senha dos usuários de sistema não deve trafegar limpa nas chamadas, seja ela da forma que for. Assim como não devem ser armazenadas sem criptografia.

1.4.16 Permitir expiração de telas apresentando ao usuário uma mensagem de expiração e realizando esta operação caso o usuário se ausente por um período parametrizável. Após expirar telas para acessar o sistema o usuário deverá fazer logon novamente.

1.4.17 Permitir que somente usuários credenciados configurem seu funcionamento da melhor maneira que convier ao BANPARÁ.

1.4.18 AUTORIZAÇÃO E CONTROLE DE ACESSO

1.4.18.1 Deverá possuir níveis de permissão de acessos às funcionalidades da Solução de forma parametrizável, permitindo inclusão/exclusão de usuários em lote/arquivo.

1.4.18.2 Deverá suportar a configuração do período de inatividade das sessões individuais de usuário, usando o timeout da sessão, para disparar um screensaver protegido por senha.

1.4.18.3 Deverá possuir um módulo independente de autorização de usuários de modo a, futuramente, agilizar integração com sistema de autorização ou active directory do BANPARÁ.

1.4.18.4 Deverá suportar o controle de timeout de sessão de forma parametrizável.

1.4.18.5 Deverá implementar os mecanismos de autenticação e autorização por intermédio das ferramentas RACF e/ou LDAP.

1.5 - ESPECIFICAÇÕES DE INTEROPERABILIDADE PARA TRILHAS DE AUDITORIA

1.5.1 - As especificações desse item deverão existir para os sistemas categorizados como críticos e não críticos tanto sistemas novo como legados.

1.5.1.1 – Para legados dever-se-á revalidar a gestão de acesso dos mesmos para verificar aderência a esse requisito e gerar solicitação de mudança para área de sistemas. Para serviço disponibilizado para cliente como cobrança não registrada e que a base é local por cliente assim como seu gerenciamento a gestão é do cliente e não do Banpará.

1.5.1.2 Dados referenciados da transação.

1.5.1.3 Deverá possuir trilha de auditoria protegida contra acessos não autorizados.

1.5.1.4 Deverá permitir pesquisa por meio de consulta e/ou impressão de relatório específico, obedecendo ao nível de acesso do usuário autorizado.

1.5.1.5 Deverá realizar arquivamento automático de informações de auditoria em mídia digital ou outro meio eletrônico quando a área de armazenamento da trilha de auditoria atingir seu volume máximo de armazenamento.

1.5.2 – Os critérios de Log de Auditoria deverão atender aos seguintes requisitos:

a) São consideradas duas categorias de Log: **Log de Segurança de Acesso** e ***Log* de Transações**.

- O **Log de Segurança** corresponde aos registros efetuados dentro do ambiente do SGA, legado integrado ao RH, como: alterações de permissões, mudanças de grupos, registros de Login, de Logout, além de Acessos específicos a Objetos dos sistemas clientes (acesso as telas de transações de empréstimos e etc.), bem como aos seus eventos.
- O **Log de Transações:** corresponde às mensagens de eventos de: Erros, Avisos, Falhas e demais transações específicas de ações efetuadas pelo usuário durante a interação nos sistemas clientes.

b) O **Log de Segurança** para os sistemas integrados ao SGA será armazenado no ambiente do SGA. Para legado integrado ao RH será armazenado pelo sistema de gestão de acesso do legado e deverá conter os registros enviados pelos sistemas gerenciados com os seguintes parâmetros:

j) Usuário de rede;
k) Login do Usuário;
l) Grupo (perfil) do usuário;
m) Operação;

n) Contexto ();
o) Endereço IP e porta lógica que realizou as transações;
p) Nome de máquina (Hostname);
q) A data e hora de evento do usuário, sendo (recomendável o uso do relógio do sistema e não o do host);
r) MAC Address;
s) Geolocalização;
t) Os registros das informações deverão ser mantidos em base de dados em ambiente de produção por período definido pela SUROP.

c) O Log de Transação de cada sistema cliente deverá ser armazenado em banco de dados próprio, possibilitando o acesso a partir do SGA aos registros deste contendo os seguintes parâmetros:

u) Login do usuário;
v) Endereço IP com porta lógica do acesso e Hostname da máquina que realizou as transações;
w) A data e hora de evento do usuário sendo (recomendável o uso do relógio do sistema e não o do *host*) com geolocalização;
x) Usuário de rede;
y) Perfil do usuário;
z) Eventos do usuário, a exemplo, gravação de arquivo, inclusão, alteração e exclusão de dados, deverão ser formatos em tabela. Em casos em que o evento for alterado, deverá ser incluso o dado anterior e posterior á ação salva;
aa) Módulo Acessado;
bb) Relatório do Log com permissão para salvar e imprimir, de acordo com a necessidade do usuário que está consultando o log.

f) O Log de Transação de sistema legado deverá ser armazenado em banco de dados próprio, possibilitando o acesso aos registros deste a partir do módulo de controle de acesso, deste o qual deve estar integrado, contendo os seguintes parâmetros:

- Login do usuário;
- Endereço IP com porta lógica do acesso e Hostname da máquina que realizou as transações;
- A data e hora de evento do usuário sendo (recomendável o uso do relógio do sistema e não o do host) com geolocalização;
- Usuário de rede;
- Eventos do usuário, a exemplo, gravação de arquivo, inclusão, alteração e exclusão de dados, deverão ser formatos em tabela. Em casos em que o evento for alterado, deverá ser incluso o dado anterior e posterior á ação salva;
- Módulo Acessado;
- Relatório do Log com permissão para salvar e imprimir, de acordo

com a necessidade do usuário que está consultando o log.

g) Eventos a serem registrados:

- operações de login e logout;
- acessos a todas as telas ou seções do sistema;
- acesso a informações com alguma restrição (eg documentos sigilosos, processos em segredo de justiça, dados pessoais ou bancários)
- documentos sigilosos, processos em segredo de justiça, dados pessoais ou ba operações de consulta, inclusão, alteração ou exclusão de registros no banco de dados;
- alteração de perfil de acesso ou status de usuários (para sistemas que possuem acesso com diferentes perfis)
- execução de jobs e tarefas automatizadas

h) Sistema gestão de acesso deve manter o registro histórico de operações efetuadas nele sob forma de log de auditoria, como supracitado. Deve estar indicado na auditoria as alterações (insert, update, delete) que foram feitas por aplicação e as de feitas manualmente no banco de dados para INSERT, UPDATE and DELETE: insert, update, delete, commit, rollback e execute. Ou seja, há necessidade de distinguir o que foi feito via aplicação, sistema de gestão de aceso ou nos sistemas integrados, e o que foi feito manualmente no banco de dados.

- As informações de log devem conter usuário do sistema (se via aplicação usuário que estava acessando o sistema ou se manualmente no banco de dados usuário que executou o registro: insert, update, delete, commit, rollback), usuário da rede, endereço IP da máquina do usuário, eventos, data e hora do evento.
- Qualquer operação de inserção, consulta, edição e exclusão sobre as entidades do sistema devem ser mantidas, bem como operações de vinculações, geração de relatórios, uso de filtros, autenticações (sejam elas bem sucedidas ou fracassadas). A exceção serão objetos não passíveis de logs conforme parametrizado.

i) Sistema deve permitir a consulta de todas as informações de logs de auditoria de todas as operações efetuadas pelo usuário no sistema de gestão de aceso.
j) A visualização das informações de logs de auditoria será liberada somente para determinados grupos/usuários, a serem determinados pelo administrador de gestão de acesso do sistema.
k) Sistema deve permitir a consulta de logs de auditoria dos sistemas integrados a ele.
l) Sistema deve permitir a consulta de todas as informações de eventos realizados sobre o usuário no sistema de gestão de acesso. As informações sobre usuário

incluem vinculações, alteração de situação, tentativas de logon, data de criação, alteração de senha e a consulta desse logs de auditoria serão liberadas somente para determinados grupos/usuários a serem determinados pelo administrador de gestão de acesso do sistema.

m) O sistema deve permitir a exportação de logs de auditoria parametrizado para um determinado sistema ou grupo ou usuário para um arquivo.

n) Sistema deve permitir a exclusão de logs de auditoria de um determinado período e por determinado grupo/usuários a serem determinados pelo administrador de gestão de acesso do sistema, entretanto não deve ser permitida a exclusão de logs dos 3 últimos anos (essa informação deve ser parametrizável). Além disso as informações de registro de logs excluídos também devem ser mantidas, sob forma de log de auditoria.

o) Não permitir alteração em banco de dados do segurança acesso se não tiver origem do servidor de aplicação desse sistema. Para os sistemas integrados a validação deve garantir que seja única a conexão entre servidores de banco de dados ou do servidor de aplicação do sistema integrado com servidor de base do sistema de segurança e acesso.

p) O sistema deve permitir relatórios dos logs de auditoria conforme a seguir:

- Relatório Auditoria
    - Sistema:
    - Módulo:
    - Documento:
    - Função:
    - Usuário de sistema:
    - Usuário de banco de dados:
    - Usuário de rede:
    - IP:
    - Data Inicial:
    - Data Final:
    - Empresa:
    - Unidade:
    - Data:
    - Operação:
    - Banco:
    - Tabela:
    - Comando Sql:
    - Mudança:
    - Nº de Linhas Incluída(s):
    - Registros Incluído(s): Nº Linha, Coluna, Descrição Coluna, Valor
- Relatório Auditoria Gestor:
    - Sistema:

- Módulo:
- Documento:
- Função:
- Usuário de sistema:
- Usuário de rede:
- IP:
- Data Inicial:
- Data Final:
- Empresa:
- Unidade:
- Data:
- Operação:
- Banco:
- Tabela:
- Nº de Linhas Incluída(s):
- Registros Incluído(s): Nº Linha, Coluna, Descrição Coluna, Valor

1.6. RELATÓRIOS:

1. Disponibilizar os seguintes relatórios: sistemas, módulos (sistemas e módulos vinculados), empresas organizacionais, unidades organizacionais, usuários (usuários ativos, bloqueados e inativos), grupos de acesso (perfis e usuários vinculados bem como perfis, sistemas, módulos e funcionalidades associadas contendo permissões), usuários e suas permissões associadas (perfis e permissões específicas), sistemas e usuários vinculados contendo suas permissões, módulos e usuários vinculados contendo suas permissões, detalhes do usuário, logs de auditoria, histórico de conta de usuários, acessos do sistema/módulo com filtros por usuário, sistema, módulo e objeto.
2. Deverá ser fornecido a consulta e relatório contendo as informações do sistema/módulo, usuários, quantidade de acesso, data e hora do último acesso
3. Disponibilizar a exportação dos relatórios para arquivos do tipo documento (.rtf), planilhas (.xls) e formato de documento portátil (.pdf)
4. Disponibilizar relatório com mapeamento de perfilxfuncionalidade por sistema na seguintes estrutura:
    - Imprimir em paisagem
    - Sistema Integrado
        - 1ª coluna: funcionalidades
        - Seguir a estrutura a seguir:
            - Sistema
            - Módulo>>Menu >> Transação >> Função
            - Módulo>>Menu >> Transação >> Função [Botão] Editar

- A partir da segunda coluna incluir um perfil por coluna até terminar todos os perfis que possuem acesso ao sistema.
- As colunas dos perfis devem ser preenchidas com: S: Possui permissão ou N: Não possui permissão.
- A última coluna após terminar os perfis que possuem acesso deve ser incluída a Legenda do mapeamento:
- Permissão:
- S: Possui permissão
- N: Não possui permissão.
- Legenda perfis de acesso:
- Listar por linha enumerada os perfis que possuem acesso (ex.: 1. Perfil xxxxx), sendo que a senguda coluna onde iniciou o mapeamento de perfil seria o primeiro perfil da legenda.
- Responsável pelas definições: área gestora do sistema.
- Responsável pela Estruturação: quem parametrizou no sistema de gestão de acessos do SPA as permissões dos perfis para o sistema integrado.

