

**AVISO DE LICITAÇÃO  
PREGÃO ELETRÔNICO Nº 019/2020**

O **BANCO DO ESTADO DO PARÁ S.A.** torna público que realizará, nos termos da Lei nº 13.303/2016 e de seu Regulamento de Licitações e Contratos<sup>1</sup>, licitação na modalidade pregão eletrônico para **Contratação de empresa especializada para execução de serviços técnicos contínuos de segurança da Informação referente a Testes de Intrusão Externos e Internos aos Sistemas e Redes do Banpará, com fornecimento de relatórios específicos de avaliação de vulnerabilidades expostas, mais Treinamento Ethical Hacking conforme condições estabelecidas no Termo de Referência de demais anexos.** Os referidos serviços deverão ser prestados nos locais definidos pelo Banco do Estado do Pará S/A e de acordo com o especificado no Termo de Referência.

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

**DATA: 14.07.2020**  
**HORÁRIO: 10h (horário de Brasília)**

SISTEMA DE LICITAÇÕES: [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br)  
**UASG: 925803**

O edital da licitação estará disponível a partir de 23/06/2020, podendo ser obtido: (i) Gratuitamente no site do BANPARÁ ([www.banpara.b.br](http://www.banpara.b.br)) e sites [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br) e [www.compraspara.pa.gov.br](http://www.compraspara.pa.gov.br) ; ou, (ii) Na sede do BANPARÁ (Av. Presidente Vargas, nº 251, Ed. BANPARÁ – 1º andar, Comércio, Belém/PA) mediante depósito identificado do valor de R\$0,15 (quinze centavos) por folha (Conta-Corrente nº 800.002-6, Agência nº 11 do BANPARÁ), não reembolsável, relativos aos custos de reprodução.

Belém-Pará, 23 de Junho de 2020.

Soraya Rodrigues  
Pregoeira

<sup>1</sup>[https://www.banpara.b.br/media/233274/regulamento\\_de\\_licitacoes\\_e\\_contratos.pdf](https://www.banpara.b.br/media/233274/regulamento_de_licitacoes_e_contratos.pdf)

## PREGÃO ELETRÔNICO Nº 019/2020 EDITAL

O **BANCO DO ESTADO DO PARÁ S.A.**, por intermédio do pregoeiro designado pela Portaria nº 163/2019 leva ao conhecimento dos interessados que, na forma da Lei nº 13.303/2016, do Regulamento de Licitações e Contratos do BANPARÁ (adiante denominado “Regulamento”), da Lei nº 10.520/2002 alterada pelas disposições do Decreto nº 10.024/2019, da Lei Complementar nº 123 e da Lei Estadual nº 8.417/2016, do Decreto Estadual nº 2.121/2018, Lei nº 12.846/2013 e do 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: Contratação de empresa especializada para execução de serviços técnicos contínuos de segurança da Informação referente a Testes de Intrusão Externos e Internos aos Sistemas e Redes do Banpará, com fornecimento de relatórios específicos de avaliação de vulnerabilidades expostas, mais Treinamento Ethical Hacking conforme condições estabelecidas no Termo de Referência de demais anexos.**

1.1.1. **MODALIDADE:** Pregão Eletrônico.

1.1.2. **MODO DE DISPUTA:** Aberto e 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 **14/07/2020**, às 10h (horário de Brasília) no sistema de licitações [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br).

**1.2. A adjudicação será POR ITEM.**

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 art. 34, item 4 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 Pregoeiro, na sessão, informar o contrário.

1.6. No campo “descrição detalhada do objeto ofertado” do sistema [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br), 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 ComprasNet, 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br), quando for o caso.

## **2. CONDIÇÕES DE PARTICIPAÇÃO E CONTRATAÇÃO**

**2.1.** Poderá 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 anexo II do presente edital.
- b) de cooperativas.
- c) de empresas reunidas em consórcio.

**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 pregoeiro, 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.
    - iv. Os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema, **até a abertura da sessão pública**.
    - v. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro 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 pregoeiro 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 pregoeiro 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 pregoeiro 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 § 2º do artigo 56 da Lei nº 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 Pregoeiro 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 Pregoeiro por solicitação escrita e justificada do licitante e formalmente aceita pelo Pregoeiro, formulada antes de findo o prazo.
  - X.** Dentre os documentos passíveis de solicitação pelo Pregoeiro, 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 Pregoeiro 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 Pregoeiro, desde que não haja majoração do preço proposto.
- j) Julgamento:**
    - I.** O critério de julgamento da presente licitação será o de menor preço.
  - k) Habilitação:**
    - I.** 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:**
    - I.** 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:**
    - I.** Os procedimentos de interposição de recurso e julgamento serão definidos no item 11 do edital.
  - n) Adjudicação e homologação:**
    - I.** 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br)**, 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 art. 42, I A 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/COMPASNET, até o momento anterior a abertura de sessão.

**4.3.** O cadastro se dará após o acesso ao site: <https://portal.brasilcidadeao.gov.br/servicos-cidadao/aceso/#/primeiro-aceso> 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br). 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@banparanet.com.br](mailto:cpl@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 07/07/2020**.

**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 pregoeiro 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 pregoeiro e será publicada no sítio eletrônico do BANPARÁ e no site [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br), assim como, todos os avisos, pedidos de esclarecimentos, impugnações e suas respectivas respostas.

**5.2.** Somente terão validade os comunicados veiculados por intermédio do pregoeiro 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 artigo 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 deverão, por ocasião do envio da proposta, declarar em campo próprio do sistema, sob as penas da lei, que atendem os requisitos do artigo 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 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, 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 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 artigo 17 da Lei Complementar nº 123/2006, os licitantes microempresas ou empresas de pequeno porte que forem optantes do Simples Nacional deverão formular suas propostas desconsiderando os benefícios tributários do regime a que fazem jus.

**6.9.** O prazo de validade das propostas será de 180 (cento e oitenta) dias, contados da data prevista para abertura dos envelopes, podendo vir a ser prorrogado mediante solicitação do BANPARÁ e aceitação do licitante.

**6.9.1)** O Pregoeiro 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 no item 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 Termo de Referência**.

## **7. JULGAMENTO**

**7.1.** A presente licitação será julgada pelo critério do menor preço e, nos termos do item 3 do artigo 104 do Regulamento, seguirá as regras de apresentação de propostas e lances estabelecidos pelo sistema eletrônico utilizado, no caso, [www.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br). No horário designado, o Pregoeiro 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 pregoeiro, 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 pregoeiro 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.

**7.5** Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes.

**7.6** 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.

**7.7** Não serão aceitos lances iguais, prevalecendo aquele que for recebido e registrado primeiro.

**7.8** Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor for considerado inexecutável.

**7.9** Não será admitida a desistência do lance efetivado, sujeitando-se o licitante desistente às penalidades previstas neste edital e na legislação vigente.

**7.10** 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 ela apresentado.

## **8. DIREITO DE PREFERÊNCIA PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**

**8.1.** Encerrada a etapa de lances, o pregoeiro deverá verificar se ocorre o empate ficto em favor de microempresa ou empresa de pequeno porte, 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 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;

ii) ocorrendo o empate, a microempresa ou a empresa de pequeno porte melhor classificada, convocada pelo pregoeiro, 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 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 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 nº 8.417/2016.

**8.2.** Caso a microempresa ou empresa de pequeno porte, classificada pelo exercício do direito de preferência, venha a ser desclassificada ou inabilitada por vícios em sua proposta ou documentação, o pregoeiro 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 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 neste item, 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 pregoeiro 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 pregoeiro 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br) no prazo estipulado pelo pregoeiro.

9.1.2. O Pregoeiro 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 ofereça 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 X, deve constar, conforme o caso:

- i. indicação dos quantitativos e dos custos unitários;
- ii. caso o licitante seja microempresa ou empresa de pequeno porte 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 pregoeiro 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 pregoeiro 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 pregoeiro 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 pregoeiro 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 pregoeiro 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 pregoeiro 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 Pregoeiro 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 Pregoeiro 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 Pregoeiro a erro;
- c) O pregoeiro deverá conceder prazo adequado, recomendando-se 02 (dois) dias úteis, prorrogáveis por igual período, para que o licitante corrija os defeitos de sua proposta;
- d) O Pregoeiro 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 Pregoeiro poderá conceder novo prazo para novas correções.

9.11. Sendo aceitável a proposta, o pregoeiro 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br) no momento da 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 nº 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:**

**10.3.1. O licitante deverá apresentar os documentos de qualificação técnica exigidos no Termo de Referência (Anexo I do edital).**

### **10.4. Qualificação econômico financeira:**

**10.4.1. O licitante deverá apresentar os documentos de qualificação econômico-financeira, exigidos no Termo de Referência (Anexo I do edital).**

**10.5. 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. Declaração de conformidade com o art. 38 da Lei 13.303/2016, conforme anexo II do presente edital.**

**10.7.** Microempresas e empresas de pequeno porte deverão atender a todas as exigências de habilitação previstas neste edital.

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

**10.7.2.** 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;

**10.7.3.** 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.

**10.8.** 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.

**10.8.1.** 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 o item 10.1 acima.

**10.9.** Se o licitante desatender às exigências habilitatórias, o pregoeiro 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.

**10.10.** 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.

**10.11.** O pregoeiro 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 pregoeiro poderá realizar diligência para esclarecer o teor ou sanar defeitos constatados nos documentos de habilitação;
- c) O pregoeiro, se for o caso de diligência, deverá conceder prazo de 02 (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 pregoeiro, 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 pregoeiro poderá conceder novo prazo para novas correções.

**10.12.** Se o licitante desatender às exigências habilitatórias, o pregoeiro 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.

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

**10.14.** 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.

**10.14.1.** O prazo estabelecido neste subitem poderá ser prorrogado por decisão fundamentada do pregoeiro, após análise de justificativa apresentada pelo licitante.

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

**10.16.** 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.

**10.17.** 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 03 (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 pregoeiro 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 pregoeiro, por e-mail para [cpl@banparanet.com.br](mailto:cpl@banparanet.com.br).

11.5. O pregoeiro 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 pregoeiro 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 pregoeiro disporá de 05 (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 05 (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 pregoeiro 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.comprasnet.gov.br](http://www.comprasnet.gov.br)

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 09h 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 do ComprasNet, salvo os anexos que, quando necessário, poderão ser encaminhados via e-mail, para: [cpl@banparanet.com.br](mailto:cpl@banparanet.com.br), o que deverá ser indicado pelo licitante em suas razões recursais, a fim de que o pregoeiro possa divulgá-los no site [www.banpara.b.br](http://www.banpara.b.br).

## **12. ADJUDICAÇÃO E HOMOLOGAÇÃO**

12.1. Se não houver recurso, a declaração de vencedor realizada pelo pregoeiro 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 o 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 05 (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 III).

13.1.1. A convocação para assinatura do contrato deverá ser atendida pelo licitante adjudicado no prazo de 05 (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) indicação da modalidade de garantia de execução que será prestada;
- b) e indicação do(s) profissional(ais) que se responsabilizará(ão) tecnicamente pela prestação dos serviços, bem como a sua vinculação com a empresa, que poderá se dar mediante a apresentação de contrato social, carteira profissional devidamente assinada e registrada ou contrato de prestação de serviços específicos para o objeto deste edital, quando for o caso.

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 neste subitem, 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 III).

### **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 02 (dois) anos, além das demais cominações legais cabíveis, nos seguintes casos:

- a) Deixar de entregar a documentação exigida no certame;
- b) Não manter 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 artigos 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93, que se aplicam à Lei 13.303 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 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](http://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 de contrato, anexo III 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 02 (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 artigo 7º e seus incisos da Lei nº 12.846/2013.

15.9. Caso os atos lesivos apurados envolvam infrações administrativas à Lei nº 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 nº 12.846/2013 e no Decreto nº 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.

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 artigo 1º da Lei nº 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 artigo 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.comprasgovernamentais.gov.br](http://www.comprasgovernamentais.gov.br), 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 o pregoeiro, por solicitação pelo e-mail [cpl@banparanet.com.br](mailto:cpl@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 pregoeiro 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 pregoeiro 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 nº 13.303/2016, Regulamento de Licitações e Contratos do BANPARÁ, Lei nº 10.520/2002, Decreto nº 10.024/2019, da Lei Complementar nº 123 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 pregoeiro.

16.18. Fazem parte integrante deste edital os seguintes anexos:

**ANEXO I – TERMO DE REFERÊNCIA**  
**ANEXO II – MODELO DE DECLARAÇÃO**  
**ANEXO III – MINUTA DE CONTRATO**

Belém-Pará, 23 de Junho de 2020.

Soraya Rodrigues  
Pregoeira

## Termo de Referência Teste de Intrusão

### 1 Objeto

---

Contratação de empresa especializada para execução de serviços técnicos contínuos de segurança da Informação referente a Testes de Intrusão Externos e Internos aos Sistemas e Redes do Banpará, com fornecimento de relatórios específicos de avaliação de vulnerabilidades expostas, mais Treinamento Ethical Hacking conforme condições estabelecidas no presente Termo de Referência.

#### 1.1 Parcelamento do objeto

Considerando a possibilidade de parcelamento do objeto almejado para aproveitar as peculiaridades do mercado e visando a economicidade o objeto será dividido em 3 (três) itens conforme tabela de Especificações do Item 5 deste Termo de Referência.

### 2 JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

---

#### 2.1 razão da necessidade da contratação:

“A informação é um ativo muito importante para qualquer organização, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé podem comprometer significativamente, não apenas a imagem da organização perante terceiros, como também o andamento dos próprios processos organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações.” (TCU – Manual de Boas Práticas em Segurança da Informação)

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

Devido à complexidade e criticidade das informações administradas pelo Banpará, enquanto instituição financeira, bem como para melhor gerenciar a Segurança da Informação nos seus aspectos de confidencialidade, integridade e disponibilidade, em conformidade com sua Política de Segurança da Informação, o Banco contratou empresa especializada para fornecimento de Solução Integrada de Serviços Gerenciados de Segurança Lógica abrangendo os seguintes serviços:

- Firewall Próxima Geração e VPN, para controle do tráfego nos segmentos protegidos;
- Prevenção de Intrusos, para detecção e bloqueio de intrusão nos segmentos protegidos;
- Gestão de Risco e Compliance, para descoberta e gestão de eventuais falhas de segurança no ambiente;
- Gateway de Web, para controle do tráfego web e proteção contra vírus, acessos indevidos e conteúdo indesejado;
- Gateway de E-mail, para controle do tráfego de e-mail e proteção contra vírus, spam e conteúdo indesejado;
- Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por vírus;
- Proteção Contra Vazamento e Integridade dos Dados, para identificar e mitigar possíveis perdas de informações sensíveis;
- Gestão de Eventos e Incidentes, para armazenagem, gerenciamento e correlacionamento de logs e eventos;

- Proteção Contra Ameaças Dia Zero, para identificar e bloquear esse tipo de ameaça no ambiente da CONTRATANTE;

Tais serviços formam o arcabouço necessário para um ambiente seguro quanto à proteção da Rede Corporativa, Estações de Trabalho, Servidores e outros ativos do Banco. No entanto, seguindo as melhores práticas em Segurança da Informação, tais serviços precisam ser testados.

Para que haja maior transparência e autonomia na análise de eventuais vulnerabilidades encontradas na rede e nos Sistemas utilizados pelo Banpará, optou-se pela contratação de empresa especializada para realizar, especificamente, os testes de intrusão, checando assim o nível de segurança do Banpará e contribuindo na gestão de segurança.

A contratação será de banco de horas a serem consumidas sob demanda, de forma planejada, a serem consumidas em um período de 1 ano.

A quantidade de total do banco de horas, estimada em 1000h (mil horas) para teste de invasão em redes e 1500h (mil e quinhentas horas) para teste de invasão em sistemas, foi baseada no seguinte cenário:

Média de 60h (sessenta horas) por aplicação e 15h (quinze horas) por serviço/ativo de rede para testes de segurança

Estimaram-se cerca de 25 (vinte e cinco) sistemas e 66 (sessenta e seis) serviços/ativos de rede a serem escolhidos em momento oportuno.

### **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**

A CONTRATADA, desde que com a prévia e expressa autorização do gestor do contrato do BANPARÁ, pode subcontratar parcela do objeto deste contrato, desde que não se refira a parcela sobre a qual o BANPARÁ exigiu atestado de capacidade técnica durante o processo licitatório. A subcontratação pode abranger aspectos acessórios e instrumentais de tais parcelas.

#### **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 Da Especificação dos Itens

Item	Objeto	Descrição	Quantidade	Unidade
1	Serviço de Teste de invasão em redes	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 ( <b>Wireless</b> ) e Rede de Área Local ( <b>LAN</b> ) do tipo Externos e/ou Internos.	1000	Horas
2	Serviço de Teste de invasão em sistemas no padrão Red Team (in loco), Blackbox, GreyBox e WhiteBox.	Testes para identificar falhas de segurança em sistemas	1500	Horas
3	Curso preparatório para EXIN Ethical Hacking e CompTIA PenTest+.	Curso preparatório tanto para a certificação EXIN Ethical Hacking Foundation quanto para a certificação CompTIA PenTest+.	2	Turmas

##### 5.1 Serviços para os itens 1 e 2

- 5.1.1** A atividade de Testes de Invasão poderá ser do tipo Externos e/ou Internos (in loco) e terá como objetivo principal análise geral do ambiente do Banpará quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do Banpará, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.
- 5.1.2** A empresa contratada deverá entregar à equipe da GESEI – Gerência de Segurança da Informação todo detalhamento dos testes de invasão a serem realizados, desde os ativos que foram testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.
- 5.1.3** O teste de invasão de redes só poderá acontecer mediante autorização da GESEI – Gerência de Segurança da Informação, com anuência da GEHAS – Gerência de Hardware e Software
- 5.1.4** O teste de invasão de sistemas só poderá acontecer mediante autorização da GESEI – Gerência de Segurança da Informação, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.
- 5.1.5** Para os casos de testes reativos, aqueles realizados após a ocorrência de um incidente de segurança, deve ser realizado uma análise forense, para identificar as ações externas que comprometeram os ativos de tecnologias, sistemas e aplicações.
- 5.1.6** Para toda vulnerabilidade encontrada, a Contratada deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a Contratada deverá justificar a necessidade, ficando a cargo do BANPARÁ decidir pela liberação.
- 5.1.7** O tempo estimado para cada teste deve considerar as atividades entre: varreduras, mapeamentos, testes e análise. O tempo gasto pelos testes automatizados devem se limitar apenas a esforço gasto para manipulação da ferramenta, desconsiderando o tempo de varredura.
- 5.1.8** Todos os testes a serem realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações do Banco.

- 5.1.9** Estes testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações do Banpará, e devem observar orientações e técnicas emanadas por padrões internacionais ou equivalente apresentados pela empresa CONTRATADA, caso possua, em seu portfólio, normativos que complementem os demonstrados abaixo:
- 5.1.10** OSSTMM 3 (*The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined*);
- 5.1.11** ISSAF/PTF (Information Systems Security Assessment Framework);
- 5.1.12** NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);
- 5.1.13** NIST Special Publication 800-42 (Guideline on Network Security Testing)
- 5.1.14** OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.
- 5.1.15** PCI DSS (Payment Card Industry Data Security Standard)
- 5.1.16** PCI SSC Information Supplement
- 5.1.17** PTES (Penetration Testinf Execution Standard)
- 5.1.18** A CONTRATADA deverá realizar, no mínimo, 01 (uma) vez a cada 06 (seis) meses, simulações de invasão ilícita e não autorizada a ativos e informações (Teste de Invasão) a serem executadas internamente (qualquer ponto da rede corporativa do Banpará) ou externamente (através da Internet), com duração de até 15 (quinze) dias cada teste.
- 5.1.18.1** **Caso necessário a CONTRATANTE poderá solicitar teste sob demanda utilizando as horas contratadas conforme item 5.1.18 e estrutura do item 5.1.4.**
- 5.1.19** Todas as fases dos "Testes de Invasão" serão acompanhadas e supervisionadas a critério da CONTRATANTE.
- 5.1.19.1** **Cada fase deve ser feita durante o período que não comprometa processamento da CONTRATANTE e que as agências estejam fechadas sendo feita em no máximo 2 dias corridos no total.**
- 5.1.20** Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.
- 5.1.2** Transferência de conhecimento técnico com apresentações dos serviços.
- 5.1.3** Evolução do atual modelo de gestão de segurança da informação com aumento consequente do nível de maturidade.
- 5.1.4** Teste de Intrusão
- 5.1.4.1** **O teste de invasão deverá obedecer às seguintes fases:**

- a. Planejamento;
- b. Descoberta;
- c. Ataque;
- d. Relatório de Teste de Invasão;
- e. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;
- f. Reavaliação, novo teste pós remediação;
- g. Relatório final do Teste de Invasão.

#### 5.1.4.2 Planejamento:

##### 5.1.4.2.1 Todas as premissas, processos, atividades descritas, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento para os tipos de teste de penetração a seguir:

- a) **PENTEST DE REDE:** Este teste é focado em recursos de rede, onde o escopo é definido em termos de endereços IP e intervalos de rede. Os testes de rede externa também podem ter o escopo definido em termos de nomes de domínio (o avaliador precisa descobrir os endereços de rede associados a esses domínios como parte do teste).
- b) **PENTEST DE APLICAÇÃO:** Este teste é focado em aplicação, geralmente aplicação web, mobile e cliente/servidor. Os avaliadores se concentrarão em encontrar e explorar vulnerabilidades somente nessa aplicação.
- c) **PENTEST DE REDE SEM FIO:** Este teste é semelhante a um pentest de rede, mas o escopo é definido por redes sem fio, tanto faz se especificadas diretamente pelos identificadores de conjunto de serviços (SSIDs) e localização física ou apenas por localização (por exemplo, "qualquer rede sem fio em nosso Prédio de escritórios principais").
- d) **PENTEST DE ACESSO REMOTO:** este teste é semelhante a pentest de rede, mas o escopo é definido em pontos específicos de acesso à rede corporativa (como VPN de acesso remoto de funcionários ou VPN B2B)
- e) **PENTEST DE ENGENHARIA SOCIAL:** quando os testes incluem uma tentativa de enganar as pessoas para fornecer dados confidenciais ou privilégios de acesso ao avaliador, os tipos de truques a serem executados (como golpes de telefone, tentativas de phishing ou acesso físico) e alvos autorizados (como pessoas que podem ser alvo do teste, incluindo executivos, agentes do call center ou qualquer pessoa no escritório principal) são parte da definição do escopo.
- f) **TESTE FÍSICO OU DE INSTALAÇÕES:** estes testes abrangem controles de segurança física, como controle de acesso a instalações e recursos de TI. Um teste típico de segurança física pode incluir acesso a um centro de dados e acesso direto aos racks dos servidores. Também pode ser focado em ambientes de escritório, verificando a disponibilidade de

informações confidenciais em papel ou acesso a desktops e laptops dos usuários.

- 5.1.4.2.2 Todos os testes bem sucedidos devem ser gravados e/ou registrados em documentos restritos para compor as ações dos serviços realizados.**
- 5.1.4.2.3 Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas, podendo ser utilizadas ambas, conforme definição do escopo:**
- 5.1.4.2.4 Técnica da caixa preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista, pois a maioria das pessoas entende que os pentes implicam fornecer ao avaliador apenas as informações necessárias sobre o ambiente alvo para definir o escopo. Embora esta seja a abordagem mais comum, conhecida como "caixa preta", esta não é a única opção. Os testes de caixa preta são adequados quando a organização está interessada em ver a quantidade de informação sobre seu ambiente e sistemas pode ser obtida pelo avaliador. Quando a intenção do teste é verificar o que um invasor externo poderia fazer, esta é a opção preferida. No entanto, a extensão do que será testado pode acabar limitada pela quantidade de informações sobre o meio ambiente que o avaliador pode obter. A falta de resultados neste caso não significa que não existam vulnerabilidades exploráveis, mas que o avaliador não conseguiu encontrar onde procurá-los).**
- 5.1.4.2.5 Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste, visto que em testes de caixa branca, a organização compartilha todas as informações sobre o ambiente alvo. Em testes de rede, isso pode incluir os endereços IP e as funções dos servidores na rede, topologias de rede e espaços de endereço existentes, ou todos os nomes de domínio usados pela organização. Os testes de aplicativos que seguem a abordagem da caixa branca geralmente incluem credenciais para o aplicativo (para que o invasor possa se concentrar em privilégios de escalada e executar transações não autorizadas em vez de obter acesso) ou mesmo o código-fonte. Os testes de caixa branca têm maiores chances de encontrar vulnerabilidades e dar mais garantia de que todos os pontos potencialmente vulneráveis são testados. Os testes de caixa branca podem ser uma opção mais realista para validar o que podem ser feitos pelos iniciados);**

- 5.1.4.2.6 Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo, ou seja, o modelo de caixa cinza é uma abordagem "do meio da estrada" que tenta ganhar valor a partir de modelos preto e branco. Em um teste de caixa cinza, a organização compartilha apenas informações suficientes para garantir que o avaliador encontre e teste os pontos que espera ser testados. Quando as redes em escopo são muito grandes, também faz sentido compartilhar algumas informações sobre os pontos mais interessantes; Isso evitará situações em que o avaliador gaste muito tempo em recursos menos importantes. Nos testes de aplicativos, fornecer credenciais de acesso básicas também garante que o avaliador testará partes do aplicativo que só são acessadas por usuários autenticados. As aplicações tipicamente terão uma boa camada de autenticação, o suficiente para evitar que o assessor acesse a área autenticada, mas existem vulnerabilidades graves nessa área. Nesses casos, Um teste puro de caixa preta pode dar à organização uma falsa percepção de segurança. É aqui que um modelo de caixa cinza pode fornecer o melhor equilíbrio entre um cenário realista e uma avaliação mais completa).**
- 5.1.4.2.7 Técnicas de Operações Red Team: Consiste em um ataque realista e sem limites no ambiente geral da CONTRATANTE onde será utilizada métodos não destrutivos necessários para atingir um conjunto de objetivos definidos de comum acordo entre as partes, simulando o comportamento de um atacante em todas as suas esferas. A atividade desta técnica imita bem os métodos de ataque aos ativos e furtivos de um atacante real com o uso de TTPs (Tactics, Techniques, and Procedures). Esta técnica objetiva externar ao CONTRATANTE avaliar a capacidade da sua equipe de segurança de detectar e responder a um cenário de ataque ativo.**

- 5.1.4.2.8** E outras técnicas novas que surgirem e não estão definidas aqui, mas acordadas com a CONTRATANTE e definidas no Plano de Teste de Penetração.
- 5.1.4.3** Deverá ser elaborado o “PLANO DE TESTE DE PENETRAÇÃO”, para cada teste ou reavaliação, novo teste pós remediação do teste realizado anteriormente, contemplando as informações de PLANEJAMENTO do teste, tais como:
- 5.1.4.4** Objetivos, premissas e escopo do teste, datas e horas dos testes, realizações, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas.
- 5.1.5** Também na fase de planejamento, deverão ser atendidas e apresentadas, no mínimo, as seguintes informações:
- 5.1.5.1** Detalhes da infraestrutura alvo dos testes de invasão;
- 5.1.5.2** Equipamentos e recursos demandados para este teste;
- 5.1.5.3** Tipos de ataque que serão realizados;
- 5.1.5.4** Prazos (janela de tempo para execução dos testes);
- 5.1.5.5** Contato da CONTRATADA (responsáveis para tratamento de questões não abordadas nos testes);
- 5.1.5.6** Tipos de testes a serem realizados pelos especialistas em segurança da informação
- 5.1.6** Os alvos dos “Testes de Invasão”, bem como as premissas e condições para realização dos mesmos serão definidos e aprovados pelo Banpará.
- 5.1.7** Planejamento das atividades: compreende a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e do cronograma de execução.
- 5.1.8** Análise de vulnerabilidades do ambiente de TI externo: avaliação da existência de vulnerabilidades para até 254 (duzentos e cinquenta e quatro) endereços IPs definidos pelo BANPARA;
- 5.1.9** A CONTRATADA não deverá alterar a integridade das informações, ou seja, não deve alterar informações dos servidores e sistemas que possam comprometer os serviços da CONTRATADA.
- 5.1.10** Teste manual das vulnerabilidades do ambiente TI interno e/ou externo: avaliação da possibilidade de exploração, comprometimento e/ou vulnerabilidades do ambiente de TI, para até 254 (duzentos e cinquenta e quatro) endereços IPs, definidos pelo BANPARA. Para o tipo de teste interno, este deverá ocorrer dentro das dependências da CONTRATADA, pois para esse teste não será fornecido VPN para realização deste tipo de teste.