5. Disponibilizar relatório com mapeamento com todas as permissões do usuário por sistema que possui acesso, sendo cada sistema na estrutura do item 4.
6. Disponibilizar relatório com mapeamento de permissões de usuários por unidade ou empresa ou combinação dos dois, filtro que for selecionado, sendo cada sistema na estrutura do item 4. Tendo a opção de escolha nesse filtro todas as empresas e todas as unidades.
7. Relatório com usuário(s) de sistema com estrutura: usuário de sistema, nome, perfil, empresa, unidade que pode acessar, data do último acesso no sistema. Sendo que pode ser selecionado um usuário e um sistema ou um sistema e todos os usuários deste ou todos os sistemas e todos os usuários de todos os sistemas: segurança acesso e sistemas integrados a ele, os quais gerencia o controle de acesso.
8. Relatório de permissão por perfil: Detalha por permissão todos os perfis que possuem acesso a essa funcionalidade. Há opção de escolher um ou mais ou todos os sistemas, ou seja, sistema de segurança acesso e todos integrados a ele. Tem que haver separação por estrutura do sistema.

Sistema deve possuir conceito de abrangência de acordo com o que for associado para usuário, ou seja, se for associado empresa(s) e unidade(s)o usuário deve gerenciar dados conforme perfil e combinação de empresa(s)/unidade(s) vinculado ao mesmo. Caso não seja vinculado nenhuma empresa/unidade o usuário não possui acesso a nada.

a. CONFIDENCIALIDADE E INTEGRIDADE

i. Deverá manter informações confidenciais criptografadas independente da mídia de armazenamento.

ii. Deverá suportar, no mínimo, os algoritmos de criptografia definidos no padrão JCA (Java Criptographic Achitecture) para garantia de sigilo de comunicação.
iii. Deverá suportar, no mínimo, os algoritmos de criptografia definidos no padrão JCA (Java Criptographic Achitecture) para proteção de dados sigilosos armazenados.

b. A arquitetura do sistema deverá ser avaliada pelas áreas de risco em fraude eletrônica e segurança da informação.

c. Sistema deve seguir o padrão de logs usado na instituição (BANPARÁ).

d. CLIENTE WEB
i. Deverá suportar acesso por meio de qualquer navegador web (browser).
ii. Deverá suportar o protocolo HTTPS.
iii. Deverá possuir controle parametrizável de timeout de sessão.
iv. Deverá permitir a gravação do log para uma agência, para um grupo de agências e para todas as agências configuradas no servidor de aplicação (Application Server).
v. Deverá possuir baixo acoplamento, permitindo que novos serviços e manutenções corretivas sejam disponibilizados separadamente, ou em conjunto de transações, e não por pacote de atualização de todo o aplicativo, e que estes não deverão indisponibilizar os demais módulos/transações do sistema.
vi. Deverá permitir que novas funcionalidades sejam adicionadas sem impactos (inconsistências) nos módulos pré-existentes.
vii. Deverá possuir um mapeamento das interdependências dos componentes que compõem o aplicativo, de forma que em caso de alteração/implementação, não seja necessário testar os componentes não afetados.
viii. Deverá suportar a integração com, no mínimo, os seguintes padrões de mercado: XML, HTML, ISO, HTTPS, SSL e mensageria MQ.
ix. Deverá suportar Certificação Digital no padrão X509
1. Deverá ser parametrizável de forma que seja possível definir, para os perfis a serem definidos pela BANPARÁ, níveis de permissão de acessos a todos os recursos e módulos do sistema.
2. Deverá permitir parametrização tanto de configurações do sistema como de lógica das regras de negócios, com registro das ações em log.
x. Todas as alterações em parâmetros devem ser registradas em log, mostrando no mínimo identificação da estação, usuário, data/hora e ação realizada.
xi. Deverá permitir conexão com ferramentas de mercado voltadas à cobrança e à prevenção de fraude;
xii. Deverá suportar arquitetura com servidores em cluster, de banco de dados e de aplicação, bem como diversas configurações de RAID, devendo a Solução ser compatível com esses recursos.
xiii. Deverá prever processamento simultâneo em dois (2) sites distintos, distantes

pelo menos 3 km a 12 km do outro, com balanceamento de carga.

xiv. A Solução deve ser customizada de forma a permitir a instalação em ambiente de alta disponibilidade, com redundância.

xv. Deverá ser capaz de montar dinamicamente menus personalizados de acordo com o perfil do usuário, de forma que sejam inibidos os serviços a usuários não autorizados.

xvi. Deverá dispor de gerenciamento de relatórios da BANPARÁ em tempo real. DE

xvii. Deverá possuir simuladores de testes das transações, inclusive simuladores de comunicação com o host.

xviii. As interfaces com o usuário (telas, formulários, relatórios, mensagens de erros), e todas as outras formas de interação com o usuário, deverão estar em português do Brasil.

xix. Deverá permitir controles centralizados da manutenção e atualização das aplicações.

xx. Deverá possuir módulo de monitoração com geração de logs e armazenamento de dados históricos de desempenho, falhas, disponibilidade da solução, disponibilidade e desempenho de cada funcionalidade da Solução e ainda deverá estar integrado com a solução de monitoração da BANPARÁ (Módulo TEC do framework IBM Tivoli)

xxi. Deverá ter dispositivo, tipo sonda, capaz de avisar rotineiramente ao ambiente PRD que está ativa e operante.

xxii. A monitoração não deverá comprometer o desempenho do sistema, seja qual for o seu nível de configuração

e. Utilizar o protocolo SHA256 ao invés do SHA1 que está em desuso ou superior.

f. Os dados não devem trafegar, em hipótese nenhuma, limpos e sim com criptografia.

g. É necessário que seja gravado histórico das funcionalidades do sistema

h. Geração de HASH único (SHA2-512) para criptografia de senha armazenada, com capacidade de ser alterada sem ônus por SUROP/GESEI.

i. Encriptar (RSA3072) a senha do cliente para o tráfego, sendo que a chave pública com validade parametrizável, ou seja, pode ser alterada em qualquer momento e o sistema se adequa a nova chave para as novas transações. Assim como informações temporárias para que um usuário não possa modifica-las em caso de fraude ao sistema.

i. Controle para não-repúdio e registro de entrega.

j. Necessário que a url https a ser utilizada use um certificado twoway e token de sessão na comunicação entre os servidores, sendo parametrizável o tempo de vida desse token e uma vez usado o número do token o mesmo não poderá ser utilizado novamente. Validação entre token de sessão e token do cookie, se for o caso.

k. Se sistema web não deve permitir alteração de informações que o mesmo utiliza, ou seja, correspondência 1-1 entre informação de sistema e de banco. E utilizar WS-ReliableMessaging para integração entre sistemas.

l. Sistema deve prevenir os seguintes ataques: tratamento inadequado de erros e exceções (ERROR HANDLING) , ataque de formação de strings (FORMAT STRINGS ATTACKS) , estouro de memória (BUFFER OVERFLOW), estouro de inteiros (INTEGER OVERFLOW), caminho reverso (PATH TRAVERSAL), execução com privilégios desnecessários, ataques de enumeração (ENUMERATION), injeção de comandos (COMMAND INJECTION), injeção de códigos SQL (SQL INJECTION), upload de arquivos potencialmente perigosos, senhas incluídas no código fonte do sistema (USE OF HARD-CODED PASSWORD), cross-site scripting (XSS), força bruta e uso de robôs automatizados, interceptação do fluxo de comunicação.

m. Quanto a segurança de banco de dados:

a) Não incluir strings de conexão na aplicação. Estas informações devem estar em um arquivo de configuração isolado em um ambiente confiável e os dados criptografados;

b) Usar procedimentos armazenados (stored procedures) para abstrair o acesso aos dados e permitir a remoção de permissões das tabelas no banco de dados;

c) Usar variáveis e consultas parametrizadas fortemente “tipadas”;

d) Utilizar validação de entrada/saída e assegurar a abordagem de meta caracteres (escaping) em instruções SQL. Se houver falha, o comando não deverá ser executado;

e) A aplicação deve conectar-se ao banco de dados com diferentes credenciais de segurança para cada tipo de configuração e publicação de sistemas.

ADENDO X
DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE SUSTENTABILIDADE

[Nome da empresa], CNPJ n.º _____sediada [Endereço completo], declara sob as penas da lei, que:

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

b) Não emprega menores de 18 anos para trabalho noturno, perigoso ou insalubre, e menores de dezesseis anos para qualquer trabalho, com exceção a categoria de Menor Aprendiz.

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

d) Respeita o direito de formar ou associar-se a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias.

e) Buscará a incorporação em sua gestão dos Princípios do Pacto Global, disponível em http: http://www.pactoglobal.org.br/artigo/56/Os-10-principios, bem como o alinhamento com as diretrizes da Política de Responsabilidade Socioambiental do Banpará disponível em http://www.banpara.b.br/media/187386/prsa.pdf.

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

g) Desenvolve suas atividades respeitando a legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como os demais dispositivos legais relacionados a proteção dos direitos humanos, abstendo-se de impor aos colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se:

i. “Condições ultrajantes”: condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo.

ii. “Condições sub-humanas”: tudo que está abaixo da condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano, situação abaixo da linha da pobreza.

iii. “Condições degradantes de trabalho”: condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão.

_____
Local e Data

_____
Nome e Identidade do Declarante

ADENDO XI
MODELO DE DECLARAÇÃO – CONFORMIDADE AO ART.38 DA LEI Nº 13.303/2016

Ao BANCO DO ESTADO DO PARÁ S.A.
Av. Presidente Vargas, nº 251, Ed. BANPARÁ – 1º andar
Comércio, Belém/PA, CEP 66.010-000

Ref: Edital de Licitação nº ...../.....
Objeto:.....