### **5.1.11 Testes de Invasão em Aplicações**

- 5.1.11.1 Deverão ser realizados testes de invasão do tipo “Cross Site Scripting (XSS)”.**
- 5.1.11.2 Deverão ser realizados testes de invasão do tipo “Injeção de Código;**
- 5.1.11.3 Deverão ser realizados testes de invasão do tipo “Inclusão Remota de Arquivos (RFI)”;**
- 5.1.11.4 Deverão ser realizados mapeamentos e sondagens, com o objetivo de identificar possíveis vetores de entradas de ataques;**
- 5.1.11.5 Deverão ser realizados testes de invasão do tipo “Referência Direta a Objetos”.**
- 5.1.11.6 Deverão ser realizados testes de invasão do tipo “Vazamento de informações”, onde deve ser verificada a exposição inadvertida de informações sobre a aplicação e o servidor que a hospeda.**
- 5.1.11.7 Deverá ser realizado testes de invasão baseado em “Gerenciamento de Sessões”.**
- 5.1.11.8 Deverão ser analisadas, pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.**
- 5.1.11.9 Caso necessário, devem ser criados ataques customizados baseados na arquitetura das aplicações;**

### **5.2 Serviço de Auditoria de Segurança em Códigos Fonte de Aplicações**

- 5.2.1 Para a efetiva correção de uma vulnerabilidade poderá ser necessário a avaliação/auditoria do código fonte de uma determinada aplicação.**
- 5.2.2 As auditorias podem ser realizadas tanto remotamente ou presencialmente na sede do CNMP.**
- 5.2.3 Para a realização das auditorias, o CNMP disponibilizará o código-fonte da aplicação a ser auditada, que deverá ser mantida sob sigilo.**
- 5.2.4 O tempo estimado para cada auditoria deve considerar as atividades de reuniões, dentre planejamentos, varreduras, mapeamentos, testes, análise e elaboração e apresentação dos resultados.**
- 5.2.5 A auditoria de códigos-fonte visa avaliar, dentre outros itens, os seguintes conceitos:**
  - 5.2.5.1 Avaliação do fluxo de informações indo desde a arquitetura física (ex: fluxo de informações entre camadas web, camadas de aplicação e bancos de dados) até o fluxo de informações entre os módulos - variáveis e parâmetros.**
  - 5.2.5.2 Avaliação das lógicas de negócio requisitadas e implementadas. Detecção de possíveis fraudes internas ou vulnerabilidades na implementação das lógicas de negócio.**

- 5.2.5.3 Avaliação da utilização das APIs e construtos da linguagem de programação apontando os locais no código onde é feito uso inseguro das bibliotecas do sistema, dos elementos da linguagem de programação e recomendações de correção classificadas por risco e custo.**
- 5.2.5.4 Avaliação da exposição do código-fonte e das regras de negócio para entidades externas apontando os aspectos do código que estariam mais sujeitos a permitir o vazamento de segredos industriais.**
- 5.2.6** Fica expressamente proibida a divulgação e utilização do código fonte pela contratante, sendo o CNMP o único dono do código.
- 5.2.7** Teste manual de vulnerabilidades de aplicações web, avaliação da possibilidade de exploração, comprometimento e/ou vulnerabilidades de no mínimo 25 (vinte e cinco) aplicações web definidos pelo BANPARA, considerando as prerrogativas abaixo:
- 5.2.8** Cada uma das aplicações web será avaliada duas vezes durante a vigência do contrato, 3 (ciclos), sendo que a distribuição das avaliações poderá ser semestral (dez avaliações a cada semestre) ou mensal (uma avaliação ou duas avaliações a cada mês), conforme critério do BANPARA.
- 5.2.9** Caso não sejam analisadas as 25 (vinte e cinco) aplicações web previstas para o 1º (primeiro) ciclo, por solicitação do BANPARA, as análises das aplicações não realizadas neste ciclo poderão ser executadas durante o 2º (segundo) ciclo, a critério do BANPARÁ e acordado previamente com a LICITANTE ou no 3º (terceiro) ciclo para análise de aplicações não avaliadas nos dois primeiros ciclos;
- 5.2.10 Prazos (janelas de tempo para execução dos testes)**
- 5.2.10.1 A CONTRATADA deverá elaborar o “Plano de Teste de Invasão”, para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste, metodologia de análise de vulnerabilidades, equipe envolvida, prazos do teste, de acordo com as informações abaixo:**
- 5.2.10.1.1 O planejamento abrange a definição dos elementos a serem avaliados/testados, bem como a definição dos testes em si e o cronograma de execução. Deve ser realizado previamente, e em conjunto com o BANPARÁ, sendo obrigatória, a autorização formal do BANPARÁ antes da execução.**
- 5.2.10.1.2 Deve apresentar todo o detalhamento das análises e testes a serem realizados, desde os ativos que serão testados, procedimentos adotados, técnicas e ferramentas utilizadas, entre outras informações que possam ser relevantes ou solicitadas.**
- 5.2.10.1.3 Deve ser demonstrado e explanado a finalidade de cada ferramenta a ser utilizada, para avaliação e autorização prévia do BANPARÁ.**

- 5.2.10.1.4** Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, o que deve ser considerado na definição do cronograma. Caso o BANPARÀ entenda que haja algum risco neste sentido, solicitará modificação da metodologia e/ou do cronograma, inclusive podendo requerer a execução em finais de semana, feriados ou fora do horário comercial.
- 5.2.10.1.5** Os testes e avaliações poderão ser interrompidos por solicitação expressa do BANPARÀ a qualquer momento.
- 5.2.10.1.6** Durante a fase de planejamento, o BANPARÀ definirá qual o tipo de teste a ser aplicado a cada ativo, dentre as seguintes possibilidades: “caixa preta”, “caixa cinza” ou “caixa branca”, segundo a definição “OWASP – Testing Guide”.
- 5.2.10.1.7** É possível paralelização de atividades, por exemplo: análise de vulnerabilidades interna/externa e teste de vulnerabilidades manual, desde que atendidas todas as demais condições.
- 5.2.10.1.8** Deverão ocorrer no mínimo 03 (três) reuniões presenciais de planejamento no BANPARÀ a cada semestre, sendo possível por parte do Banco, solicitar demais reuniões presenciais para alinhamento de informações adicionais relativas a esta etapa de planejamento.
- 5.2.10.1.9** Todas as ferramentas e recursos utilizados para a prestação dos serviços são de responsabilidade da CONTRATADA.
- 5.2.11** Fornecer visualização da aplicação web através de relatório de ‘mapa do site’.
- 5.2.12** Fornecer análise detalhada de scripts e páginas estáticas descobertas em servidores web analisados que reflete as strings de conexão de banco de dados, endereços de e-mail, campos de formulário ocultos e outros itens potencialmente sensíveis.
- 5.2.13** Suportar autenticação para varredura de aplicações web protegidas por credenciais.
- 5.2.14** Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pelo Banpará.
- 5.2.15** Todas as fases (ciclos) dos “Testes de Invasão” poderão ser acompanhadas e supervisionadas a qualquer momento pelo Banpará.
- a. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada ao Banpará, haja vista a necessidade do Banco de manter a disponibilidade dos seus ambientes, ativos e serviços.

#### **5.2.16 Descoberta:**

**5.2.16.1 Deverá ser utilizado, pelo menos, 01 (uma) ferramenta de análise de vulnerabilidade comercial e 01 (uma) ferramenta de análise de vulnerabilidade gratuita, além de técnicas manuais de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e aprovação em sua utilização, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades.**

#### **5.2.17 Ataque**

#### **5.2.18 *Análise de vulnerabilidades do ambiente de TI***

**5.2.18.1 O serviço deve contemplar a realização semestral de análise de vulnerabilidade em até 254 (duzentos e cinquenta e quatro) endereços IPs externos definidos pelo BANPARÁ, visando identificar pontos de falha em suas configurações e versões que possam implicar em não atendimento as melhores práticas de segurança estabelecidas pelo mercado, além de identificar possíveis vulnerabilidades presentes em ativos, servidores, aplicações, sistemas, serviços, versões e configurações em produtos atualmente em uso pelo BANPARÁ;**

**5.2.18.2 Os endereços IPs externos a serem testados serão definidos pelo BANPARÁ durante a etapa de planejamento. Estes endereços IPs podem não ser todos pertencentes diretamente ao BANPARÁ e, não necessariamente farão parte do mesmo bloco de endereços;**

**5.2.18.3 Neste processo é aceito o uso de ferramentas automatizadas de escaneamento próprias e padrões de mercado.**

**5.2.18.4 A análise de vulnerabilidade deve considerar as principais vulnerabilidades informadas pelos principais meios de informações até a data de execução da análise, tais como fabricante de softwares, canais de divulgações de vulnerabilidades, além de recomendações aceitas como boas práticas pelo mercado.**

**5.2.18.5 O método de análise de vulnerabilidades deve contemplar, no mínimo, não restringindo-se somente a estes, os seguintes itens:**

**5.2.18.5.1 Identificação de pontos de entrada;**

**5.2.18.5.2 Mapeamento todas as portas abertas e serviços;**

**5.2.18.5.3 Descoberta de ativos, servidores, aplicações, sistemas, serviços e configurações;**

**5.2.18.5.4 Identificação versões utilizadas e informar se esta é a versão atualizada;**

**5.2.18.5.5 Testes de configuração;**

**5.2.18.5.6 Testes de vulnerabilidades;**

**5.2.18.5.7 Vetores de acesso;**

**5.2.18.5.8 Vetores de criação;**

- 5.2.18.5.9 Vetores de alteração;
- 5.2.18.5.10 Vetores de exclusão;
- 5.2.18.5.11 Vetores de negação de serviço (comprometimento geral/parcial);
- 5.2.18.5.12 Análise de mensagens de erro;
- 5.2.18.5.13 Identificação da vulnerabilidade (de acordo com CVE-<http://cve.mitre.org/>), problema, bug, erro ou item em não conformidade com boas práticas de segurança.
- 5.2.18.6 O mapeamento deve ser pró-ativo, identificando as ameaças confirmadas e ameaças potenciais, mapeando o grau do risco e classificando conforme padrões de mercado.
- 5.2.18.7 Todos os endereços IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações foco da análise, devem ser previamente aprovados pelo BANPARÁ, que pode eventualmente impedir alguns tipos de análises, bem como solicitar análises específicas, com foco de verificar a segurança de determinado ativo.
- 5.2.18.8 O resultado da análise deve seguir as seguintes etapas e conter os seguintes itens para análise de vulnerabilidades de infraestrutura:
  - 5.2.18.8.1 Identificação e explicação do endereço IPs, ativos, servidores, aplicações, sistemas, serviços, versões e configurações encontrados;
  - 5.2.18.8.2 Identificação de vulnerabilidades;
  - 5.2.18.8.3 Metodologia utilizada passo-a-passo (descrição do teste);
  - 5.2.18.8.4 Resultados obtidos (descrição do resultado);
  - 5.2.18.8.5 Evidência do teste;
  - 5.2.18.8.6 Classificar e priorizar as vulnerabilidades por risco (seguindo o padrão CVSS - <http://www.first.org/cvss/>);
  - 5.2.18.8.7 Controles mitigatórios aplicáveis;
  - 5.2.18.8.8 Definição da recomendação técnica para solução.

### **5.2.19 Teste manual das vulnerabilidades do ambiente de TI externo**

**5.2.19.1** O escopo deste serviço prevê a realização semestral de testes manuais de vulnerabilidades de infraestrutura para até 70 (setenta) IPs externos definidos pelo BANPARÁ, no intuito de aprofundar o mapeamento realizado na etapa anterior de análise de vulnerabilidades, tentando explorar as vulnerabilidades identificadas no ambiente.

**5.2.19.2** Os endereços IPs externos serão os mesmos definidos na etapa anterior “2.2 - Análise de vulnerabilidades do ambiente de TI externo”;

**5.2.19.3** Os testes devem incluir pelo menos as seguintes atividades, não se restringindo somente a estas:

**5.2.19.3.1** Leitura/Alteração/exclusão de configurações.

**5.2.19.3.2** Fingerprint.

**5.2.19.3.3** Descoberta da senha de acesso do ativo.

**5.2.19.3.4** Escalonamento(salto) de acessos, até o ponto máximo possível.

**5.2.19.4** Os testes devem ser feitos nas seguintes camadas:

**5.2.19.4.1** Aplicação;

**5.2.19.4.2** Apresentação;

**5.2.19.4.3** Sessão;

**5.2.19.4.4** Transporte;

**5.2.19.4.5** Rede.

**5.2.19.5** Os testes devem avaliar a possibilidade de exploração, comprometimento e/ou vulnerabilidades de:

**5.2.19.5.1** Servidores (diversas plataformas);

**5.2.19.5.2** Serviços (web, ftp, telnet, e-mail, dns, outros..);

**5.2.19.5.3** Ativos de rede (Firewall, IPS, Switches, Roteadores, Soluções de Balanceamentos, outros..).

**5.2.19.6** Nos testes deve ser utilizado a última metodologia disponível OSSTMM, item “Testes de Segurança em Rede de Dados (Capítulo 11 - Data Networks Security Testing)”.

**5.2.19.7** Deve ser imediatamente comunicado ao BANPARÁ cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.

### **5.2.20 Teste manual de vulnerabilidades de aplicações web**

- 5.2.20.1** O escopo deste serviço prevê a realização de testes manuais de vulnerabilidades de até 50 (cinquenta) aplicações web por ciclo, definidos pelo BANPARÁ;
- 5.2.20.2** Cada uma das 50 (cinquenta) aplicações web será avaliada apenas uma vez a cada ciclo, sendo que a distribuição das avaliações poderá ser semestral (dez avaliações a cada semestre) ou mensal (uma avaliação ou duas avaliações a cada mês), conforme critério do BANPARÁ. Caso não sejam analisadas as 50 (cinquenta) aplicações web previstas para o 1º (primeiro) ciclo, por solicitação do BANPARÁ, as análises das aplicações não realizadas neste ciclo poderão ser executadas durante o 2º (segundo) ciclo, desde que previamente acordado com a LICITANTE VENCEDORA;
- 5.2.20.3** Os testes devem englobar baseados na publicação OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project):
- 5.2.20.3.1** Aplicações acessadas via internet ou Intranet;
- 5.2.20.3.2** Portais web disponíveis;
- 5.2.20.3.3** Serviços web diversos detectados;
- 5.2.20.3.4** Webservices;
- 5.2.20.3.5** Sockets.
- 5.2.20.4** A critério do BANPARÁ, será definido qual escopo de usuários utilizado em cada teste, podendo ser definidos um ou mais destes critérios para uma mesma aplicação:
- 5.2.20.4.1** Sem credenciais;
- 5.2.20.4.2** Credenciais comuns;
- 5.2.20.4.3** Credenciais de administrador.
- 5.2.20.5** Os testes devem contemplar todas as páginas, telas e transações disponíveis na aplicação, incluindo páginas/telas disponíveis para usuários sem credencias, com credencias, páginas/telas de administração, bem como demais existentes.
- 5.2.20.6** Os testes manuais em aplicações devem contemplar as seguintes fases e itens em seu planejamento e execução, não se limitando somente a estes:
- 5.2.20.6.1** Coleta de Informações;
- 5.2.20.6.2** Teste de lógica de negócios;
- 5.2.20.6.3** Teste de autenticação;
- 5.2.20.6.4** Gerenciamento de Sessões;
- 5.2.20.6.5** Testes de validação de Dados;
- 5.2.20.6.6** Teste de Web Services;

**5.2.20.6.7 Negação de Serviço.**

**5.2.20.7 Deve incluir os testes listados e descritos nas duas últimas versões do TOPTEN disponibilizadas pela OWASP;**

**5.2.20.8 Pentest deve incluir a avaliação funcional de segurança, inspeção de segurança de código fonte e a avaliação de vulnerabilidade, sobre uma aplicação genérica de porte médio em uma ou mais das linguagens abaixo definidas:**

**5.2.20.8.1 Java**

**5.2.20.8.2 C#**

**5.2.20.8.3 C, C++, Objective-C**

**5.2.20.8.4 Ruby**

**5.2.20.8.5 Python**

**5.2.20.8.6 Power Builder**

**5.2.20.8.7 Perl**

**5.2.20.8.8 Basic, VB, VB.NET, VBScript**

**5.2.20.8.9 Pascal, Delphi**

**5.2.20.8.10 HTML5, JavaScript**

**5.2.20.8.11 .NET, ASP**

**5.2.20.9 E demais a ser informada na reunião prévia entre a CONTRATADA e o Banpará.**

**5.2.20.10 Deve ser imediatamente comunicado ao BANPARÁ cada salto (escalonamento de acesso) de endereços IPs, ativos, servidores, aplicações, sistemas, serviços ou domínios efetuados com sucesso, durante a realização de todos os testes manuais.**

**5.2.20.11 Avaliação funcional de segurança com análise de código e segurança em software que consiste em avaliação automatizada seguida por inspeção manual por amostragem. Essa forma é a mais custo eficiente para identificação de problemas no código.**

**5.2.20.12 A Avaliação funcional de segurança com análise de código e segurança em software totalmente automatizada tende a apresentar grande número de falsos positivos e ainda pode deixar de identificar algumas vulnerabilidades.**

**5.2.20.13 A Avaliação funcional de segurança com análise de código e segurança em software totalmente manual implica em um esforço e prazos muito longos que, tipicamente, não apontam nenhuma vulnerabilidade adicional ao processo misto. A inspeção de código é realizada em duas etapas.**

- 5.2.20.14** Numa primeira verificação, o analista irá executar um sistema de inspeção automatizada de código fonte sobre este código. O sistema de Avaliação funcional de segurança com análise de código e segurança em software irá destacar trechos do código que considerar sensíveis. A atividade de inspeção de código tem por objetivo:
- 5.2.20.14.1** Indicar código malicioso inserido pelo desenvolvedor;
  - 5.2.20.14.2** Apontar código inseguro e sugerir melhorias;
  - 5.2.20.14.3** Identificar vulnerabilidades latentes;
  - 5.2.20.14.4** Apontar uso de funções do sistema operacional com problemas conhecidos de segurança;
  - 5.2.20.14.5** Indicar implementações de controles de segurança fora dos padrões e normas.
- 5.2.20.15** Deve-se notar que a Avaliação funcional de segurança com análise de código e segurança em software de código é muito mais eficiente para detectar os ataques de falha de configuração de segurança, falha de controle de acesso e, principalmente, falhas ou backdoors introduzidos propositalmente pelo desenvolvedor. Este último caso, particularmente, só é identificado com inspeção de código.
- 5.2.20.16** Cada ponto fraco identificado é apontado com o código correspondente, descrição do problema e forma de solução.
- 5.2.20.17** Deve ser feita uma análise detalhada e manual do código-fonte do aplicativo. Muitas das vulnerabilidades detectadas em uma análise de código-fonte são semelhantes às vulnerabilidades detectadas durante um Teste de penetração de aplicativo.
- 5.2.20.18** Ao contrário de um teste de penetração, uma análise de código permite uma maior amplitude de cobertura e um aumento no nível de confiança nos resultados da avaliação. Este é principalmente o resultado de ter uma compreensão mais completa do design, da arquitetura de software e de seus componentes internos, o que permite que vulnerabilidades identificadas tenham sua exploração totalmente avaliada a partir de uma perspectiva de risco.
- 5.2.20.19** Algumas vulnerabilidades ou falhas de design também são mais fáceis de detectar em uma análise de código, tal como uma funcionalidade “oculta” em um aplicativo ou deficiências em controles de auditoria.
- 5.2.20.20** Deve-se personalizar o plano de teste para adequar a tecnologia usada pelo aplicativo.
- 5.2.21** *Relatório de Teste de Invasão:*

- 5.2.21.1 A CONTRATADA deverá elaborar “Relatório de Teste de Invasão” para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidades vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências apuradas; fontes de pesquisa, pontos positivos encontrados, referências e ferramentas utilizadas.**
- 5.2.21.2 Os relatórios deverão ser validados junto ao BANPARA, onde poderão ser solicitadas tantas alterações e correções quantas forem necessárias, até que se chegue a uma versão final aceita por ambas as partes.**
- 5.2.21.3 Não serão aceitos relatórios obtidos diretamente por ferramentas automatizadas utilizadas para a realização dos testes, sem a devida transcrição e contextualização adequada, bem como atendimento de todos os requisitos do edital.**
- 5.2.21.4 Os relatórios devem ser entregues na língua portuguesa com atendimento aos requisitos do edital.**
- 5.2.21.5 Deve ser comunicado ao BANPARA, e devidamente documentado, o andamento da análise/teste, especialmente se identificada uma situação crítica.**
- 5.2.21.6 As entregas devem ser realizadas por meio físico e/ou digital a ser definido pelo BANPARA. Se digital disponibilizar: 1 arquivo .doc não protegido contra gravação e 1 arquivo pdf assinado digitalmente com certificado digital ICP Brasil; e protegido por criptografia que deverá conter no mínimo código hash de cada documento, a fim de garantir integridade destas entregas. A versão digital dos documentos deverá ser assinada digitalmente com certificado digital ICP Brasil.**
- 5.2.21.7 Ao final do projeto, deve ser realizada uma apresentação detalhada, nas dependências do BANPARÁ em Belém, com local a ser definido posteriormente, das documentações e conclusões.**
- 5.2.21.8 Para auxiliar na solução para correção das vulnerabilidades identificadas, o relatório deve indicar ao BANPARÁ mais de uma opção de correção para cada item de vulnerabilidade identificado. Estas opções devem ser validadas com BANPARÁ durante a redação dos relatórios, de forma que considerem as peculiaridades do ambiente BANPARA, até o aceite final do mesmo.**
- 5.2.21.9 A CONTRATADA deve fornecer ao BANPARÁ todas informações necessárias para correção da vulnerabilidade, clarificando eventuais dúvidas durante a vigência de todo o contrato.**
- 5.2.22 Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste:**
- 5.2.22.1 Deverão ser entregues 04 (quatro) tipos de relatórios:**

- 5.2.22.1.1 Relatório Técnico de Análise de Vulnerabilidade:** O relatório semestral deve ser entregue ao final de cada ciclo contendo uma visão completa de todas as vulnerabilidades encontradas nos 70 IP's, com a explicação da vulnerabilidade, evidência e procedimento de teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades, conforme requisitos deste documento.
- 5.2.22.1.2 Relatório Técnico de Teste manual das vulnerabilidades do ambiente de TI (interno e externo):** O relatório semestral deve ser entregue ao final de cada ciclo contendo todos os procedimentos efetuados e todos os resultados da etapa do teste de vulnerabilidades manual de infraestrutura nos 70 IP's, com a identificação do problema de segurança, explicação do procedimento detalhado, evidência do teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas no processo de teste de vulnerabilidades manual. Este deve descrever o passo-a-passo de como a vulnerabilidade/falha pode ser explorada, para efeito de validação da solução aplicada por parte do BANPARÁ, e atender itens conforme requisitos deste documento.
- 5.2.22.1.3 Relatório Técnico de Teste manual de vulnerabilidades de aplicações web (se houver distinção):** O relatório mensal ou semestral, conforme estipulado a critério do BANPARÁ na etapa de planejamento, deve ser entregue ao final de cada mês ou ao final de cada ciclo, contendo todos os procedimentos efetuados e todos os resultados da etapa do teste de vulnerabilidades manual de aplicações Web. Deve conter a identificação dos problemas de segurança, explicação do procedimento detalhado, evidência do teste, recomendações concretas e detalhadas para aprimoramento e correção das falhas e vulnerabilidades exploradas no processo de teste de vulnerabilidades manual. Este deve descrever o passo-a-passo de como a vulnerabilidade ou falha pode ser explorada, para efeito de validação da solução aplicada por parte do BANPARÁ, e atender itens conforme requisitos deste documento.
- 5.2.22.1.4 Relatório Executivo Final, com considerações e recomendações:** O relatório anual, a ser entregue ao final do segundo ciclo, deverá conter um histórico com a evolução da situação real do ambiente diante das análises e testes aplicados, bem como processo de mitigação e verificações feitas que elenquem as conclusões do trabalho, recomendações referentes às vulnerabilidades identificadas e exploradas resolvidas e não resolvidas, conforme requisitos deste documento.
- 5.2.23 Sugestão para perfis seguros de estações**
- 5.2.24** Deverão constar como anexos as filmagens dos ataques bem sucedidos (ex. com a utilização de softwares como o Camtasia)
- 5.2.25 Reavaliação, novo teste após remediação**

- 5.2.25.1 A contratada fará novos testes do mesmo tipo em até 60 dias após a correção das vulnerabilidades apontadas no respectivo relatório por parte do Banpará.**
- 5.2.25.2 A contratada não obterá nenhuma informação e acesso sobre serviços e Sistemas da Contratante, devendo por seu próprio esforço obter informações necessárias para análises e testes, quando acordado com BANPARÁ no planejamento.**
- 5.2.26** Os alvos dos testes a serem efetuados, assim como suas condições serão definidos em reunião prévia entre a CONTRATADA e o Banpará.
- 5.2.27** As atividades utilizadas para a execução dos testes não se resumirão apenas ao uso de ferramentas, devendo incluir também procedimentos e técnicas com interação humana e não oferecidos por ferramentas conhecidas.
- 5.2.28** Decorridos 5 (cinco) dias do início efetivo dos testes, a contratada poderá solicitar informações e acessos necessários ao Banpará para obter acesso aos sistemas web como usuário básico com o objetivo de simular possibilidades de escalonamento de privilégios e acessos indevidos à outros níveis/sistemas.
- 5.2.29** Execução das análises de projeto, inspeções de código e testes de invasão com todas as características disponíveis.
- 5.2.30** Utilização de ferramenta como uma aplicação local (mantém todos os dados localmente no seu próprio computador).
- 5.2.31** Utilização de ferramenta Web, instalada no BANPARÁ, para rodar uma análise rápida, sem instalar o software.
- 5.2.32** Para a obtenção das informações poderão ser utilizadas técnicas de Engenharia Social e PhishingScam.

### **5.2.33 Restrições e Limites**

- 5.2.33.1 As janelas de tempo para a execução dos testes serão acordadas entre CONTRATADA e Banpará, priorizando sempre os períodos/horários de menor pico de forma a não impactar no negócio.**

Restrição	Exemplo	Razão da Restrição
Tempo de restrição	Teste de intrusão só poderá ser feito durante final de semana ou dia não útil	reduzir risco de causar impacto durante horas de trabalho normal para assegurar que as atividades do teste sejam controladas e monitoradas devidamente.
Tipo de teste	<ul style="list-style-type: none"><li>• Não executar teste de engenharia social</li></ul>	<ul style="list-style-type: none"><li>• Focar na análise dos resultados técnicos somente</li></ul>

	<ul style="list-style-type: none"><li>• Não execute ataque de força bruta em sistema com autenticação</li></ul>	<ul style="list-style-type: none"><li>• Evitar problemas de bloqueio de credenciais advindo do ataque de força bruta.</li></ul>
IPs e aplicações	<ul style="list-style-type: none"><li>• Não executar teste em IPs não especificados no escopo</li><li>• Teste não deve envolver determinado componente de sistema X</li></ul>	<ul style="list-style-type: none"><li>• Evitar ambiente compartilhado</li><li>• Evitar impacto no negócio com corrupção/interrupção de determinado sistema</li></ul>

#### 5.2.33.2 Tipo de teste a ser feito

#### 5.2.33.3 Redes e aplicações incluídas ou excluídas do escopo

#### 5.2.33.4 Pessoas afetadas

#### 5.2.33.5 Dado autorizado a ser acessado.

**5.2.33.6 Escopo de teste autorizado pelo CONTRATANTE para realização do teste acordado, assinado pelo gestor do contrato. Documento deve conter as tecnologias dos componentes e infraestrutura física, incluindo serviço na nuvem se for o caso.**

**5.2.33.7 Cada fase deve ser feita durante o período que não comprometa processamento da CONTRATANTE e que as agências estejam fechadas sendo feita em no máximo 2 dias corridos no total.**

### 5.2.34 TREINAMENTO ETHICAL HACKING – CAPACITAÇÃO TÉCNICA PARA O ITEM 3

#### 5.2.34.1 PLANEJAMENTO

**5.2.34.2 A CONTRATADA deverá se reunir com os gestores técnico e executivo do contrato, em local a ser definido pela BANPARÁ, no prazo máximo de até 5 (cinco) dias úteis, contados a partir do dia seguinte da solicitação formal do BANPARÁ. A data da reunião deverá ser agendada em comum acordo entre a CONTRATADA e a BANPARÁ.**

Nesta reunião a CONTRATADA deverá alinhar junto ao representante do órgão responsável pela UNIBANP (Universidade Banpará) do BANPARÁ, itens referentes a capacitação técnica, tais como: conteúdo programático, perfil dos participantes,

carga horária, cronograma de execução, infraestrutura, local de realização, material didático, avaliação e demais informações pertinentes ao processo de capacitação.