Prezados senhores,

A ....., inscrita no CNPJ sob o nº ....., sediada .....(endereço completo)....., com o telefone para contato nº (.....).....-..... e email ....., por intermédio do seu representante legal o(a) Sr.(a) ....., ...(cargo)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº ....., residente e domiciliado(a) no .....(endereço completo)....., DECLARA, para os devidos fins legais, que a empresa não incorre em nenhum dos impedimentos para participar de licitações e ser contratada, prescritos no art. 38 da Lei nº 13.303/2016, quais sejam:

(i) cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;
(ii) suspensa pela empresa pública ou sociedade de economia mista;
(iii) declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;
(iv) constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;
(v) cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;
(vi) constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
(vii) cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
(viii) que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

Aplica-se a vedação também:

(i) à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;
(ii) a quem tenha relação de parentesco, até o terceiro grau civil, com:
a) dirigente de empresa pública ou sociedade de economia mista;
b) empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

c) autoridade do ente público a que a empresa pública ou sociedade de economia mista esteja vinculada.

(iii) cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a respectiva empresa pública ou sociedade de economia mista promotora da licitação ou contratante há menos de 06 (seis) meses.

.....
(Local e Data)

.....
(representante legal)

ANEXO II - MINUTA DE INSTRUMENTO DE CONTRATO

Contrato nº ...../.....

TERMO DE CONTRATO DE ..... QUE ENTRE SI FAZEM O BANCO DO ESTADO DO PARÁ S.A. E A EMPRESA .....

Por este instrumento particular, de um lado, o BANCO DO ESTADO DO PARÁ S.A., instituição financeira, com sede em Belém do Pará, na Avenida Presidente Vargas, n.º 251, Bairro Comércio, CEP. 66.010-000, Belém-PA, inscrito no Ministério da Fazenda sob o CNPJ n.º 04.913.711/0001-08, neste ato representada legalmente por dois de seus Diretores infra-assinados, doravante denominado BANPARÁ e, de outro lado, ..., estabelecida à ....., inscrita no CNPJ sob o nº ....., por seus representantes, infra-assinados, doravante designada simplesmente CONTRATADA, celebram o presente contrato mediante as cláusulas seguintes:

1. CLÁUSULA PRIMEIRA – OBJETO

O presente contrato tem como objeto **contratação de Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um dos padrões: PCI DSS, ISO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework**, conforme especificações, exigências e condições estabelecidas no edital e seus Anexos.

1.1. O presente contrato decorre do processo nº **0298/2020**, realizado pelo edital da licitação do PE nº 028/2021.

2. CLÁUSULA SEGUNDA – ADENDOS

2.1 Fazem parte integrante do presente contrato, como se nele estivessem transcritos, os seguintes adendos:

Adendo 1 – Edital / Anexos / Termo de Referência

Adendo 2 – Proposta de Preços

Adendo 3 - Declaração de Conformidade ao art.38 da Lei nº 13.303/2016.

Adendo 4 – Termo de Política Anticorrupção

2.2 Este contrato e seus adendos 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 adendos, prevalecerão as regras deste contrato e, na sequência, na ordem dos adendos.

3. CLÁUSULA TERCEIRA – PRAZOS

3.1 O prazo de vigência desta contratação é de 12 (doze) meses, contados da assinatura do mesmo, podendo ser prorrogado a critério do Banpará, conforme legislação vigente, contados da assinatura do Contrato.

3.2 Os prazos previstos neste contrato, de execução e vigência, poderão ser prorrogados, durante a vigência contratual, com a aquiescência da CONTRATADA, por meio de termo aditivo.

4 CLÁUSULA QUARTA – VALOR DO CONTRATO E RECURSOS ORÇAMENTÁRIOS

4.1 Como contrapartida à execução do objeto do presente contrato, o BANPARÁ deve pagar à CONTRATADA o valor total de ....., conforme o valor da tabela abaixo e nas condições estabelecidas no **Termo de Referência** (**ANEXO I** do Edital e Adendo 1 deste contrato):

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 à boa realização do objeto desta contratação, isentando o BANPARÁ de quaisquer ônus adicionais.

ITEM	**DESCRIÇÃO**	**VALOR TOTAL**
1	Serviço de Auditoria em Segurança da Informação, voltada a segurança cibernética de acordo com um	

	dos padrões: PCI DSS, ISSO 27001, NIST SP 800-53 ou NIST Cybersecurity Framework, conforme descritas nos termos do Edital, Termo de Referência e seus anexos	

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 BANPARÁ, 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 3 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação contratual e complementada em casos de aditivos e apostilas para reajustes.

5.1.1 A CONTRATADA deve prestar garantia numa das seguintes modalidades:

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

i. Estatuto Social e ata de posse da diretoria da Instituição Financeira;

ii. Quando Procuradores, encaminhar as procurações devidamente autenticadas, com poderes específicos para representar a Instituição Financeira;

iii. Balanços Patrimoniais e Demonstração de Resultado dos últimos dois anos, acompanhado das notas explicativas e respectivos pareceres do Conselho de Administração e Auditores Independentes;

iv. Memória de cálculo do Índice de Adequação de Capital (Índice da Basileia) e Índice de Imobilização, comprovando que a instituição financeira está enquadrada no limite estabelecido pelo Banco Central, para comparação e validação com os dados disponíveis no “site” do Banco Central do Brasil (www.bcb.gov.br).

b) Caução em dinheiro, valor **depositado** pela CONTRATADA, no Banco ....., Agência ....., Conta Corrente n. ....., em nome do BANPARÁ. 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 para análise e aceitação por parte do BANPARÁ.

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 BANPARÁ decorrentes de culpa ou dolo durante a execução do contrato;

c) Multas moratórias e compensatórias aplicadas pelo BANPARÁ 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 BANPARÁ 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 BANPARÁ, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato; ou

b) Após 3 (três) meses do término da vigência do presente contrato.

6 CLÁUSULA SEXTA – EXECUÇÃO DO CONTRATO

6.1 O contrato deve ser cumprido fielmente pelas partes de acordo com as Cláusulas e condições avençadas, as normas ditadas pela Lei n. 13.303/2016 e pelo Regulamento de Licitações e Contratos do BANPARÁ, bem como, de acordo com todas as obrigações, condições e exigências estabelecidas no Termo de Referência e anexos, respondendo cada uma das partes pelas consequências de sua inexecução total ou parcial.

6.2 A CONTRATADA deverá executar o objeto especificado nos detalhamentos deste instrumento de contrato, cumprindo todas as obrigações e responsabilidades a si indicadas no Termo de Referência (**ANEXO I** do Edital e Adendo 1 deste contrato):

6.2.1 O BANPARÁ deverá acompanhar e assegurar as condições necessárias para a execução do contrato, cumprindo rigorosamente todas as obrigações e responsabilidades a si indicadas no Termo de Referência (**ANEXO I** do Edital e Adendo 1 deste contrato).

6.3 A CONTRATADA é responsável pelos danos causados direta ou indiretamente ao BANPARÁ ou a terceiros em razão da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo BANPARÁ.

6.4 A gestão do presente contrato deve ser realizada pela área técnica do BANPARÁ. 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.

6.5 A fiscalização da execução do presente contrato será realizada por agentes de fiscalização, que devem ser designados pelo gestor do contrato, permitindo-se designar mais de um empregado e atribuir-lhes funções distintas, como a fiscalização administrativa e técnica, consistindo na verificação do cumprimento das obrigações contratuais por parte da CONTRATADA, com a alocação dos recursos, pessoal qualificado, técnicas e materiais necessários.

6.6 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.

6.7 O CONTRATANTE poderá, a qualquer momento, solicitar a apresentação, pela CONTRATADA, os documentos pertinentes à sua regularidade jurídico-fiscal, para fins de comprovar a manutenção das condições de habilitação durante a execução do Contrato.

6.7.1 Verificada eventual situação de descumprimento das condições de habilitação, o CONTRATANTE pode conceder prazo para que a CONTRATADA regularize suas obrigações ou sua condição de habilitação, conforme disposto

no Art. 95, itens 5 e 6 do Regulamento, quando não identificar má fé ou incapacidade da CONTRATADA corrigir tal situação.

6.7.2 O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação, podem ensejar rescisão contratual sem prejuízo das demais sanções.

6.8 Constatada qualquer irregularidade na licitação ou na execução contratual, o gestor do contrato deve, se possível, saneá-la, evitando-se a suspensão da execução do contrato ou outra medida como decretação de nulidade ou rescisão contratual.

6.8.1 Na hipótese prevista neste subitem, a CONTRATADA deve submeter ao BANPARÁ, por escrito, todas as medidas que lhe parecerem oportunas, com vistas a reduzir ou eliminar as dificuldades encontradas, bem como os custos envolvidos. O BANPARÁ 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.

6.9 As partes CONTRATANTES não são responsáveis pela inexecução, execução tardia ou parcial de suas obrigações, quando a falta resultar, comprovadamente, de fato necessário decorrente de caso fortuito ou força maior, 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.

6.10 No caso de uma das partes se achar impossibilitada de cumprir alguma 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.

6.10.1 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.

6.10.2 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.

6.11 A não utilização pelas partes de quaisquer dos direitos assegurados neste contrato, ou na Lei em geral, ou no Regulamento, ou a não aplicação de quaisquer sanções, não invalida o restante do contrato, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação ou de ações futuras.

6.12 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 BANPARÁ - .....

E-mail CONTRATADA - .....

6.12.1 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.

6.12.2 Os prazos indicados nas comunicações iniciam em 2 (dois) dias úteis a contar da data de envio do e-mail.

6.12.3 As partes estão obrigadas a comunicarem uma a outra, com 5 (cinco) dias de antecedência, qualquer alteração nos respectivos e-mails. No caso de falha ou problema técnico, as partes devem comunicar, uma a outra, em até 5 (cinco) dias.

7 CLÁUSULA SÉTIMA – RECEBIMENTO

7.1 O BANPARÁ, por meio do agente de fiscalização técnica, deve HOMOLOGAR os produtos entregues e os serviços executados conforme as regras estabelecidas no Termo de Referência, Adendo 1 deste contrato.

8 CLÁUSULA OITAVA – CONDIÇÕES DE FATURAMENTO E PAGAMENTO

8.1 Os pagamentos serão efetuados conforme as regras estabelecidas no Termo de Referência, Adendo 1 deste contrato.

8.2 O pagamento será condicionado ao recebimento dos serviços por etapas e nos percentuais, conforme Termo de Referência (Adendo 1 deste contrato), e somente após validação do responsável do BANPARÁ pelo projeto. O pagamento será efetuado mediante a apresentação de Nota Fiscal/Fatura pela CONTRATADA à unidade de gestão de contrato do BANPARÁ, que deve conter o detalhamento da etapa executada, com especificações dos serviços efetuados, o número do contrato, a agência bancária e conta corrente na qual deve ser depositado o respectivo pagamento.