**5.2.34.3 Como produto da reunião descrita no subitem 5.2.34.2 deste Termo de Referência, a CONTRATADA deverá encaminhar por meio eletrônico, em até 10 (dez) dias úteis após a realização da reunião, o Plano de Capacitação.**

O Plano de Capacitação deverá conter: instrutoria, conteúdo programático, carga horária, cronograma de execução, local de realização e demais informações pertinentes ao processo de capacitação, bem como o material didático a ser utilizado na capacitação.

**5.2.34.4 No prazo de até 5 (cinco) dias úteis, a partir do recebimento formal do Plano de Capacitação, o BANPARÁ deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido a CONTRATADA um novo prazo de até 5 (cinco) dias úteis para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do Plano de Capacitação será a versão aprovada pela Equipe Técnica do BANPARÁ.**

**5.2.35 DA INFRAESTRUTURA DO TREINAMENTO PARA O ITEM 3**

**5.2.36** A **CONTRATADA** será responsável pelo local da capacitação e deverá providencia-lo, seja em suas próprias instalações ou em instalações de terceiros, podendo em acordo com o **BANPARÁ** utilizar a sala de treinamento caso haja disponibilidade. Em qualquer dos casos, o local deverá estar situado em zona considerada de fácil acesso e bem servida de opções de transporte público, observando-se a distância máxima de até 10 km das unidades do **BANPARÁ** nos seguintes locais:

**LOCALIDADE ENDEREÇO**

- **Banpará Municipalidade**  
**End.:** Rua Municipalidade, 1036 - Umarizal - Belém – Pa – CEP: 66.050.350

**5.2.37** Quanto a infraestrutura física, o local deverá dispor de:

- a) Climatização adequada, com regulagem de temperatura;
- b) Adequado isolamento acústico, de forma a impedir que ruídos externos venham a prejudicar a atenção dos treinandos e, conseqüentemente, o aprendizado;
- c) Banheiro masculino e feminino separados e em boas condições de funcionamento e limpeza; e
- d) Mobiliário (cadeiras e mesas) ergonômico e adequado para uso de computador.

**5.2.38** Quanto a infraestrutura tecnológica e de ensino, o local deverá oferecer equipamento, capaz de suportar de maneira eficaz e ininterrupta o funcionamento da solução e demais softwares necessários, direta ou indiretamente, a transmissão dos conhecimentos, tendo em vista a satisfatória contemplação dos objetivos da capacitação, exigindo-se:

- a) Um computador por treinando, tanto em atividades teóricas quanto práticas;
- b) Rede local conectada a internet, com sinal estável e velocidade compatível com o fluxo de dados que será exigido pelas atividades a serem desenvolvidas, caso necessário;
- c) Ambientes de máquinas virtuais adequadamente configurados e em pleno funcionamento, caso sejam utilizados;
- d) Projetor multimídia; e
- e) Quadro branco.

**5.2.39** As turmas de capacitação deverão ser realizadas no local estabelecido na versão definitiva do plano de capacitação (descrito no **subitem 5.2.34.4** deste **Termo de Referência**). O local poderá ser alterado, desde que seja realizado em comum acordo entre a **CONTRATADA** e o **BANPARÁ**. Neste caso, a **CONTRATADA** deverá comunicar formalmente o **BANPARÁ** sobre o local onde a capacitação será ministrada, **com antecedência mínima de 15 (quinze) dias úteis** do início da realização da mesma.

**5.2.40** O **BANPARÁ** reserva-se o direito de realizar, se julgar necessária, visita de vistoria ao local em que deverá ocorrer a capacitação de forma a se assegurar do atendimento de todas as exigências aqui relacionadas a infraestrutura.

**5.2.41** Caso o **BANPARÁ** constate algum problema ou irregularidade durante a vistoria, notificará a **CONTRATADA**, que terá o prazo máximo de **5 (cinco) dias úteis**, contados a partir do dia seguinte a confirmação de recebimento da notificação, para sanar tais problemas ou para providenciar um novo local. Se tais ações não forem tomadas pela **CONTRATADA**, a realização da capacitação estará suspensa até que o **BANPARÁ** aprove definitivamente as instalações.

**5.2.41.1** **Caso, no decorrer das capacitações, sejam identificados problemas no local que contrariem os requisitos expressos neste Termo de Referência e afetem a qualidade dos serviços, o BANPARÁ poderá exigir a sua mudança devendo ser prontamente atendida pela CONTRATADA.**

### **5.2.42 REQUISITOS DE QUALIFICAÇÃO TÉCNICA PARA O ITEM 3**

- a) Atestado de Capacidade técnica, conforme ADENDO III, que comprove a experiência em ministrar o objeto do item 3.
- b) 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.
- c) Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes aos mesmo grupo empresarial da **CONTRATADA**.
- d) O atestado de capacidade técnica 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.

#### **5.2.43 CONDIÇÕES DE CONTRATAÇÃO - PARA O ITEM 3**

**5.2.44** A **CONTRATADA** deverá apresentar ao **BANPARÁ** os dados do instrutor, que deverá possuir certificação do fabricante da solução adquirida, que lhe confira as competências necessárias para ministrar a capacitação nas disciplinas descritas no **subitem 5.2.48** deste Termo de Referência juntamente com Atestado de Capacidade técnica, conforme ADENDO III, que comprove a experiência em ministrar o objeto do item 3.

**5.2.45** A certificação exigida no **subitem 5.2.44** deve estar válida durante o período de prestação da capacitação.

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

**5.2.47** A capacitação técnica deverá ser ministrada em língua portuguesa **obrigatoriamente**.

#### **5.2.48 DISCIPLINAS E COMPOSIÇÃO DAS TURMAS PARA O ITEM 3**

**5.2.49** A capacitação técnica nas disciplinas abaixo descritas deverá contemplar **2 (duas) turmas fechadas**, com no **mínimo 15 (quinze) participantes**, a serem realizadas sob demanda, considerando a duração mínima de **40 (quarenta) horas** por turma.

**5.2.50** A capacitação técnica provida deverá abranger, no mínimo, os seguintes tópicos:

1. Planejamento e preparação
  - 1.1. Escopo do Teste
  - 1.2. Perfil do atacante
  - 1.3. Limitações de Tempo
  - 1.4. Tratamento de questões especiais
  - 1.5. Permissão
  - 1.6. Detalhes da Infraestrutura
  - 1.7. Acordo de confidencialidade (NDA)
  - 1.8. Equipamento e recursos necessários
  - 1.9. Relatório de linha do tempo
  - 1.10. Acesso a testes anteriores
  - 1.11. Inspeção física
2. Obtenção de Informações
  - 2.1. Whois
  - 2.2. Buscas na Internet
  - 2.3. Entradas DNS
  - 2.4. Engenharia Social
  - 2.5. Trashing (Dumpster Diving)
  - 2.6. Cópia de Website
  - 2.7. Ferramentas

3. Sondagem e mapeamento
  - 3.1. Busca por hosts vivos
  - 3.2. Varredura por portas e serviços
  - 3.3. Mapeamento de perímetro
  - 3.4. Identificando serviços críticos
  - 3.5. Fingerprinting de SO's e serviços
  - 3.6. Identificando rotas
  - 3.7. Ferramentas
  
4. Identificação de Vulnerabilidades
  - 4.1. Identificação de Serviços Vulneráveis
  - 4.2. Varredura por vulnerabilidades
  - 4.3. Senhas padrão
  - 4.4. Correlacionamento de vulnerabilidades
  - 4.5. Enumeração de vulnerabilidades encontradas
  - 4.6. Ferramentas
  
5. Invasão
  - 5.1. Quebrando senhas
  - 5.2. Ataques a aplicações Web
    - 5.2.1. Injeção de SQL
    - 5.2.2. Buffer Overflow
    - 5.2.3. Cross-site Scripting (XSS)
    - 5.2.4. Execução Remota de Código
    - 5.2.5. Vulnerabilidades de Strings de Formatação
    - 5.2.6. Autenticação e Autorização Fracas (enumeração, senhas, SIDs)
  - 5.3. Ataques de negação de serviço
  - 5.4. Escalada de Privilégios
  - 5.5. Enumeração posterior
    - 5.5.1. Quebra offline de senhas
    - 5.5.2. Sniffing e análise de tráfego
  - 5.6. Mantendo Acesso
    - 5.6.1. Canais secretos
    - 5.6.2. Backdoors
    - 5.6.3. Rootkits
  - 5.7. Apagando Rastros
    - 5.7.1. Escondendo arquivos
    - 5.7.2. Limpando Logs
    - 5.7.3. Vencer Verificadores de Integridade
    - 5.7.4. Burlar antivírus
  - 5.8. Segurança Física
    - 5.8.1. Pontos de rede
    - 5.8.2. Informações expostas
    - 5.8.3. Conversas de funcionários
    - 5.8.4. Janelas, fechaduras e portas de acesso
    - 5.8.5. Pontos de entrada
    - 5.8.6. Guardas/Recepcionistas
    - 5.8.7. Lixo
  - 5.9. Ferramentas
  
6. Finalizando
  - 6.1. Gerando relatório
  - 6.2. Limpeza do Sistema

**5.2.51** As turmas de capacitação deverão ser realizadas durante a vigência contratual, conforme estabelecido no cronograma de execução aprovado pelo **BANPARÁ** na versão definitiva do plano de capacitação (descrito no **subitem 5.2.34.2** deste **Termo de Referência**). Este cronograma poderá sofrer alterações, desde que essas sejam realizadas em comum acordo entre a **CONTRATADA** e o **BANPARÁ**.

**5.2.52** As turmas deverão ser realizadas no horário compreendido entre 08:00 e 18:00 horas, de segunda a sexta-feira, em turno integral ou parcial, não podendo haver duas turmas na mesma semana.

**5.2.53** Conforme prática de mercado, as horas de intervalo para almoço dos treinandos não deverão ser computadas para fins de cálculo da carga horária.

#### **5.2.54 MATERIAL DIDÁTICO PARA O ITEM 3.**

**5.2.55** A **CONTRATADA** deverá fornecer o material didático de acompanhamento detalhado, original do fabricante, **preferencialmente em português**, contendo todos os assuntos abordados na capacitação. Entende-se como material didático, apostilas, slides de apresentações, manuais, livros textos, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em português do material original do fabricante, será aceito apenas material em inglês.

**5.2.56** As apostilas ou manuais impressos deverão ser oferecidas em quantidade idêntica ao número de treinandos, com conteúdo oficial do fabricante e atualizado, de acordo com a versão da solução a ser ministrada.

**5.2.57** O **BANPARÁ** reserva-se o direito de realizar a validação técnica e pedagógica do material didático por meio do setor UNIBANP, podendo vir a solicitar a **CONTRATADA** eventuais correções ou adequações.

#### **5.2.58 AVALIAÇÃO DA CAPACITAÇÃO PARA O ITEM 3**

**5.2.59** Ao término de cada turma, será realizada uma Avaliação tendo em vista a medição e avaliação da qualidade da capacitação. O **BANPARÁ** aplicará a Avaliação em todos os treinandos, através de formulário web o qual será disponibilizado acesso por e-mail, com o objetivo de avaliar a satisfação com a capacitação.

**5.2.60** Caso a **CONTRATADA**, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão do **BANPARÁ**, ela poderá utilizar o seu próprio formulário, porém o mesmo não será utilizado para aprovação da capacitação por parte do **BANPARÁ**.

**5.2.61** Cinco fatores serão objeto de avaliação pelo formulário, a dizer: Instrutoria, Material Didático, Conteúdo Programático, Ambiente da Capacitação e Autoavaliação:

- **Instrutoria** - Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto a sua habilidade didático-pedagógica e de interação com a turma.

- **Material Didático** - Avalia a percepção dos participantes sobre a adequação e clareza do material didático utilizado na capacitação.
- **Conteúdo Programático** - Avalia a percepção dos treinandos quanto ao equilíbrio entre teoria e prática, nível de profundidade, exemplos de exercícios, aderência e aplicabilidade.
- **Ambiente da Capacitação** - Avalia a infraestrutura física e técnica utilizada para a capacitação.
- **Autoavaliação** - Avalia a percepção dos participantes quanto a aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado.

Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio da utilização de quatro conceitos, quais sejam: **Fraco, Regular, Bom e Excelente**.

**5.2.62** Para fins de avaliação dos fatores, na fase de tabulação dos resultados, a cada conceito atribuído a um item, corresponderá um peso. Após o cálculo da média ponderada alcançada por cada grupo de itens, será obtida a média geral dos fatores correspondentes.

Na avaliação geral de cada fator, para fins de atribuição do conceito final da ação, serão utilizados os seguintes intervalos numéricos:

Conceito	Peso	Intervalo
Ruim	1	de 0 a 1,59
Regular	2	de 1,60 a 2,59
Bom	3	de 2,60 a 3,59
Muito Bom	4	de 3,60 a 4,00
Excelente	5	de 4,01 a 5,00

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

**5.2.63** Com base nas informações registradas pelos participantes no Formulário de Avaliação do **BANPARÁ**, a **CONTRATADA** deverá emitir o Relatório Consolidado da Avaliação com a média calculada da turma para cada fator da avaliação e respectivos itens. A **CONTRATADA** deverá enviar para ao setor UNIBANP do **BANPARÁ**, em até **5 (cinco) dias úteis** após o encerramento de cada turma, por meio eletrônico, os Formulários de Avaliação preenchidos e assinados pelos treinandos (digitalizados) e o Relatório Consolidado da Avaliação.

**5.2.64** A capacitação técnica provida pela **CONTRATADA** será submetida a aprovação por parte do **BANPARÁ**, conforme descrito nos **subitens 5.2.58 e 5.2.65**

### **5.2.65 GARANTIA DA CAPACITAÇÃO PARA O ITEM 3**

**5.2.66** O resultado da capacitação será considerado **INSATISFATÓRIO** quando pelo menos uma das situações abaixo ocorrer:

- a) Média final da turma igual ou inferior ao conceito regular, excluindo-se o fator **Autoavaliação**;
- b) Média do fator **Instrutoria** igual ou inferior ao conceito regular;

- c) Média de, pelo menos, dois fatores igual ou inferior ao conceito regular, excluindo-se o fator **Autoavaliação**.

**5.2.67** A **CONTRATADA** será obrigada a realizar, sem ônus para o **BANPARÁ**, nova capacitação para todas as turmas em que ficar configurado como resultado **INSATISFATÓRIO**. A critério do **BANPARÁ**, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados. A nova capacitação deverá acontecer segundo um novo calendário a ser definido pelo **BANPARÁ**.