8.3 As faturas que apresentarem erros ou cuja documentação suporte esteja em desacordo com o contratualmente exigido devem ser devolvidas à CONTRATADA pela unidade de gestão de contrato do BANPARÁ para a correção ou substituição. O

BANPARÁ, 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 BANPARÁ.

8.4 A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer cláusulas contratuais.

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

8.6 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário e órgãos administrativos, atribuídos ao CONTRATANTE, oriundos de problemas na execução do contrato por ato da CONTRATADA, serão repassados a esta e deduzidos do pagamento realizado pelo Banco, independente de comunicação ou interpelação judicial ou extrajudicial.

8.7 Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo BANPARÁ, incidirá sobre os valores em atraso juros de mora no percentual de 1% (um por cento) ao mês, *pro rata die*, calculados de forma simples sobre o valor em atraso e devidos a partir do dia seguinte ao do vencimento até a data da efetiva liquidação do débito.

9 CLÁUSULA NONA – DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO

9.1 Fica, desde já, entendido que os profissionais que prestam serviços para a CONTRATADA não possuem qualquer vínculo empregatício com o CONTRATANTE.

9.1.1 A CONTRATADA obriga-se a realizar suas atividades utilizando profissionais regularmente contratados e habilitados, cabendo-lhe total e exclusiva responsabilidade pelo integral atendimento de toda legislação que rege os negócios jurídicos e que lhe atribua responsabilidades, com ênfase na previdenciária, trabalhista, tributária e cível.

9.1.2 A CONTRATADA obriga-se a reembolsar ao CONTRATANTE todas as despesas decorrentes de:

a) Reconhecimento judicial de titularidade de vínculo empregatício de prepostos seus com o **CONTRATANTE**, ou qualquer empresa do mesmo grupo econômico;

b) Reconhecimento judicial de solidariedade ou subsidiariedade do **CONTRATANTE** ou qualquer outra empresa do mesmo grupo econômico no cumprimento das obrigações previdenciárias da **CONTRATADA**.

9.1.3 O CONTRATANTE não assumirá responsabilidade alguma pelo pagamento de impostos e encargos que competirem à CONTRATADA, nem se obrigará a restituir-lhe valores, principais ou acessórios, que esta, porventura, despender com pagamentos desta natureza.

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 BANPARÁ, 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 a ser atendido pela obra ou pelo serviço;

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

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

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

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

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 BANPARÁ, 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 BANPARÁ; e

c) Submetidas à área jurídica e, quando for o caso, à área financeira do BANPARÁ;

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 BANPARÁ.

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

a) A variação do valor contratual para fazer face ao reajuste de preços;

b) As atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no contrato;

c) A correção de erro material havido no instrumento de contrato;

d) As alterações na razão ou na denominação social da CONTRATADA;

e) As alterações na legislação tributária que produza efeitos nos valores contratados.

11 CLÁUSULA DÉCIMA PRIMEIRA – EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO

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

a) Reajuste: instrumento para manter o equilíbrio econômico-financeiro do contrato diante de variação de preços e custos que sejam normais e previsíveis, relacionadas com o fluxo normal da economia e com o processo inflacionário, devido ao completar 1 (um) ano a contar da data da proposta;

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

11.2 Os valores contratados serão reajustados anualmente, a contar da data de assinatura deste contrato, no prazo da lei, segundo a variação acumulada do INPC do Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro, na falta deste, que estiver estabelecido na legislação à época de cada reajuste.

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 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 BANPARÁ, reduzindo-se o preço.

11.3.2 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 BANPARÁ 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 BANPARÁ 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.

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

12 CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

12.1 O inadimplemento contratual de ambas as partes autoriza a rescisão, que deve ser formalizada por distrato e antecedida de comunicação à outra parte contratante sobre a intenção de rescisão, apontando-se as razões que lhe são determinantes, dando-se o prazo de 5 (cinco) dias úteis para eventual manifestação.

12.2 A parte que pretende a rescisão deve avaliar e responder motivadamente a manifestação referida no subitem precedente no prazo de 5 (cinco) 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 serviços 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 BANPARÁ pode conceder prazo para que a CONTRATADA regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade da CONTRATADA de corrigir a situação.

13 CLÁUSULA DÉCIMA TERCEIRA – SANÇÕES ADMINISTRATIVAS

13.1 Pela inexecução total ou parcial do contrato, o BANPARÁ poderá, garantida a prévia defesa, de acordo com o processo administrativo preceituado no artigo 99 do Regulamento, aplicar ao contratado as sanções de advertência ou suspensão temporária de participação em licitação e impedimento de contratar com o BANPARÁ por prazo não superior a 2 (dois) anos, que podem ser cumuladas com multa.

13.2 As sanções administrativas devem ser aplicadas diante dos seguintes comportamentos da CONTRATADA:

a) Dar causa à inexecução parcial ou total do contrato;

b) Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

c) Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

d) Prestar declaração falsa durante a licitação ou a execução do contrato;

e) Praticar ato fraudulento na execução do contrato;

f) Comportar-se com má-fé ou cometer fraude fiscal.

13.3 A sanção de suspensão, referida no inciso III do artigo 83 da Lei n. 13.303/2016, deve observar os seguintes parâmetros:

a) Se não se caracterizar má-fé, a pena base deve ser de 6 (seis) meses;

b) Caracterizada a má-fé ou intenção desonesta, a pena base deve ser de 1 (um) ano e a pena mínima deve ser de 6 (seis) meses, mesmo aplicando as atenuantes previstas.

13.3.1 As penas bases definidas neste subitem devem ser qualificadas nos seguintes casos:

a) Em 1/2 (um meio), se a CONTRATADA for reincidente;

b) Em 1/2 (um meio), se a falta da CONTRATADA tiver produzido prejuízos relevantes para o BANPARÁ.

13.3.2 As penas bases definidas neste subitem devem ser atenuadas nos seguintes casos:

a) Em 1/4 (um quarto), se a CONTRATADA não for reincidente;

b) Em 1/4 (um quarto), se a falta da CONTRATADA não tiver produzido prejuízos relevantes para o BANPARÁ;

c) em 1/4 (um quarto), se a CONTRATADA tiver reconhecido a falta e se

dispuser a tomar medidas para corrigi-la; e

d) em 1/4 (um quarto), se a CONTRATADA comprovar a existência e a eficácia de procedimentos internos de integridade, de acordo com os requisitos do artigo 42 do Decreto n. 8.420/2015.

13.3.3 Na hipótese deste subitem, se não caracterizada má-fé ou intenção desonesta e se a CONTRATADA contemplar os requisitos para as atenuantes previstos nas alíneas acima, a pena de suspensão deve ser substituída pela de advertência, prevista no inciso I do artigo 83 da Lei n. 13.303/2016.

13.4 A CONTRATADA, para além de hipóteses previstas no presente contrato e no Termo de Referência, estará sujeita à multa:

a) De mora, por atrasos não justificados no prazo de execução de 0,2% (dois décimos por cento) do valor da parcela do objeto contratual em atraso, por dia de atraso, limitada a 5% (cinco por cento) do valor do contrato.

b) Compensatória, pelo descumprimento total do contrato, no montante de até 5% (cinco por cento) do valor do contrato.

b.1) se houver inadimplemento parcial do contrato, o percentual de até 5% deve ser apurado em razão da obrigação inadimplida.

13.4.1 Se a multa moratória alcançar o seu limite e a mora não se cessar, o contrato pode ser rescindido, salvo decisão em contrário, devidamente motivada, do gestor do contrato.

13.4.2 Acaso a multa não cubra os prejuízos causados pela CONTRATADA, o BANPARÁ pode exigir indenização suplementar, valendo a multa como mínimo de indenização, na forma do preceituado no parágrafo único do artigo 416 do Código Civil Brasileiro.

13.4.3 A multa aplicada pode ser descontada da garantia, dos pagamentos devidos à CONTRATADA em razão do contrato em que houve a aplicação da multa ou de eventual outro contrato havido entre o BANPARÁ e a CONTRATADA, aplicando-se a compensação prevista nos artigos 368 e seguintes do Código Civil Brasileiro.

14 CLÁUSULA DÉCIMA QUARTA – RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANPARÁ

14.1 Com fundamento no artigo 5º da Lei n. 12.846/2013, constituem atos lesivos ao BANPARÁ 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;

d) Manipular ou fraudar o equilíbrio econômico-financeiro deste contrato;

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, Lei n. 8.666/1993, 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 BANPARÁ, 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 do Contratado ou, na sua falta, em publicação de circulação nacional;

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

c) No sítio eletrônico do Contratado, 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 BANPARÁ será apurada e apenada em Processo Administrativo de Responsabilização (PAR), instaurado pelo Diretor Presidente do BANPARÁ e conduzido por comissão composta por 2 (dois) servidores designados.

14.3.1 Na apuração do ato lesivo e na dosimetria da sanção eventualmente aplicada, o BANPARÁ 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. 8.666/1993, 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 do Estado do Pará.

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 BANPARÁ resultantes de ato lesivo cometido pelo licitante, 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.

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 subitem se aplicam quando o licitante 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 BANPARÁ. Para os efeitos desta Cláusula, deve ser formulada a solicitação, por escrito, ao BANPARÁ, informando todos os pormenores da intenção da CONTRATADA, reservando-se, ao BANPARÁ, o direito de aceitar ou não o pedido, no todo ou em parte.

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 na Política de Controles Internos e Compliance do BANPARÁ e no Código de Ética e de Conduta Institucional do BANPARÁ, cuja íntegra esta disponibilizada no *site* do BANPARÁ (www.banpara.b.br), bem como no termo de compromisso que integra o presente contrato.

16.2 O BANPARÁ 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 BANPARÁ dentro de 5 (cinco) dias a contar de sua solicitação.

17 CLÁUSULA DÉCIMA SETIMA – DAS CLÁUSULAS DE TRATAMENTO DE DADOS

17.1. O CONTRATANTE, denominado **CONTROLADOR DE DADOS** e a CONTRATADA, ora **OPERADOR DE DADOS**, concordam com o seguinte:

Definições

Para fins de cláusulas, serão utilizadas as definições conforme disposto na Lei Geral de Proteção de Dados, Lei Nº 13.709/2018, no artigo 5º e seus incisos:

a) Dados pessoais é toda informação relacionada a pessoa natural identificada ou identificável;

b) Dados pessoais sensíveis é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

c) Titular de dados é toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

d) Controlador é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

e) Operador é toda pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

f) Encarregado é pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

g) Tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

17.2. Escopo/Objeto

Este Contrato de processamento de dados se aplica exclusivamente ao processamento de dados pessoais que está sujeito à Lei Geral de Proteção de Dados (LGPD) entre as partes, durante a vigência do contrato para a prestação dos serviços de atendimento técnicos para resolução de problemas.

Os dados pessoais dos clientes tratados no âmbito desde processo se limitam a: **nome dos clientes, endereço, dados bancários internacionais: código IBAN, identificação do banco e da conta no exterior.**

Os dados pessoais serão tratados apenas para as finalidades deste contrato, quais sejam, prestação do serviço de consultoria externa para avaliação de risco de segurança da informação para o processo de transferências financeiras internacionais utilizando o sistema SWIFT, onde será avaliado controles de segurança e infraestrutura.