**5.2.68** No caso da turma obter o resultado da avaliação **INSATISFATÓRIO**, o cronograma aprovado será automaticamente suspenso até que os problemas identificados sejam considerados sanados pelo **BANPARÁ**.

### **5.2.69 ENTREGA DOS MATERIAIS UTILIZADOS NA CAPACITAÇÃO PARA O ITEM 3**

**5.2.70** Após a conclusão da capacitação, a **CONTRATADA** deverá fornecer ao **BANPARÁ** uma cópia da apresentação utilizada em mídia eletrônica (CD, DVD ou PENDRIVE), em formatos padrão de mercado (PDF, DOC, PPT ou HTML).

**5.2.71** O **BANPARÁ** se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes, para realizar capacitações internas de seus empregados.

### **5.2.72 CERTIFICADOS E LISTA DE PRESENÇA PARA O ITEM 3**

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

**5.2.74** A **CONTRATADA** deverá enviar ao **BANPARÁ** lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos, através de suas assinaturas em cada dia de capacitação.

**5.2.75** Para fins de comprovação dos serviços prestados, visando o faturamento, a **CONTRATADA** deverá encaminhar para a **área da UNIBANP** do **BANPARÁ**, em até **5 (cinco) dias úteis** após o encerramento de cada turma, os certificados e o documento de presença digitalizados.

## **6 Níveis Mínimos de Serviço/ Indicadores de Desempenho Esperados Para os Itens 1 e 2.**

---

- 6.1** A ferramenta de análise de vulnerabilidade comercial deverá contemplar, ao menos, as seguintes características que serão comprovadas através de relatórios:
- 6.1.1** Prover identificação e correlação de ameaças, além de avaliar o potencial risco das vulnerabilidades encontradas;
  - 6.1.2** Fornecer evidências de ativos “não vulneráveis” através de provas conclusivas como:
    - 6.1.2.1.1 Resultados de varreduras esperados e obtidos;**
    - 6.1.2.1.2 Lista de ativos não analisados;**
    - 6.1.2.1.3 Falhas nas varreduras.**
  - 6.1.3** A solução de análise de vulnerabilidades não deve ser baseada na necessidade de instalação prévia de agentes no ambiente corporativo pela CONTRATANTE.
  - 6.1.4** Resultados de varredura enviados para o banco de dados através da rede corporativa devem ser criptografados.
  - 6.1.5** Fornecer cobertura de conteúdo para executar verificações com autenticação e sem autenticação.
  - 6.1.6** Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando as credenciais para se autenticar em sistemas Windows, UNIX ou qualquer ativo de infraestrutura, tais como dispositivos de rede, etc;
  - 6.1.7** Permitir o acesso seguro ao back-end do banco de dados de modo a permitir a mineração de dados para possíveis relatórios personalizados que sejam solicitados;
  - 6.1.8** Deve ter certificado pelo EAL Common Criteria e validar criptografia FIPS-140-2.
  - 6.1.9** Suportar métricas de pontuação baseadas em risco;
  - 6.1.10** O processo de varredura deve ter um impacto mínimo sobre a rede, não superior a 10 Mbps de tráfego (podendo ser revisto após discussão e aprovação da CONTRATANTE);
  - 6.1.11** Permitir o ajuste de desempenho para adequar a quantidade de banda consumida na rede durante a varredura de análise de vulnerabilidade, tanto para a realização de varreduras mais rápidas que consomem mais recursos;
  - 6.1.12** A descrição de vulnerabilidade deve possuir no mínimo os seguintes detalhes:
    - 6.1.12.1 Nome;**
    - 6.1.12.2 Nível de Risco;**
    - 6.1.12.3 Intrusiva (sim/não)**

6.1.12.4 Descrição;

6.1.12.5 Observação;

6.1.12.6 Recomendação de remediação;

6.1.12.7 Link do patch ou da correção;

6.1.12.8 Número CVE;

6.1.12.9 SANS / FBI referência Top 20;

6.1.12.9.1 IAVA (Information Assurance Vulnerability Alert) Referência

6.1.12.10 Realizar análise de vulnerabilidades Segundo as seguintes tecnologias:

6.1.12.10.1 XCCDF

6.1.12.10.2 OVAL

6.1.12.10.3 CVSS

6.1.12.10.4 CVE

6.1.12.10.5 CPE

6.1.12.10.6 CCE

6.1.13 Em caso de problemas durante a execução dos testes de penetração/vulnerabilidade o BANPARÁ acionará a Contratada para manutenções corretivas. Ao acionar a CONTRATADA o BANPARÁ classificará o problema em um dos níveis de criticidade da tabela a seguir Cada nível de severidade possui diferentes níveis mínimos de serviço, conforme descrito também nas tabelas a seguir:

CLASSIFICAÇÃO DE EVENTOS	
(A) EMERGENCIAL	São consideradas como “Emergência” todas as falhas cujas consequências tenham impactos sobre o serviço, rede, tráfego de dados e sincronismo e/ou recursos de manutenção (Ex.: sistema de bancários) que exigem ação corretiva imediata (independente da hora do dia ou do dia da semana).
(B) ALTA PRIORIDADE	Situações que podem configurar uma severidade emergencial. São situações potenciais e exigem atenção imediata. São situações potenciais que precedem, em sua maioria, uma situação que pode ser classificada num segundo momento como severidade emergencial.
(C) MÉDIA PRIORIDADE	Problemas que não prejudicam significativamente o funcionamento dos sistemas / serviços. São problemas graves ou perturbações que afetam uma área específica de determinada funcionalidade. Exemplos: degradação de desempenho, perda de funcionalidades.

(D) BAIXA PRIORIDADE E CONSULTA	Consulta geral e problemas secundários que têm um efeito pequeno na funcionalidade do produto. Ex.: Falhas de documentação, falhas no projeto e questionamentos operacionais.
---------------------------------	---

NÍVEL	SEVERIDADE	TEMPO PARA RESTABELECIMENTO DO SISTEMA APÓS ABERTURA DO CHAMADO	TEMPO PARA SOLUÇÃO DEFINITIVA DO PROBLEMA
A	EMERGENCIAL	até 1 hora	até 4 dias corridos
B	ALTA PRIORIDADE	até 2 horas	até 7 dias corridos
C	MEDIA PRIORIDADE	até 4 horas	até 10 dias corridos
D	BAIXA PRIORIDADE E CONSULTA	Até 24horas	até 15 dias corridos

## 7 Das Definições do Acordo de Nível de Serviços (SLA).

**7.1** A CONTRATADA deverá cumprir rigorosamente os prazos estabelecidos pelo Banco referente à prestação dos serviços conforme Item 6.1.13, no caso de extrapolação dos prazos definidos será aplicado um redutor sobre o valor da fatura mensal do contrato, referente a cada nível de severidade, conforme tabela abaixo:

**7.2** O redutor será aplicado por hora corrida extrapolada em relação ao Tempo de Para Restabelecimento do Sistema Após Abertura do Chamado.

NÍVEL DE SEVERIDADE	REDUTOR	REFERÊNCIA
A	0,5%	Fatura Global
B	0,4%	Fatura Global
C	0,2%	Fatura Global
D	0,1%	Fatura Global

- 7.3** O Total de descontos não poderá extrapolar 20% da fatura global.
- 7.4** A CONTRATADA deverá cumprir os níveis de serviço que estão expostos na seção de sanções.
- 7.5** Os descontos serão efetuados quando da emissão da fatura do respectivo pedido.
- 7.6** O Banco comunicará formalmente a CONTRATADA, via email, o percentual de SLA a ser aplicado.
- 7.7** Os Atrasos de qualquer natureza deverão ser justificados formalmente ao CONTRATANTE.
- 7.8** Os Acordos de Níveis de Serviços – SLA poderão ser aplicados cumulativamente.

## **8 Dos Requisitos de Habilitação**

---

- 8.1** Requisitos de Qualificação Técnica Para os Itens 1 e 2
- 8.1.1** A empresa licitante deverá apresentar pelo menos dois atestados de capacidade técnico-operacional (ADENDO III) emitido por pessoa jurídica de direito público ou privado, onde são ou foram prestados pelo menos os seguintes serviços: Testes de Invasão poderá ser do tipo Externos e/ou Internos nos sistemas (web e legados), processos e ativos de infraestrutura tecnológica (rede cabeada e wi-fi) nos 12 meses anteriores a licitação deste edital com comprovação. Estas obrigações dar-se-ão devido a sensibilidade das informações da instituição que serão expostas nos testes, sendo assim é necessário termos empresas qualificadas para a execução do objeto deste Termo de Referência.
- 8.1.2** 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.
- 8.1.3** Nos casos de atestado(s)/certidão(ões)/declaração(ões) emitidos por empresas da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes aos mesmo grupo empresarial da CONTRATADA.
- 8.1.4** O atestado de capacidade técnica 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.
- 8.1.5** Certidão Negativa de Licitante Inidôneo do Tribunal de Contas do Estado do Pará e do Tribunal de Contas da União.

**8.2** PERFIS PROFISSIONAIS PARA OS ITENS 1 E 2

- 8.2.1** 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.
- 8.2.2** 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.
- 8.2.3** A CONTRATADA deve retirar dos serviços qualquer empregado que, a critério do BANPARÁ, seja julgado inconveniente ao bom andamento dos trabalhos;
- 8.2.4** Comprovação de possuir no seu quadro permanente no ato da contratação, no mínimo, em conjunto de profissionais com os certificados abaixo:

**8.2.5 Gerente de Projetos**

ITEM	DESCRIÇÃO
<b>PERFIL E EXPERIÊNCIA PROFISSIONAL</b>	
Gerência de Projetos	Deverá ter experiência comprovada em, no mínimo, 03 (três) projetos em gerência de projetos de pen tests/ethical hacking com objeto semelhante ao descrito neste edital devido a rápida evolução tecnológica em relação as execuções de testes.
<b>CAPACITAÇÃO</b>	
Nível Superior	Possuir graduação em de Bacharel em Ciências da Computação ou Engenharia da Computação ou área afim e Pós-Graduação em áreas afim. (stricto sensu).
Certificação PMP e CISM	Possuir certificação PMP (Project Management Professional) e Certified Information Security Manager - CISM, emitida pelo PMI dentro do período de validade.

**8.2.6 Responsável Técnico e sua Equipe**

ITEM	DESCRIÇÃO
<b>PERFIL E EXPERIÊNCIA PROFISSIONAL</b>	
Análise de Vulnerabilidades	Deverá ter experiência de, no mínimo, 03 (três) anos em execução de teste de intrusão, devido a rápida evolução tecnológica em relação as execuções de testes.
<b>CAPACITAÇÃO</b>	
Certificação Profissional em Segurança da Informação com foco em Auditoria e Gestão	Possuir certificação CISA (Certified Information Systems Auditor) ou CISSP (Certified Information Systems Security Professional)
Certificação Técnica em Segurança da Informação	CompTIA Cybersecurity Analyst (CySA+), CompTIA Security+ e CompTIA Security Analytics Professional (CSAP), Certified Ethical Hacker (CEH), ITIL Foundation Examination V3 e ISO/IEC 27001.
Nível Superior	Possuir graduação em de Bacharel em Ciências da Computação ou Engenharia da Computação ou área afim e Pós-Graduação em áreas afim. (stricto sensu).

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

- 8.2.8** A prestação do Serviço de Teste de Invasão em Redes e Sistemas deverá ser realizada por equipe de profissionais que possua, pelo menos 5 (cinco) das seguintes certificações, pois para o objeto é necessário que o profissional possua certificações para executar com a melhor técnica os testes de intrusão devido a rápida evolução tecnológica:

Item	Certificação
1	Data Protection Officer (DPO)
2	Certified Information Security Manager (CISM)
3	Certified Information Systems Security Professional (CISSP)
4	EC-Council Certified Ethical Hacker (CEH)
5	EC-Council Licensed Penetration Tester (LPT) Master
6	CompTIA Cybersecurity Analyst (CySA+)
7	CompTIA Security+
8	CompTIA Security Analytics Professional (CSAP)
9	ISO/IEC 27001 - Information Security Management
10	IACRB Certified Penetration Tester (CPT)
11	CompTIA Security+ (SYO-401)
12	EXIN Privacy and Data Protection Practitioner
13	EXIN Privacy and Data Protection Foundation
14	Certified Expert Penetration Tester (CEPT)
15	Certified Mobile and Web Application Penetration Tester (CMWAPT)
16	ITIL Foundation Examination V3
17	Certified Red Team Operations Professional (CRTOP)
18	CompTIA PenTest +
19	Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
20	Global Information Assurance Certification (GIAC) Web Application Penetration Tester (GWAPT)
21	Global Information Assurance Certification (GIAC) Certified Intrusion Analyst (GCIA)
22	Global Information Assurance Certification (GIAC) Exploit Researcher and Advanced Penetration Tester (GXPN)
23	Offensive Security Certified Professional (OSCP)
24	EC Council Security Analyst (ECSA)
25	Certified Mobile and Web Application Penetration Tester (CMWAPT)
26	Certified Secure Software Lifecycle Professional (CSSLP)

- 8.2.9** A CONTRATADA deverá apresentar também, na assinatura do contrato, a lista 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.
- 8.2.10** O Responsável Técnico deverá, durante as análises e testes internos, estar presente, no mínimo 1 (um) dia por semana nas dependências do CONTRATANTE para efetuar o acompanhamento dos serviços e repassar as informações para o CONTRATANTE;
- 8.3** Dos Documentos Comprobatórios aos Critérios de Sustentabilidade
- 8.3.1** A contratada se compromete, sob pena de infração e rescisão contratual, a:
- 8.3.2** 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;
- 8.3.3** 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;
- 8.3.4** 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;
- 8.3.5** Respeitar o direito de formar ou associar-se a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias;
- 8.3.6** Buscar a incorporação em sua gestão dos Princípios do Pacto Global, disponível em <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>;
- 8.3.7** 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;
- 8.3.8** 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.

**8.3.9** 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.

**8.3.10** Plano de Gerenciamento de Resíduos Sólidos ou Declaração de Sustentabilidade Ambiental;

**8.3.11** 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.

**8.4** Da Qualificação Econômico-Financeira para os itens 1, 2 e 3.

8.4.1. Na habilitação econômico financeira, a Licitante deverá apresentar os seguintes documentos:

**8.4.1.1. Certidão negativa de pedido de falência, expedida pelo cartório distribuidor da comarca da sede da pessoa jurídica;**

- 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.