17.3. Responsabilidades

O **CONTROLADOR DE DADOS** irá determinar o escopo, o propósito e a maneira pela qual os dados pessoais podem ser tratados pelo **OPERADOR** e este processará os dados pessoais apenas conforme o estabelecido nas instruções escritas pelo **CONTROLADOR DE DADOS**.

O **OPERADOR DE DADOS** processará os dados pessoais somente sob as instruções documentadas do **CONTROLADOR**, de maneira que – e na medida em que – seja apropriado para a prestação dos serviços, exceto quando necessário para cumprir uma obrigação legal. Nesse caso, o **OPERADOR** deverá informar ao

CONTROLADOR dessa obrigação legal antes de realizar o processamento, a menos que essa obrigação legal proíba o fornecimento de tais informações ao **CONTROLADOR**.

O **OPERADOR DE DADOS** nunca deverá processar os dados pessoais de maneira inconsistente com as instruções documentadas pelo **CONTROLADOR**.

O **OPERADOR DE DADOS** deverá informar imediatamente ao **CONTROLADOR** se verificar ou houver suspeita de que uma instrução infrinja a Lei Geral de Proteção de Dados ou outras disposições de proteção de dados do país ou regulamentos/tratados internacionais.

O **OPERADOR DE DADOS** deverá fornecer ao **CONTROLADOR DE DADOS** a documentação relevante, por exemplo, sua política de privacidade, política de gerenciamento de registros, código de conduta aprovado (quando disponível), política de segurança da informação, plano de continuidade de negócio, documentação com regras para tratamento de dados sensíveis, tanto para transporte como repouso, além do relatório de incidentes de cada semestre. Toda a documentação deverá ser realizada anualmente, no mínimo, e deverá ser entregue em até 15 (quinze) dias após a assinatura do contrato.

O **OPERADOR** também deverá fornecer a estrutura de log transacional e de auditoria de sistemas e de redes, relatório de teste de intrusão do sistema/ativo rede cabeada/sem fio; documentação que informe a segurança e requisitos conforme ISO 27001 em relação ao seu Data Center, bem como Nuvem, caso operem; documentação da adequação do sistema para LGPD; relatório que atende aos requisitos de segurança conforme normativo interno de desenvolvimento seguro e normas de requisitos de segurança para controle de acesso e auditoria nos sistemas corporativos; documentação sobre segurança da arquitetura do sistema, bem como segurança no transporte dos dados do sistema na DMZ, se houver, e internamente dentro da estrutura de Data Center; aderência as políticas de segurança da informação e segurança cibernética, tal como os seus desdobramentos em normativos internos institucionalizados.

Caso o **OPERADOR DE DADOS** venha a executar tratamento diferente daquele definido pelo **CONTROLADOR DE DADOS**, de maneira a decidir a finalidade e os meios de tratamento, será alçado à condição de **CONTROLADOR** e terá as mesmas responsabilidades.

17.4 Confidencialidade

Sem prejuízo de quaisquer acordos contratuais existentes entre as Partes, o **OPERADOR DE DADOS** tratará todos os dados pessoais como estritamente confidenciais e informará todos os seus funcionários, agentes e/ou suboperadores aprovados [se permitido] envolvidos no processamento de dados pessoais de natureza confidencial.

O **OPERADOR** deverá garantir que todas essas pessoas ou partes tenham assinado um contrato de confidencialidade apropriado e estejam de outra forma vinculadas a um dever de confidencialidade ou estejam sob uma obrigação estatutária apropriada de confidencialidade. A qualquer momento o **CONTROLADOR** poderá solicitar a prestação de contas sobre tal ato.

O **OPERADOR** deverá garantir que as informações confidenciais deverão ser utilizadas apenas para os propósitos do Contrato Nº <nº do contrato>, e que serão divulgadas apenas para seus Diretores, Sócios, Administradores, Empregados, Prestadores de Serviço, Preposto ou quaisquer representantes, respeitando o princípio do privilégio mínimo, com a devida classificação de informação, conforme disposto na ISO/IEC 27002:2005 (ABNT NBR).

O **OPERADOR** não poderá divulgar, publicar ou de qualquer forma revelar qualquer informação **CONFIDENCIAL, RESTRITA, SENSÍVEL** ou **INTERNA** recebida através do **CONTROLADOR** para qualquer pessoa física ou jurídica, de direito público ou privado, sem a prévia autorização escrita do **CONTROLADOR**.

Quaisquer informações relativas ao presente contrato de **TRATAMENTO DE DADOS** somente poderão ser dadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, mediante requisição por escrito a ser encaminhada para avaliação do **CONTROLADOR**, informando todas as minúcias da intenção do **OPERADOR**, reservando-se ao **CONTROLADOR** o direito de deferir ou não o pedido, no todo ou em parte.

O **CONTROLADOR** poderá solicitar ao OPERADOR, a qualquer momento, o retorno de todas as **INFORMAÇÕES SIGILOSAS** recebidas pelo **OPERADOR** de forma escrita ou tangível, incluindo cópias, reproduções ou outra mídia contendo tais informações, dentro de um período máximo de 10 (dez) dias a contar da formalização do pedido.

O **OPERADOR** deverá dar ciência das referidas cláusula a todos os seus sócios, empregados, prestadores de serviço, prepostos ou quaisquer representantes que

participarão do tratamento de dados descritos no contrato e que venham a ter acesso a quaisquer dados e informações **CONFIDENCIAIS, RESTRITAS, SENSÍVEIS** ou **INTERNA** do **CONTROLADOR** para que cumpram as obrigações constantes neste documento e que será **responsável solidariamente por eventuais descumprimentos das cláusulas descritas neste instrumento contratual**.

Entende-se por informação sigilosa os dados, informações e conhecimentos, orais ou escritos, por cada uma das PARTES, assim como os conhecimentos adquiridos no decorrer do CONTRATO por qualquer das PARTES, especialmente aqueles decorrentes de pesquisas, do desenvolvimento comercial de quaisquer produtos e serviços não anunciados, invenções, planos e processos internos de negócio e informações financeiras. Tais documentos e informações não se limitam, mas poderão constar de dados digitais, desenhos, relatórios, estudos, materiais, produtos, tecnologia, programas de computador, especificações, manuais e outras informações submetidas oralmente, por escrito ou qualquer outro tipo de mídia.

17.5. Segurança

Levando em consideração o estado da arte, os custos de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como o risco de probabilidades e severidade variáveis dos direitos e liberdades das pessoas físicas, sem prejuízo de outras normas de segurança agredido pelas Partes, o **CONTROLADOR** e o **OPERADOR** devem implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança no processamento de dados pessoais apropriado ao risco.

Essas medidas devem procurar garantir que:

- Os dados podem ser acessados, alterados, divulgados ou excluídos apenas com autorização do **CONTROLADOR**;
- Os dados permaneçam precisos e completos em relação à finalidade pela qual estão sendo tratados;
- Os dados permaneçam acessíveis e utilizáveis, ou seja, se os dados pessoais forem acidentalmente perdidos, alterados ou destruídos, deverá ser garantida a recuperação dos mesmos, evitando qualquer dano às partes envolvidas.

O **OPERADOR** deverá realizar testes de penetração e varredura de vulnerabilidades de forma regular. Os testes deverão ter seus resultados documentados e

apresentados ao **CONTROLADOR**. A periodicidade dos testes será definida pelo **CONTROLADOR**. Caso os testes evidenciem algum tipo de vulnerabilidade, caberá ao **OPERADOR** implementar as salvaguardas apropriadas e evidenciá-las ao **CONTROLADOR**.

O **OPERADOR** deverá apresentar, sempre que solicitado pelo **CONTROLADOR**, evidências de que o ambiente de realização dos serviços contratados possui o grau de segurança necessário para garantir o sigilo das informações a ela confiadas.

Os produtos gerados pelo **OPERADOR** deverão respeitar todos os padrões de segurança estabelecidos pelo **CONTROLADOR**.

O OPERADOR deverá comprovar controles de segurança da informação nas quais estipula melhores práticas, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. Sendo obrigatório os seguintes controles até 60 (sessenta) dias da contratação para validação. Em caso de não validação de alguma documentação apresentada a mesma deve ser corrigida em até 30 (trinta) dias:

• Política de Segurança da Informação;
• Organização da Segurança da Informação;
• Gestão de ativos;
• Segurança em recursos humanos;
• Segurança física e lógica do ambiente;
• Segurança das operações e comunicações;
• Controle de acesso e rastreabilidade/irretratabilidade;
• Aquisição, desenvolvimento e manutenção de sistemas;
• Gestão de incidentes de segurança da informação;
• Gestão da continuidade do negócio; e
• Conformidade.

O **OPERADOR** deverá encaminhar ao **CONTROLADOR** um documento com recomendações para gerenciamento de riscos de segurança da informação, assim como de segurança cibernética enfrentados e tratados pela organização com, no mínimo, atualização anual.

O OPERADOR, na forma aqui representada, declara ciência quanto às disposições da Política de Segurança Cibernética e de Segurança da Informação do

CONTROLADOR, e de suas respectivas atualizações, além de documentos correlatos, conforme aplicável, a ser(em), a critério do CONTROLADOR comprometendo-se em cumpri-la(os) e fazê-la(os) cumprir por seus empregados e prepostos, em especial, mas não se limitando a, acerca dos controles e procedimentos voltados à prevenção e ao tratamento de incidentes, a serem adotados pelo OPERADOR, observadas as políticas de Segurança Cibernética, Segurança da Informação e Privacidade do CONTROLADOR.

Poderá o CONTROLADOR solicitar, a qualquer tempo, evidências que demonstrem as medidas tomadas pelo OPERADOR, a fim de atender as Políticas de Segurança Cibernética assim como de Segurança da Informação e providências correlatas mencionadas neste Contrato.

17.6. Compartilhamento e Transferência

O **OPERADOR** deverá notificar de forma imediata ao **CONTROLADOR** que quaisquer transferências permanentes ou temporárias (planejadas) de dados pessoais para um país fora do Brasil sem um nível adequado de proteção e somente deverá realizar essa transferência (planejada) após obter a autorização do **CONTROLADOR**, que poderá recusar a seu próprio critério.

O **OPERADOR** deverá se utilizar de criptografia para realizar a transferência de dados pessoais, de modo a fornecer proteção eficaz contra a interceptação da comunicação por terceiros enquanto os dados estiverem em transferência, seja ela realizada pela Internet, por uma rede de comunicação sem fio ou quando os dados passarem por uma rede não confiável.