**8.4.1.2. 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 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;
- 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, Demonstração do Resultado do Exercício, Demonstração de lucros ou prejuízos acumulados e Demonstração de mutações do patrimônio líquido extraídos do Sistema Público de Escrituração Digital – Sped.**

**8.4.1.3. 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;

**9.4.1.4. Declaração do licitante**, acompanhada da relação de compromissos assumidos, conforme modelo constante do **ADENDO IV**, de que **um doze avos** dos contratos firmados com a Administração Pública e/ou com a iniciativa privada **vigentes na data apresentação da proposta não é superior ao Patrimônio Líquido do licitante**, observados os seguintes requisitos:

**Fórmula de cálculo:**

Valor do Patrimônio Líquido x 12 > 1

Valor total dos contratos

**Obs.:** Esse resultado deverá ser superior a 1.

Exemplo: Declaração – R\$ 120.000,00 (valor total dos Contratos vigentes)

Patrimônio Líquido deve ser superior a R\$ 10.000,00 (1/12 avos de R\$ 120.000,00 = R\$ 10.000,00)

Exemplo numérico 1: considerando o Patrimônio Líquido de R\$ 20.000,00

Valor do Patrimônio Líquido – R\$ 20.000,00

Valor Total dos Contratos – R\$ 120.000,00

**Cálculo:** 20.000 x 12 = 2 > 1

120.000

1/12 avos de R\$ 120.000,00 = R\$ 10.000,00

Patrimônio Líquido deve ser superior a R\$ 10.000,00

Cálculo demonstrativo visando a comprovar que o Patrimônio Líquido não é superior a 1/12 (um doze avos) do valor dos Contratos firmados com a Administração Pública e com a iniciativa privada.

Exemplo numérico 2: considerando o Patrimônio Líquido de R\$ 5.000,00

Valor do Patrimônio Líquido – R\$ 5.000,00

Valor Total dos Contratos – R\$ 120.000,00

**Cálculo:**  $\frac{5.000}{120.000} \times 12 = 0,5 < 1$

120.000

- a) A declaração deve ser acompanhada da Demonstração do Resultado do Exercício – DRE, relativa ao último exercício social;
- b) Caso a diferença entre a declaração e a Receita Bruta discriminada na Demonstração do Resultado do Exercício – DRE apresentada seja superior a 10% (dez por cento), para mais ou para menos em relação à receita bruta, **o licitante deverá apresentar justificativas.**

#### **Fórmula de cálculo:**

$$\frac{(\text{Valor da Receita Bruta} - \text{Valor total dos Contratos}) \times 100}{\text{Valor da Receita Bruta}} =$$

**Obs.:** Caso o percentual encontrado seja maior que 10% (positivo ou negativo) em relação à receita bruta, a licitante deverá apresentar as devidas justificativas.

Exemplo numérico 1: considerando a Receita Bruta de R\$ 130.000,00;

considerando o Valor Total dos Contratos – R\$ 120.000,00

**Cálculo:**  $\frac{(130.000 - 120.000)}{130.000} \times 100 = 7,69\% < 10\%$

130.000

**Obs.:** Para essa situação, não é necessário justificativa.

Exemplo numérico 2: considerando a Receita Bruta de R\$ 150.000,00;  
considerando o Valor Total dos Contratos – R\$ 120.000,00

$$\text{Cálculo: } \frac{(150.000 - 120.000)}{150.000} \times 100 = 20\% > 10\%$$

**Obs.:** Para essa situação, é necessário justificativa.

**8.4.1.5.** Apresentar boa situação financeira por meio da satisfação de índices de Liquidez Geral (**LG**), de Liquidez Corrente (**LC**) e de Solvência Geral (**SG**) > 1.0 (maior que 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:

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

b) As empresas que apresentarem quaisquer dos índices calculados na alínea anterior menor ou igual a 1,0 (um) deverão comprovar Capital Social ou Patrimônio Líquido de valor não inferior a 10% (trinta 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.

d) certidão negativa de feitos sobre falência da sede do interessado.

## 8.5 Da Visita Técnica

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

## 9 Da Adjudicação do Objeto

---

Por item.

---

## **10 Das Condições de Contratação – para o item 1 e 2**

---

- 10.1** A empresa licitante deverá demonstrar qualificação técnica necessária à prestação dos serviços apresentando material que comprove a posse de portfólio de serviços de segurança da informação sendo uma condição de contratação.
- 10.2** A empresa deve apresentar currículo assinado pelo próprio profissional, de pelo menos um dos profissionais que participarão dos testes de intrusão, que contemple ao menos três dos seguintes requisitos:
- 10.2.1** OSSTMM 3 (The Open Source Security Testing Methodology Manual: at least those three channels PHYSSEC, SPECSEC, COMSEC or/and any new one which will be defined);
- 10.2.2** ISSAF/PTF (Information Systems Security Assessment Framework);
- 10.2.3** NIST Special Publication 800-115 (Technical Guide to Information Security Testing and assessment);
- 10.2.4** NIST Special Publication 800-42 (Guideline on Network Security Testing)
- 10.2.5** OWASP TESTING GUIDE 3.0 – The Open Web Application Security Project.
- 10.2.6** PCI DSS (Payment Card Industry Data Security Standard)
- 10.2.7** PCI SSC Information Supplement
- 10.2.8** PTES (Penetration Testinf Execution Standard)
- 10.2.9** As certificações apresentadas no item anterior garantem que a empresa vencedora executará com excelência o objeto do certame, uma vez que são certificações voltadas para os Testes de Intrusão, reconhecidas nacional e internacionalmente.

---

## **11 Da Garantia**

---

### **11.1 Da Garantia Contratual**

- 11.1.1** 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.
- 11.1.2** A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
- a) Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
  - b) Prejuízos causados à administração ou à terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
  - c) As multas moratórias e punitivas aplicadas pela Administração à **CONTRATADA**;
  - d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela **CONTRATADA**.
- 11.1.3** Não serão aceitas garantias na modalidade seguro-garantia em cujos termos não constem expressamente os eventos indicados nas letras “a” a “d” desta cláusula.
- 11.1.4** 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.
- 11.1.5** A garantia na modalidade fiança bancária deverá ser apresentada, conforme o modelo referente ao **ADENDO V**.
- 11.1.6** 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).
- 11.1.7** O garantidor deverá declarar expressamente que tem plena ciência dos termos do Edital e das cláusulas contratuais.
- 11.1.8** 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**.
- 11.1.9** 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.

- 11.1.10** Isenção de responsabilidade da garantia:
- 11.1.11** O Banpará não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:
1. Caso fortuito ou força maior;
  2. Alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;
  3. Descumprimento das obrigações pela **CONTRATADA** decorrentes de atos ou fatos praticados pela Administração;
  4. Atos ilícitos dolosos praticados por servidores da Administração.
- 11.1.12** Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.
- 11.1.13** 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.
- 11.2** Da Garantia do Objeto
- 11.2.1** O Prazo de Garantia do objeto fornecido é o previsto na legislação vigente, ou aquele ofertado pelo fabricante.
- 11.2.2** Os produtos objeto destas Especificações Técnicas deverão ser garantidos contra defeitos oriundos de projeto, fabricação ou materiais diferentes dos especificados, no prazo de garantia fixado pelo fabricante, que deverá estar expresso na proposta, em caso de não atendimento à garantia quando constatadas no momento apropriado, o fornecedor, além de multas, deverá efetuar o ressarcimento dos prejuízos de acordo com a legislação vigente.
- 11.2.3** 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.

## **12 Características e Condições da Execução do Contrato**

---

- 12.1** A execução do contrato será iniciada a partir da assinatura do mesmo.
- 12.2** Da validade
- 12.2.1** 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.

### 12.3 Da Entrega

- 12.3.1** A empresa contratada deverá entregar à equipe da GESEI – Gerência de Segurança da Informação todo detalhamento dos testes de invasão a serem realizados, desde os ativos que foram testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.
- 12.3.2** O teste de invasão de redes só poderá acontecer mediante autorização da GESEI – Gerência de Segurança da Informação, com anuência da GEHAS – Gerência de Hardware e Software
- 12.3.3** O teste de invasão de sistemas só poderá acontecer mediante autorização da GESEI – Gerência de Segurança da Informação, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.
- 12.3.4** Os serviços serão solicitados sob demanda por meio de ordem de serviço ADENDO IX, a ser emitida pelo BANPARA;
- 12.3.5** Os serviços deverão ser prestados localmente da sede do BANPARA, salvo aprovação e autorização em contrário pelos fiscais do contrato, mediante justificativa a ser emitida pela CONTRATANTE;
- 12.3.6** O BANPARÁ irá solicitar o serviço a ser executado, sempre que achar necessário, mediante a validação de escopo entre as partes;
- 12.3.7** O escopo dos serviços deverá ser acordado entre o BANPARÁ e a CONTRATADA por meio de reuniões para definição do escopo, de estimativa de esforço, cronograma e prazo para o início da execução da ordem de serviço
- 12.3.8** A execução será sempre precedida de emissão de Ordem de Serviço (OS), contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados, técnicos que atuarão no projeto;
- 12.3.8.1** **Não serão aceitos técnicos que não tenham as certificações exigidas neste edital;**
- 12.3.8.2** **Uma Ordem de Serviço (OS) somente será autorizada após conferência e ateste do Gestor do Contrato;**
- 12.3.8.3** **Toda OS deverá ser assinada pelo Preposto da Empresa Contratada perante a CONTRATANTE, declarando a concordância da Contratada em executar as atividades descritas na OS de acordo com as especificações estabelecidas;**
- 12.3.8.4** **Os serviços deverão estar sempre de acordo com as especificações constantes nas OS;**

- 12.3.8.5 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução - quando a OS é emitida, durante a execução - com o acompanhamento e supervisão de responsáveis da CONTRATANTE, e ao término da execução - com o fornecimento dos respectivos relatórios pela CONTRATADA e atesto dos mesmos pelos respectivos responsáveis;**
- 12.3.8.6 Todos os serviços prestados pela Contratada deverão ser necessariamente documentados (passo-a-passo), registrados e entregues ao BANPARÁ em forma digital complementarmente aos relatórios dos serviços;**
- 12.3.9** Uma vez definido escopo, prazo e cronograma, o início da execução dos serviços deverá ocorrer na data e prazo previstos.
- 12.3.10** Caso o trabalho ultrapasse a quantidade de horas estimadas, o BANPARÁ deverá ser informado imediatamente que deliberará sob a nova quantidade estimada.
- 12.3.11** O aceite e o posterior pagamento dos serviços não eximem a Licitante vencedora das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades causadas por estes.
- 12.3.12** Será designado representante para acompanhar e fiscalizar a realização dos serviços, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.
- 12.3.13** As decisões e providências que ultrapassarem a competência do representante deverão ser solicitadas ao seu gestor, em tempo hábil para adoção das medidas convenientes.
- 12.3.14** O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.
- 12.3.15** O BANPARA, poderá rejeitar, no todo ou em parte, se em desacordo com o Termo de Referência.
- 12.3.16** Quaisquer exigências da Fiscalização, inerentes ao Objeto da presente contratação, deverão ser prontamente atendidas pela CONTRATADA.

## **12.4** Do Recebimento do Objeto

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

## **12.5** Obrigações da Contratada

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

**12.5.2** Cumprir os prazos e obrigações estabelecidas no Edital.

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

**12.5.4** Observar as normas e procedimentos internos do CONTRATANTE no que se refere à segurança (Política de Segurança da Informação e seus Manuais de Normas e Procedimentos – ADENDO VII) e sigilo dos dados manuseados, bem como no que é pertinente à documentação (Termo de Confidencialidade, Acordo de Confidencialidade da Informação e Responsabilidade – ADENDO VI e Acordo de Proteção de Dados Pessoais – ADENDO X, sobre os quais se obriga a dar ciência a seus funcionários, que tiverem acesso às dependências do CONTRATANTE, e aos que possuem acesso remoto);

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

**12.5.6** 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.

**12.5.7** 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.

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

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

**12.5.10** 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;

- 12.5.11** Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 12.5.12** 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;
- 12.5.13** Manter garantia contra defeitos de hardware e software, inclusive atualização de versões dos programas utilizados para objeto deste Edital;

## **12.6** Obrigações da Contratante

- 12.6.1** 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;
- 12.6.2** Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA sobre os produtos objeto desta licitação;
- 12.6.3** Acompanhar e atestar nas Notas-Fiscais/Faturas a efetiva entrega do produto/serviço do objeto deste Edital;
- 12.6.4** Aplicar à CONTRATADA as penalidades regulamentares e contratuais, previstas em lei e neste Edital;
- 12.6.5** Comunicar à CONTRATADA, quaisquer irregularidades observadas no objeto deste Edital.
- 12.6.6** Verificar a regularidade da situação fiscal da CONTRATADA, antes de efetuar o pagamento devido.
- 12.6.7** Proceder às advertências, descontos e demais cominações legais pelo descumprimento das obrigações assumidas pela CONTRATADA.
- 12.6.8** 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.

## **13** Das Sanções Administrativas

---

- 13.1** 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](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.

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

**13.3** 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.

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

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

**13.6** 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.

**13.7** Da sanção de advertência:

**13.7.1** 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.

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

**13.8** Da sanção de multa:

**13.8.1** A multa poderá ser aplicada nos seguintes casos:

- a) em decorrência da não regularização da documentação de habilitação, nos termos do art. 43, § 1º da Lei Complementar nº 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 11.1.6 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 <i>e-mail</i> , 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/metras 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

<b>NÍVEL</b>	<b>CORRESPONDÊNCIA</b> (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.

**13.8.2 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

**13.9** Da sanção de suspensão:

**13.9.1** 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.

**13.9.2** 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 nº 12.846, de 2013.

**13.9.3** 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.

**13.9.4** 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.

**13.10** Do cometimento de falta grave:

**13.10.1** 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:

**13.10.2** 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;

**14 Do Faturamento**

---

**14.1** O valor será faturado mediante execução da Ordem de Serviço correspondente.

**14.1.1** Após o recebimento do objeto e da Nota Fiscal/Fatura a CONTRATANTE disporá de até 10 (dez) dias úteis para emissão do respectivo Termo de Aceite, aprovando os serviços prestados.