O **OPERADOR**, ao transmitir dados pessoais pela Internet, particularmente dados pessoais sensíveis, deverá usar um protocolo de comunicação criptografado apropriado (por exemplo, TLS versões 1.2 ou superior), além de seguir as instruções e autorização do **CONTROLADOR**, a fim de cumprir suas obrigações com base no Contrato de Serviços, jamais para qualquer outro propósito.

17.7. Obrigações em Caso de Incidente

Quando o **OPERADOR** tomar conhecimento de um incidente que afeta o processamento dos dados pessoais que está sujeito ao Contrato de Serviços, deverá notificar imediatamente ao **CONTROLADOR** sobre o mesmo, sem demora injustificada, devendo sempre cooperar com o **CONTROLADOR** e seguir as suas

instruções em relação a esses incidentes, a fim de permitir que o **CONTROLADOR** realize uma investigação completa sobre o incidente, formule uma resposta correta e tome as medidas adequadas a respeito do incidente.

O **OPERADOR** deverá correlacionar riscos/vulnerabilidades mitigados com os incidentes referentes a segurança da informação e cibernética ocorridos no ambiente do **CONTROLADOR**, encaminhando relatório mensal para controle de possíveis incidentes envolvendo violação e dados pessoais do **CONTROLADOR**.

Ao relatar uma violação, o **OPERADOR** deverá fornecer ao **CONTROLADOR**:

- Uma descrição da natureza da violação de dados pessoais, incluindo, sempre que possível as categorias e o número aproximado de titulares de dados em causa e as categorias e o número aproximado de registros de dados pessoais em questão;
- O nome e os detalhes de contato do responsável pela proteção de dados ou outro ponto de contato onde mais informações possam ser obtidas;
- Uma descrição das prováveis consequências da violação de dados pessoais;
- Uma descrição das medidas adotadas, ou propostas a serem adotadas, para lidar com a violação de dados pessoais, incluindo, se for o caso, as medidas adotadas para mitigar possíveis efeitos adversos.

17.8. Subcontratações

O **OPERADOR** não deverá subcontratar para nenhuma de suas atividades relacionados ao serviço que consistam, mesmo que parcialmente, no processamento de dados pessoais ou na exigência de que os dados pessoais sejam processados por terceiros sem a autorização prévia por escrito do **CONTROLADOR**.

17.9. Devolução ou Descarte dos Dados

Após a rescisão deste Contrato de Tratamento de Dados, mediante solicitação por escrito do **CONTROLADOR** ou após o cumprimento de todos os propósitos acordados no contexto dos Serviços, nos quais nenhum processamento adicional é necessário, o **OPERADOR** deverá, a critério do **CONTROLADOR**, excluir, destruir ou devolver todos os dados pessoais ao **CONTROLADOR** e destruir ou devolver quaisquer cópias existentes, a menos que exista alguma obrigação legal que exija que os dados pessoais permaneçam armazenados.

Os dados deverão ser restituídos pelo **OPERADOR** juntamente com o dicionário de dados que permita entender a organização do banco de dados, em até 30 (trinta) dias ou em eventual prazo acordado entre as Partes. Após esse procedimento de volta dos dados do CONTROLADOR com integridade e disponibilidade que após essa confirmação os dados serão destruídos os documentos em formato digital, segundo a norma DoD 5220.22-M (ECE) ou o método descrito por Peter Gutmman no artigo "Secure Deletion of Data From Magnetic and Solid-State Memory" ou através da utilização de desmagnetizadores (degausser).

O **OPERADOR** deverá notificar todos os terceiros que apoiam seu próprio processamento dos dados pessoais da rescisão do Contrato de Tratamento de Dados e deverá garantir que todos esses terceiros destruam os dados pessoais ou devolvam os dados pessoais ao **CONTROLADOR**, no critério definido por este.

O **OPERADOR** deverá emitir documento para o **CONTROLADOR** ratificando que todos os dados pessoais foram devolvidos ou descartados. Todas as atividades de devolução ou descarte de dados não devem gerar ônus ao **CONTROLADOR**.

Todos os dados contidos no banco de dados são de propriedade do **CONTROLADOR**.

17.10. Assistência ao Outro Agente

O **OPERADOR** deverá auxiliar o **CONTROLADOR** por medidas técnicas e organizacionais apropriadas, na medida do possível, para o cumprimento da obrigação do **CONTROLADOR** de responder à solicitação de exercício dos direitos dos titulares de dados sobre a Lei Geral de Proteção de Dados, como solicitações de acesso, solicitações de retificação ou descarte de dados pessoais e objeções ao tratamento.

O **OPERADOR** deverá auxiliar o **CONTROLADOR** a garantir o cumprimento das obrigações previstas nas cláusulas de Segurança e nas consultas realizadas pela Autoridade Nacional de Proteção de Dados, levando em consideração a natureza do processamento e as informações disponíveis para o **OPERADOR**.

O **OPERADOR** deverá cumprir com as suas obrigações de manter os dados pessoais seguros, notificar violações de dados pessoais ao **CONTROLADOR**, notificar violações de dados pessoais aos Titulares de Dados, realizar avaliações de impacto na proteção de dados pessoais (DPIAs) quando necessário ou solicitado e consultar

o **CONTROLADOR** quando um DPIA indicar que existe um alto risco que não poderá ser mitigado.

17.11. Responsabilidade e Regresso

O **OPERADOR** deverá indenizar o **CONTROLADOR** e o isentar de todas as reivindicações, ações, reivindicações de terceiros, perdas, danos e despesas incorridas pelo **CONTROLADOR** e decorrentes, direta ou indiretamente, de ou em conexão com uma violação deste Contrato de Tratamento de Dados e/ou a Lei Geral de Proteção de Dados Aplicável pelo **OPERADOR**.

O **OPERADOR** deverá notificar o **CONTROLADOR** sobre as reclamações e solicitações que os titulares de dados (por exemplo, sobre a correção, exclusão, complementação e bloqueio de dados) e sobre as ordens de tribunais, autoridades públicas e reguladores competentes e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo.

Fica assegurado ao **CONTROLADOR**, nos termos da lei, o direito de regresso em face do **OPERADOR** diante de eventuais danos causados por este em decorrência do descumprimento das obrigações aqui assumidas em relação à Proteção de Dados.

17.12. Auditorias e Diligências

O **OPERADOR** deverá fornecer ao **CONTROLADOR** todas as informações necessárias para demonstrar o cumprimento das medidas técnicas de proteção de dados pessoais.

O **OPERADOR** deverá permitir e contribuir para auditorias e diligências realizadas pelo **CONTROLADOR** ou por um auditor nomeado por este. Os métodos usados para monitorar a conformidade e a frequência do monitoramento dependerão das circunstâncias do processamento e serão definidas pelo **CONTROLADOR**.

O **CONTROLADOR** deverá avaliar se o **OPERADOR** possui conhecimento técnico suficiente para auxiliar no cumprimento de obrigações previstas na Lei Geral de Proteção de Dados, como medidas técnicas, notificações de violações e DPIAs.

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

que estejam em poder do OPERADOR tanto para auditoria interna do CONTROLADOR como para órgão regulados desse parceiro.

17.13 Propriedades dos dados em geral

O presente Contrato não transfere a propriedade dos dados do **CONTROLADOR** ou dos clientes desta para o **OPERADOR**. Os dados gerados, obtidos ou coletados a partir da prestação dos serviços ora contratados são de propriedade do **CONTROLADOR**.

O **CONTROLADOR** é o exclusivo titular dos direitos de propriedade intelectual sobre qualquer novo elemento de dados, produto ou subproduto que seja criado a partir do tratamento de dados estabelecido por este Contrato, quando houver.

O **CONTROLADOR** não autoriza o **OPERADOR** 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 etabelecido por este Contrato.

17.14 Prazos e Vigência

As cláusulas de Tratamento de Dados entram em vigor na data da assinatura do Contrato.

A rescisão ou expiração deste Contrato de Tratamento de Dados não exonera o **OPERADOR** de suas obrigações de confidencialidade, de acordo com as cláusulas de Confidencialidade.

O **OPERADOR** deverá processar os dados pessoais até a data de rescisão do contrato, a menos que instruído de outra forma pelo **CONTROLADOR**, ou até que esses dados sejam retornados ou destruídos por instrução do **CONTROLADOR**.

O OPERADOR aceita um prazo de 30 (trinta) dias para solicitação de interrupção do serviço pelo CONTROLADOR.

No caso de qualquer tipo de inconsistência entre as disposições deste Contrato de Tratamento de Dados e as disposições do Contrato de Serviço, as disposições deste Contrato de Tratamento de Dados prevalecerão.

18 CLÁUSULA DÉCIMA OITAVA – FORO

18.1 As partes contratantes elegem o foro da Comarca de Belém, Estado do Pará, para a solução de qualquer questão oriunda do presente contrato, com exclusão de qualquer outro.

E, por estarem justas e contratadas, as partes assinam o presente instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo, para que produzam os efeitos legais, por si e seus sucessores.

....., ... de .....de .....

Pelo BANPARÁ:

.....	.....
Diretor Presidente	Diretor .....

Pela CONTRATADA:

.....

Nome :

CPF.:

Cargo:

Testemunhas:

1ª.....	2ª.....
Nome:	Nome:
CPF:	CPF:

ADENDO 4 AO CONTRATO
TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO

Por este instrumento particular, a CONTRATADA compromete-se a cumprir integralmente as disposições da Políticas de Controles Internos e de Compliance do BANPARÁ, 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", (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:
    i. 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 BANPARÁ ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro;
    ii. assegurar vantagem imprópria;
    iii. 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 BANPARÁ ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro; ou

iv. 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 BANPARÁ ou seus negócios, se obrigam a:

a) permanecer em inteira conformidade com as Leis Anticorrupção, e qualquer legislação antissuborno, anticorrupção e de conflito de interesses aplicável, ou qualquer outra legislação, regra ou regulamento de propósito e efeito similares, abstendo-se de qualquer conduta que possa ser proibida a pessoas sujeitas às Leis Anticorrupção;
b) tomar todas as precauções necessárias visando prevenir ou impedir qualquer incompatibilidade ou conflito com outros serviços ou com interesses do BANPARÁ, o que inclui o dever de comunicar as relações de parentesco existentes entre os colaboradores da CONTRATADA e do BANPARÁ; e
c) observar, no que for aplicável, o Código de Ética e de Condutas Institucionais do BANPARÁ, 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 BANPARÁ 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.

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 BANPARÁ, por meio do Canal de Denúncias .....

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

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

.....
(Local e Data)

.....
(Representante legal)

ANEXO I
SEGURANÇA DA INFORMAÇÃO

Garantir os seguintes itens conforme MNP de Segurança para Sistemas Corporativos em especial os listados a seguir:
4.8. Para versão web deve protocolo https e usar SSL (TSL 1.2) no servidor e também rodar o certificado SSL para comunicação
4.9. Não permitir que senha copiada ou que esteja na área de transferência seja colada no campo senha para fazer login.
4.10. Senha dos usuários de sistema não deve trafegar limpa nas chamadas, seja ela da forma que for. Assim como não devem ser armazenadas sem criptografia.
4.11. Permitir expiração de telas apresentando ao usuário uma mensagem de expiração e realizando esta operação caso o usuário se ausente por um período parametrizável. Após expirar telas para acessar o sistema o usuário deverá fazer logon novamente.
4.12. Permitir que somente usuários credenciados configurem seu funcionamento da melhor maneira que convier ao Banpará

Garantir que atende as melhores práticas de desenvolvimento seguro conforme elencado a seguir assim como MNP de Desenvolvimento Seguro:
1.1. Validação dos dados de Entrada / Saída
1.1.1. Efetuar toda a validação dos dados em um sistema confiável, centralizado no servidor/aplicação;
1.1.2. Identificar todas as fontes de dados e classificá-las como sendo confiáveis ou não. Em seguida, validar os dados provenientes de fontes nas quais não se possa confiar (ex: base de dados, stream de arquivos etc.)
1.1.3. Especificar o conjunto de caracteres apropriado (ex: UTF-8) e determinar se o sistema suporta essa codificação, validando se os dados recebidos estão realmente neste formato;
1.1.4. Quando ocorrer falha na validação dos dados, a aplicação deve rejeitar as informações e impedir o prosseguimento das atividades;
1.1.5. Validar todos os dados provenientes de redirecionamento ou inseridos por clientes antes do processamento, incluindo parâmetros, campos de formulário, conteúdo e cabeçalhos. Certificar-se ainda de incluir mecanismos automáticos de postback nos blocos de código JavaScript, Flash ou qualquer outra estrutura embutida;
1.1.6. Verificar se os valores de cabeçalho, tanto das requisições, como das respostas, contêm apenas caracteres ASCII
1.1.7. Quando na integração com outros sistemas, utilizar preferencialmente API's que executem tarefas específicas para função desejada. Deve-se evitar que a aplicação execute comandos diretamente no sistema operacional, especialmente através da utilização de shells;
1.1.8. Validar, sempre que possível, todos os dados de entrada através de um método baseado em "listas brancas" que utilizem uma lista de caracteres ou expressões regulares com os caracteres permitidos. Em geral: a-z (inclusive acentuados), A-Z (inclusive acentuados), 0-9;
1.1.9. Se qualquer caractere potencialmente perigoso precisa ser permitido na entrada de dados da aplicação – como campos de senha, por exemplo – certificar-se de que foram implementados controles adicionais como a codificação dos dados de

saída. Como exemplo de caracteres potencialmente “perigosos”, temos: ' " < > ./ \ - | ( ) ;
1.1.10. Incluir a verificação das seguintes entradas para a validação dos dados: bytes nulos (%00), caracteres de nova linha (%0d, %0a, \r, \n) e caracteres “ponto-ponto barra” (../ ou ..\);
1.1.11. A “canonicalização” deve ser utilizada para resolver problemas de codificação dupla (double encoding) ou ataques por ofuscação;
1.1.12. Um computador é capaz de interpretar diversas formas de representação para um mesmo caractere, tais como: DECIMAL, HEXADECIMAL, OCTAL, HTML/UNICODE e BINÁRIO. Por esse motivo, considerar filtros e proteções em variadas formatações. Para mais informações, vide ANEXO I – REPRESENTAÇÃO DE CARACTERES ESPECIAIS.
1.1.13. Dentro do modelo MVC (Model View Controler) utilizar a validação através do serviço de controle ao invés de deixar a regra na camada de Visão ou Interface.

1.2. Gerenciamento de Arquivos
1.2.1. Solicitar autenticação antes de permitir que seja feito o upload de arquivos;
1.2.2. Limitar os tipos de arquivos que podem ser enviados para aceitar somente os tipos necessários ao propósito do negócio (trabalhar com o modelo de white list). Validar os arquivos através da verificação dos cabeçalhos, uma vez que extensões de arquivos são facilmente modificadas;
1.2.3. Não salvar arquivos no mesmo diretório de contexto da aplicação, principalmente se esta for web. Preferencialmente, utilizar servidores de conteúdo ou bases de dados específicas;
1.2.4. Nos diretórios onde serão recebidos arquivos de upload, desativar privilégios de execução de binários, scripts ou arquivos de linguagens específicas, tais como: ASP, PHP, Perl, etc.
1.2.5. Não enviar caminhos de diretórios ou de arquivos em requisições. Utilizar mecanismos de mapeamento desses recursos para índices definidos em uma lista pré-definida de caminhos;
1.2.6. Nunca devolver o caminho absoluto do arquivo para o cliente da aplicação ou usuário final;
1.2.7. Quando necessário referenciar outros aplicativos, não utilizar nome relativos e sim o caminho absoluto do sistema. Por exemplo, ao invés de regedit.exe, utilizar %systemroot%\regedit.exe;
1.2.8. Ao realizar chamadas de outros aplicativos, utilizar mecanismos de verificação de integridade por checksum ou hash.

1.3. Gerenciamento de Memória
1.3.1. Instanciar explicitamente todas as variáveis e dados persistentes durante a declaração, ou antes da primeira utilização;
1.3.2. Ao usar funções que aceitem determinado número de bytes para realizar cópias (ex.: strncpy()), verificar se o tamanho do buffer de destino é igual ao tamanho do buffer de origem. Neste caso, ele não pode encerrar a sequência de caracteres com valor nulo (null);
1.3.3. Verificar os limites do buffer caso as chamadas à função sejam realizadas em ciclos (loop) e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado;

1.3.4. Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação;
1.3.5. Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo, dentre outros, não contar exclusivamente com o “garbage collector” e realizar a tarefa de liberação de memória explicitamente;
1.3.6. Atentar para as discrepâncias de tamanho de byte, precisão, distinções de sinal (signed/unsigned), truncamento, conversão de variáveis (type casting), cálculos que devolvam erros do tipo not-a-number e representação interna de números muito grandes ou pequenos;
1.3.7. Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos os pontos de saída.

1.4. Controle de Acessos
1.4.1. Utilizar um único componente para realizar o processo de verificação de autorização de acesso. Isto inclui bibliotecas que invocam os serviços externos de autorização. Caso a aplicação não seja possível às configurações de segurança, negar todos os acessos;
1.4.2. Garantir o controle de autorização em todas as requisições, inclusive em scripts do lado servidor, "includes" e requisições do lado cliente, tais como: AJAX, Flash, etc; dessa forma se requer autenticação para todas as páginas e recursos.
1.4.3. Isolar do código da aplicação os trechos de código que contêm lógica privilegiada, isto é, com permissões exclusivas;
1.4.4. Quando a aplicação tiver que ser executada com privilégios elevados, realizar esta atividade o mais tarde possível e revogá-los logo que seja possível;
1.4.5. Proteger variáveis compartilhadas e os recursos contra acessos concorrentes inapropriados;
1.4.6. Restringir o acesso somente aos usuários autorizados de URLs, funções protegidas, serviços e dados da aplicação (atributos e campos), referências diretas e configurações de segurança, incluindo definições do servidor, arquivos de configuração e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação;
1.4.7. Não incluir credenciais diretamente no código-fonte. Adicionalmente, utilizar ofuscação de código para a proteção de dados sensíveis, tais como consultas SQL (PROTEÇÃO CONTRA ENGENHARIA REVERSA)
1.4.8. As regras de controle de acesso representadas pela camada de apresentação devem coincidir com as regras presentes no lado servidor;
1.4.9. Caso seja necessário armazenar o estado dos dados no lado cliente, utilizar mecanismos de criptografia e verificação para detectar possíveis alterações;
1.4.10. Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo;
1.4.11. Não utilizar os campos de cabeçalho (por exemplo: referer, user-agent, cookie, etc) individualmente como forma de validação de autorização. Estes devem ser utilizados sempre em conjunto com outros recursos;
1.4.12. Isolar do código da aplicação os trechos de código que contêm lógica privilegiada
1.4.13. Restringir o acesso aos arquivos e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação, somente aos usuários autorizados
1.4.14. Restringir o acesso às URLs protegidas somente aos usuários autorizados

1.4.15. Restringir o acesso às funções protegidas somente aos usuários autorizados
1.4.16. Restringir o acesso às referências diretas aos objetos somente aos usuários autorizados
1.4.17. Restringir o acesso aos serviços somente aos usuários autorizados
1.4.18. Restringir o acesso aos dados da aplicação somente aos usuários autorizados
1.4.19. Restringir o acesso aos atributos e dados dos usuários, bem como informações das políticas usadas pelos mecanismos de controle de acesso
1.4.20. Restringir o acesso às configurações de segurança relevantes apenas aos usuários autorizados
1.4.21. Se for permitida a existência de sessões autenticadas por longos períodos de tempo, fazer a revalidação periódica da autorização do usuário para garantir que os privilégios não foram modificados e, caso tenham sido, realizar o registro em log do usuário e exigir nova autenticação.
1.4.22. Separar a lógica de autenticação do recurso que está a ser requisitado e usar redirecionadores dos controladores de autenticação centralizados
1.4.23. Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial
1.4.24. As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como “Nome de usuário incorreto” ou “Senha incorreta”, utilize apenas mensagens como: “Usuário e/ou senha inválidos”, para ambos os casos de erro. As respostas de erro devem ser idênticas nos dois casos.
1.4.25. Utilizar autenticação para conexão a sistemas externos que envolvam tráfego de informação sensível ou acesso a funções
1.4.26. As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em um local protegido de um sistema confiável, por exemplo, no servidor da aplicação.
Obs.: o código-fonte não é considerado um local seguro
1.4.27. Utilizar apenas requisições POST para transmitir credenciais de autenticação
1.4.28. Somente trafegar senhas (não temporárias) através de uma conexão protegida (SSL/TLS) ou no formato de dado cifrado, como no caso de envio de e-mail cifrado. Senhas temporárias enviadas por e-mail podem ser um caso de exceção aceitável
1.4.29. A entrada da senha deve ser ocultada na tela do usuário. Em HTML, utilizar o campo do tipo "password"
1.4.30. Notificar o usuário quando a senha for reiniciada (reset)
1.4.31. Desativar a funcionalidade de lembrar a senha nos campos de senha do navegador
1.4.32. A data/hora da última utilização (bem ou mal sucedida) de uma conta de usuário deve ser comunicada no próximo acesso ao sistema
1.4.33. Realizar monitoramento para identificar ataques contra várias contas de usuários, utilizando a mesma senha. Esse padrão de ataque é utilizado para explorar o uso de senhas padrão
1.4.34. Utilizar autenticação de múltiplos fatores (utilizando simultaneamente token, senha, biometria etc.5) via multifatorial
1.4.35. Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo (parametrizável).

1.4.36. Utilizar o campo “referer” do cabeçalho somente como forma de verificação suplementar. O mesmo não deve ser usado sozinho como forma de validação de autorização porque ele pode ter o valor adulterado
1.4.37. Implementar a auditoria das contas de usuário e assegurar a desativação de contas não utilizadas. A aplicação deve dar suporte à desativação de contas e ao encerramento das sessões quando terminar a autorização do usuário.
1.4.38. . As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos não podem efetuar autenticação no sistema

1.5. Gerenciamento de sessões e comunicações
1.5.1. Utilizar controles de gerenciamento de sessão baseados no servidor ou em framework confiável. A aplicação deve reconhecer apenas esses identificadores de sessão como válidos;
1.5.2. O controle de gestão de sessão deve usar algoritmos conhecidos, padronizados e bem testados que garantam a aleatoriedade dos identificadores de sessão.
1.5.3. Definir o domínio e o caminho para os cookies que contenham identificadores de sessão autenticados, para um valor devidamente restrito ao site;
1.5.4. A funcionalidade de saída (logout) necessita estar disponível em todas as páginas que requerem autenticação e deve encerrar completamente a sessão ou conexão associada. Adicionalmente, não permitir logins persistentes (sem prazo de expiração);
1.5.5. Estabelecer um tempo de expiração baseado nos riscos e requisitos funcionais do negócio;
1.5.6. Não permitir logins persistentes (sem prazo de expiração) e realizar o encerramento da sessão periodicamente, mesmo quando ela estiver ativa. Isso deve ser feito, especialmente, em aplicações que suportam várias conexões de rede ou que se conectam a sistemas críticos. O tempo de encerramento deve estar de acordo com os requisitos do negócio e o usuário deve receber notificações suficientes para atenuar os impactos negativos dessa medida
1.5.7. Se uma sessão estava estabelecida antes do login, ela deve ser encerrada (gerando um novo identificador de sessão) para que uma nova seja estabelecida;
1.5.8. Não permitir conexões simultâneas com o mesmo identificador de usuário;
1.5.9. Não expor os identificadores de sessão em URLs, mensagens de erro ou logs. Os identificadores de sessão devem apenas ser encontrados no cabeçalho do cookie HTTP. Por exemplo, não trafegar os identificadores de sessão sob a forma de parâmetros GET;
1.5.10. Gerar um novo identificador de sessão caso a segurança da conexão mude de HTTP para HTTPS. Uilizar HTTPS de forma constante em vez de alternar entre HTTP e HTTPS
1.5.11. Configurar o atributo “secure” para cookies enviados de conexões SSL/TLS;
1.5.12. Configurar os cookies com o atributo HttpOnly, a menos que seja explicitamente necessário ler ou definir os valores dos mesmos através de scripts do lado cliente da aplicação;
1.5.13. Somente trafegar senhas através de uma conexão protegida (SSL/TLS) ou conexões cifradas. Senhas temporárias devem ser avaliadas junto a equipe de segurança;
1.5.14. Filtrar os parâmetros que contenham informações sensíveis, provenientes do “HTTP referer”, nos links para sites externos;

1.5.15. Não transferir, diretamente, dados fornecidos pelo usuário para qualquer função de execução dinâmica sem realizar o tratamento dos dados de modo adequado;
1.5.16. As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos devem possuir o menor privilégio possível
1.5.17. Utilizar mecanismos complementares ao mecanismo padrão de gerenciamento de sessões para operações sensíveis do lado servidor – como no caso de operações de gerenciamento de contas, transações financeiras ou informações que se enquadrem como CONFIDENCIAL conforme MNP de Classificação e Tratamento da Informação –. através da utilização de tokens aleatórios ou parâmetros em cada requisição em vez de basear-se apenas na sessão. Esse método usado para prevenir ataques do tipo Cross Site Request Forgery (CSRF)
1.6. Autenticação e gerenciamento de credencias
1.6.1. Assegurar que os usuários sejam autenticados em todas as páginas e recursos do sistema, exceto para dados públicos;
1.6.2. Os controles de autenticação devem ser executados em um sistema confiável, centralizado e possível com bibliotecas exclusivas para esse tipo de atividade;
1.6.3. Mediante situações excepcionais nos controles de autenticação, negar quaisquer solicitações;
1.6.4. Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial;
1.6.5. As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como “nome de usuário incorreto” ou “senha incorreta”, utilize apenas “usuário e/ou senha inválidos”;
1.6.6. As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em local protegido, por exemplo, no servidor da aplicação;
1.6.7. Em aplicações web, utilizar apenas requisições com o método POST para transmitir credenciais de acesso;
1.6.8. A entrada da senha deve permanecer ofuscada. Em HTML, utilizar o campo do tipo "password";
1.6.9. Os processos de redefinição de senhas e operações de mudanças devem exigir os mesmos níveis de controle previstos para a criação de contas e autenticação;
1.6.10. Se optar por usar redefinição de senha baseada em e-mail, enviar a mensagem conforme definido em integração com Multifatorial
1.6.11. Exigir a mudança de senhas temporárias quando na realização do primeiro logon, a não ser que esteja integrado ao AD e assim quem gerencia a conformidade de senha/validade/força/integração com RH é o AD. Entretanto deve utilizar integração via LDAPs.
1.6.12. Informar ao usuário autenticado data/hora e o endereço IP da sua última utilização do sistema;
1.6.13. Se a aplicação gerenciar um repositório de credenciais, o sistema deverá garantir que as senhas sejam armazenadas na base de dados somente sob a forma de hash, conforme padronização contida no capítulo “Padrões de Criptografia e Funções de Hash”;
1.6.14. Para evitar ataques de brute force ou mesmo a utilização inadvertida de rôbos, adotar mecanismos de CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), para a diferenciação entre máquinas e humanos.

Por se tratar de um desafio cognitivo, considera-se que aquele que incorpora uma solução correta é presumidamente humano.

1.7. Práticas de Criptografia:
1.7.1. Todas as funções de criptografia utilizadas para proteger dados sensíveis dos usuários da aplicação, devem ser implantadas em um sistema confiável (neste caso o servidor)
1.7.2. A senha mestre deve ser protegida contra acessos não autorizados
1.7.3. Quando ocorrer alguma falha nos módulos de criptografia, permitir que as mesmas ocorram de modo seguro
1.7.4. Todos os números, nomes de arquivos, GUIDs e strings aleatórias devem ser gerados usando um módulo criptográfico com gerador de números aleatórios, somente se os valores aleatórios gerados forem impossíveis de serem deduzidos
1.7.5. Os módulos de criptografia usados pela aplicação devem ser compatíveis com a FIPS 140-2 ou com um padrão equivalente (http://csrc.nist.gov/groups/STM/cmvp/validation.html)
1.7.6. Estabelecer e utilizar uma política e processo que defina como é realizado o gerenciamento das chaves criptográficas

1.8. Tratamento de Erros e Log:
1.8.1. Não expor informações sensíveis nas repostas de erros, inclusive detalhes de sistema, identificadores de sessão ou informação da conta do usuário
1.8.2. Usar mecanismos de tratamento de erros que não mostrem informações de depuração (debug) ou informações da pilha de exceção
1.8.3. Usar mensagens de erro genéricas e páginas de erro personalizadas
1.8.4. A aplicação deve tratar os erros sem se basear nas configurações do servidor
1.8.5. A memória alocada deve ser liberada de modo apropriado quando ocorrerem condições de erro
1.8.6. O tratamento de erros lógicos associados com os controles de segurança devem, por padrão, negar o acesso
1.8.7. Todos os controles de log devem ser implementados em um sistema confiável, por exemplo, centralizar todo o processo no servidor
1.8.8. Os controles de log devem dar suporte tanto para os casos de sucesso como os de falha relacionados com os eventos de segurança
1.8.9. Garantir que os logs armazenam eventos importantes
1.8.10. Garantir que as entradas de log que incluam dados nos quais não se confia não sejam executadas como código-fonte na interface de visualização de logs
1.8.11. Restringir o acesso aos logs apenas para pessoal autorizado
1.8.12. Utilizar uma rotina centralizada para realizar todas as operações de log
1.8.13. Não armazenar informações sensíveis nos registros de logs, como detalhes desnecessários do sistema, identificadores de sessão e senhas
1.8.14. Garantir o uso de algum mecanismo que conduza (ou facilite) o processo de análise de logs
1.8.15. Registrar em log todas as falhas de validação de entrada de dados
1.8.16. Registrar em log todas as tentativas de autenticação, especialmente as que falharam por algum motivo
1.8.17. Registrar em log todas as falhas de controle de acesso
1.8.18. Registrar em log todos os eventos suspeitos de adulteração, inclusive alterações inesperadas no estado dos dados

1.8.19. Registrar em log as tentativas de conexão com tokens de sessão inválidos ou expirados
1.8.20. Registrar em log todas as exceções lançadas pelo sistema
1.8.21. Registrar em log todas as funções administrativas, inclusive as mudanças realizadas nas configurações de segurança
1.8.22. Registrar em log todas as falhas de conexão TLS com o backend
1.8.23. Registrar em log todas as falhas que ocorreram nos módulos de criptografia
1.8.24. Utilizar uma função de hash criptográfica para validar a integridade dos registros de log

1.9. Segurança nas comunicações:
1.9.1. Utilizar criptografia na transmissão de todas as informações sensíveis. Isto deve incluir TLS para proteger a conexão e deve ser complementado com criptografia de arquivos que contém dados sensíveis ou conexões que não usam o protocolo HTTP
1.9.2. Os certificados TLS devem ser válidos, possuírem o nome de domínio correto, não estarem expirados e serem instalados com certificados intermediários, quando necessário
1.9.3. Quando ocorrer alguma falha nas conexões TLS, o sistema não deve fornecer uma conexão insegura
1.9.4. Utilizar conexões TLS para todo o conteúdo que requerer acesso autenticado ou que contenha informação sensível
1.9.5. Utilizar TLS para conexões com sistemas externos que envolvam funções ou informações sensíveis
1.9.6. Utilizar um padrão único de implementação TLS configurado de modo apropriado
1.9.7. Especificar a codificação dos caracteres para todas as conexões
1.9.8. Filtrar os parâmetros que contenham informações sensíveis, provenientes do “HTTP referer”, nos links para sites externos

1.10. Gerenciamento de Memória:
1.10.1. Utilizar controle de entrada/saída para os dados que não sejam confiáveis
1.10.2. Verificar se o buffer é tão grande quanto o especificado
1.10.3. Ao usar funções que aceitem determinado número de bytes para realizar cópias, como strncpy(), esteja ciente de que se o tamanho do buffer de destino for igual ao tamanho do buffer de origem, ele não pode encerrar a sequência de caracteres com valor nulo (null)
1.10.4. Verificar os limites do buffer caso as chamadas à função sejam realizadas em ciclos e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado
1.10.5. Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação
1.10.6. Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo etc., não contar com o “garbage collector” e realizar a tarefa explicitamente
1.10.7. Usar pilhas não executáveis, quando disponíveis
1.10.8. Evitar o uso de funções reconhecidamente vulneráveis como printf(), strcat(), strcpy() etc.

1.10.9. Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos pontos de saída