## 15 Do Pagamento

---

- 15.1** 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;
- 15.2** O pagamento do contrato será feito depois das emissões dos Termos de Aceite (ADENDO VIII) dos serviços entregues e aceitos a partir dos relatórios gerados de cada Teste de Intrusão feitos. Quanto ao treinamento o pagamento será feito em parcela única correspondendo ao valor do mesmo em até 30 (trinta) dias corridos após a realização do treinamento e avaliação do mesmo.
- 15.2.1** A Reavaliação, novo teste de intrusão pós remediação e entrega dos relatórios gerados a partir do Teste de Intrusão, faz parte da estrutura do Teste de intrusão como um todo e não acarretará pagamento a mais tanto por essa fase como pela entrega do Relatório final do Teste de Invasão que ocorrerá após a reavaliação.
- 15.3** 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.
- 15.4** Nenhum pagamento será efetivado enquanto estiver pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidades ou inadimplência contratual.
- 15.5** 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.
- 15.6** A devolução da Nota/Fatura não servirá de pretexto ao descumprimento de quaisquer cláusulas contratuais.
- 15.7** 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.
- 15.8** De acordo com a legislação tributária e fiscal em vigor será efetuada a retenção na fonte dos tributos e contribuições incidentes no objeto contratado.
- 15.9** É permitido ao BANPARÁ descontar dos créditos da CONTRATADA qualquer valor relativo à multa, ressarcimentos e indenizações, sempre observado o contraditório e ampla defesa.

- 15.10** 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.
- 15.11** 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.
- 15.12** 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
- 15.13** Nos casos em que for constatada inobservância relativa à quantidade de testes solicitados pelo Banpará e entregues pela Contratada, bem como inobservância da qualidade dos testes entregues via relatórios (desconformidade com as especificações técnicas constantes no Termo de Referência - Item 5.1.4), o prazo só será feito após regularização da situação pela contratada, ou seja, quando da emissão, pelo Contratante, do Termo de Aceite do serviço e após a revalidação da qualidade do serviço entregue.
- 15.14** A nota fiscal deverá ser emitida com uma cópia do(s) Termo(s) de Aceite (ADENDO VIII). Em caso de incompatibilidade entre Serviço solicitado e a informado na nota fiscal, o Banco devolverá a nota para a devida correção.

## **16 Fiscalização do Contrato**

---

**16.1** 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.

**16.2** 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.

**16.3** 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.

### **16.4 Fiscalização Técnica**

**16.4.1** A Fiscalização Técnica do fornecimento do objeto será exercida pelo Gerente ou um funcionário da SUROP - Superintendência de RISCO OPERACIONAL / GESEI - Gerência de Segurança da Informação , a ser nomeado pelo BANPARA;

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

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

### **16.5 Fiscalização Administrativa**

**16.5.1** 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.

**16.5.2** A Fiscalização Administrativa do fornecimento do objeto será exercida Pela Gerência ou por um funcionário da GECAD – Gerência de Contratos Administrativos, a ser nomeado pelo BANPARA;

**16.6** A fiscalização da execução do contrato abrange as seguintes rotinas:

**16.6.1 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 BANPARÁ 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;

**16.6.2 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 convencionalizada 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	QUANTIDADE (A)	UNIDADE	PRODUTOS /SERVIÇOS	
				VALOR UNITÁRIO (B)	SUBTOTAL A x B
1	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 ( <b>Wireless</b> ) e <b>Rede</b> de Área Local ( <b>LAN</b> ) do tipo Externos e/ou Internos.	1000	Horas	R\$	R\$
2	Serviço de Teste de invasão em sistemas no padrão Red Team (in loco), Blackbox, GreyBox e WhiteBox.	1500	Horas	R\$	R\$
3	Curso preparatório para EXIN ETHICAL HACKING e CompTIA PenTest+ - Curso preparatório tanto para certificação EXIN Ethical Hacking Foundation quanto para a certificação CompTIA PenTest+	2	Turmas	R\$	R\$
<b>TOTAL PRODUTOS / SERVIÇOS</b>					<b>R\$</b>

**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	QUANTIDADE (A)	UNIDADE	PRODUTOS /SERVIÇOS
------	-----------	----------------	---------	--------------------

				VALOR UNITÁRIO (B)	SUBTOTAL A x B
1	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 ( <b>Wireless</b> ) e <b>Rede</b> de Área Local ( <b>LAN</b> ) do tipo Externos e/ou Internos.	1000	Horas	R\$	R\$
2	Serviço de Teste de invasão em sistemas no padrão Red Team (in loco), Blackbox, GreyBox e WhiteBox.	1500	Horas	R\$	R\$
3	Curso preparatório para EXIN ETHICAL HACKING e CompTIA PenTest+ - Curso preparatório tanto para certificação EXIN Ethical Hacking Foundation quanto para a certificação CompTIA PenTest+	2	Turmas	R\$	R\$
<b>TOTAL PRODUTOS / SERVIÇOS</b>					R\$

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.

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

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 N°. **[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 N°. **[CNPJ da Empresa Emitente do atestado]**, situada no **[endereço da Empresa Emitente do atestado]**, conforme discriminado 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**  
**DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E A ADMINISTRAÇÃO PÚBLICA**

Declaro que a empresa \_\_\_\_\_, inscrita no CNPJ (MF) nº \_\_\_\_\_, inscrição estadual nº \_\_\_\_\_, estabelecida em \_\_\_\_\_, possui os seguintes contratos firmados com a iniciativa privada e a administração pública:

Nome do Órgão/Empresa	Vigência do Contrato	Valor total do contrato
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
Valor total dos Contratos		R\$ _____

Local e data

\_\_\_\_\_

Assinatura e carimbo do emissor

**Observação:**

Além dos nomes dos órgãos/empresas, o licitante deverá informar também o endereço completo dos órgãos/empresas, com os quais tem contratos vigentes.

**ADENDO V****MODELO DE CARTA DE FIANÇA BANCÁRIA PARA GARANTIA DE EXECUÇÃO CONTRATUAL**

1. Pela presente, o (a) \_\_\_\_\_ (nome da instituição fiadora) com sede em \_\_\_\_\_ (endereço completo), por seus representantes legais infra-assinados, declara que se responsabiliza como FIADOR e principal pagador, com expressa renúncia dos benefícios estatuídos no Artigo 827, do Código Civil Brasileiro, da empresa \_\_\_\_\_ (nome da empresa), com sede em \_\_\_\_\_ (endereço completo), até o limite de R\$ \_\_\_\_\_ (valor da garantia) ( \_\_\_\_\_ ) (valor por escrito) para efeito de garantia à execução do Contrato nº \_\_\_\_\_ (número do contrato, formato xx/ano), decorrente do processo licitatório \_\_\_\_\_ (modalidade e número do instrumento convocatório da licitação – ex.: PE nº xx/ano), firmado entre a AFIANÇADA e o Banco do Estado do Pará - BANPARÁ para \_\_\_\_\_ (objeto da licitação), tendo este FIADOR plena ciência dos termos do referido Edital licitatório e das cláusulas contratuais.
2. A fiança ora concedida visa garantir o cumprimento, por parte de nossa AFIANÇADA, de todas as obrigações estipuladas no contrato retromencionado, abrangendo o pagamento de:
- a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
  - b) prejuízos causados à Administração contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;
  - c) multas moratórias e punitivas aplicadas pela Administração contratante à AFIANÇADA; e
  - d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela AFIANÇADA.
3. Esta fiança é válida por \_\_\_\_\_ (prazo, contado em dias, correspondente à vigência do contrato) ( \_\_\_\_\_ ) (valor por escrito) dias, contados a partir de \_\_\_\_\_ (data de início da vigência do contrato), vencendo-se, portanto em \_\_\_\_\_ (data).
4. Na hipótese de inadimplemento de qualquer das obrigações assumidas pela AFIANÇADA, o (a) \_\_\_\_\_ (nome da instituição fiadora) efetuará o pagamento das importâncias que forem devidas, no âmbito e por efeito da presente fiança, até o limite acima estipulado, no prazo de 48 (quarenta e oito) horas, contado do recebimento de comunicação escrita do Banco do Estado do Pará - BANPARÁ.
5. A comunicação de inadimplemento deverá ocorrer até o prazo máximo de 90 (dias) após o vencimento desta fiança.
6. Nenhuma objeção ou oposição da nossa AFIANÇADA será admitida ou invocada por este FIADOR com o fim de escusar-se do cumprimento da obrigação assumida neste ato e por este instrumento perante o Banco do Estado do Pará - BANPARÁ.
7. Obriga-se este FIADOR, outrossim, pelo pagamento de quaisquer despesas judiciais e/ou extrajudiciais, bem assim por honorários advocatícios, na hipótese do Banco do Estado do Pará - BANPARÁ se ver

compelido a ingressar em juízo para demandar o cumprimento da obrigação a que se refere a presente fiança.

8. Se, no prazo máximo de 90 (noventa) dias após a data de vencimento desta fiança, o (a) \_\_\_\_\_ (nome da instituição fiadora) não tiver recebido do Banco do Estado do Pará - BANPARÁ qualquer comunicação relativa a inadimplemento da AFIANÇADA, ou termo circunstanciado de que a AFIANÇADA cumpriu todas as cláusulas do contrato, acompanhado do original desta Carta de Fiança, esta fiança será automaticamente extinta, independentemente de qualquer formalidade, aviso, notificação judicial ou extrajudicial, deixando, em consequência, de produzir qualquer efeito e ficando o FIADOR exonerado da obrigação assumida por força deste documento.

9. Declara, ainda, este FIADOR, que a presente fiança está devidamente contabilizada e que satisfaz às determinações do Banco Central do Brasil e aos preceitos da legislação bancária aplicáveis e, que, os signatários deste Instrumento estão autorizados a prestar a presente fiança.

10. Declara, finalmente, que está autorizado pelo Banco Central do Brasil a expedir Carta de Fiança e que o valor da presente se contém dentro dos limites que lhe são autorizados pela referida entidade federal.

(Local e data)

(Instituição garantidora)

(Assinaturas autorizadas)

## **ADENDO VI**

### **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 Guttmann 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\_\_\_\_\_

XXXXXXXXXXXXXXXXXXXX

Diretor Presidente

**Banco do Estado do Pará SA**  
**CONTRATANTE**

XXXXXXXXXXXXXXXXXXXX

Representante  
**CONTRATADA**

**ADENDO VII**

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**  
**Versão 6.0**

**DICRI/SUROP**

**ÍNDICE**

1.	INTRODUÇÃO	98
2.	OBJETIVO	98
3.	TERMOS E DEFINIÇÕES	98
4.	DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO	98
4.2.	Comportamento Seguro	98
4.3.	Controle de Acesso Físico aos Ambientes de TI	99
4.4.	Ativos: Hardware e Software	99
4.5.	E-mail e Internet	99
4.8.	Registro e Monitoramento	100
5.	PAPÉIS E RESPONSABILIDADES	101
6.	AValiação CONTÍNUA DOS RISCOS	102
7.	GESTÃO DA SEGURANÇA DA INFORMAÇÃO	102
7.1.	Estrutura Normativa	103
8.	SEGURANÇA CIBERNÉTICA	103
9.	VIOLAÇÕES E SANÇÕES	104

<b>Título: Política de Segurança da Informação</b>
--

<b>Classificação: Nível II - (Interna)</b>
--

<b>Data:</b>
--------------

<b>02/06/2016</b>
-------------------

<b>Versão:</b>
----------------

<b>5.0</b>
------------

<b>Proprietário:</b>
----------------------

<b>SUSEM</b>
--------------

<b>Destinatário: Todas as unidades do Banco e colaboradores</b>
---

## 1. INTRODUÇÃO

1.1. A Política de Segurança da Informação do **Banpará** é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores.

## 2. OBJETIVO

2.1. Estabelecer as diretrizes a serem seguidas pelo Banco no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

## 3. TERMOS E DEFINIÇÕES

- **Informação:** Conjunto de dados relacionados entre si que contenham algum significado, podendo estar na forma escrita, verbal ou imagística, e em meio digital ou físico.
- **Segurança da Informação:** Conjunto de controles, incluindo política, processos, estruturas organizacionais, normas e procedimentos de segurança, que objetiva a proteção das informações dos clientes e da empresa, nos seus aspectos de confidencialidade, integridade e disponibilidade.
- **Classificação da Informação:** Ação de definir o nível de sensibilidade da informação, a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a Organização.
- **Integridade:** Somente alterações, supressões e adições autorizadas pela instituição devem ser realizadas nas informações.
- **Confidencialidade:** Somente pessoas devidamente autorizadas pela instituição devem ter acesso à informação.
- **Disponibilidade:** A informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.
- **Controle:** Forma de gerenciar o risco, incluindo políticas, normas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controle de segurança da informação].
- **Perímetro de Segurança:** Barreiras de segurança múltiplas e controles de acesso físico e implantados para proteger áreas sensíveis contra acesso não autorizado, danos, interferências, incluindo (mas não se limitando) a paredes, portas externas, fechaduras, controles de entrada por cartão, biometria, alarmes e firewalls.
- **Colaboradores:** Diretores, Superintendentes, Chefes de Núcleo, Gerentes, Funcionários, Estagiários, Terceirizados e Prestadores de Serviços.
- **Terceiros:** Funcionários de empresa prestadora de serviços.

## 4. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

4.1. As diretrizes abaixo elencadas constituem os pilares da Gestão de Segurança da Informação do Banco, norteando a elaboração de Normas e Procedimentos de Segurança, que devem contemplar, no mínimo, o descrito neste documento.

### 4.2. COMPORTAMENTO SEGURO

4.2.1. Independentemente do meio ou da forma em que se apresente, a informação faz parte do trabalho de todos os colaboradores. Portanto, são fundamentais para a proteção e salvaguarda das informações, que sejam adotados comportamentos seguros e consistentes.

4.2.2. Todos os colaboradores devem assumir atitude proativa e de engajamento no que diz respeito à proteção das informações do Banco, procurando compreender ameaças externas que possam afetar a segurança da informação. Todo tipo de acesso à informação do Banco que não for explicitamente autorizado é proibido.

Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a Superintendência de Gestão de Risco Operacional – SUROP.

#### 4.3. CONTROLE DE ACESSO FÍSICO AOS AMBIENTES DE TI

4.3.1. O acesso aos locais de processamento de informações críticas ou dados sensíveis será controlado, com perímetro de segurança, ficando protegidos fisicamente contra acessos não autorizados, danos e interferências, de forma a garantir que os acessos a essas áreas ocorram somente mediante autorização expressa.

#### 4.4. ATIVOS: HARDWARE E SOFTWARE

4.4.1. O Banpará disponibiliza para seus colaboradores equipamentos (computadores, impressoras, dentre outros, também conhecidos como “hardwares”) exclusivamente para o desempenho de suas atividades profissionais.

4.4.2. O Banco deve manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade, etc).

4.4.3. Cada colaborador é responsável pelos arquivos que recebe e envia através da infraestrutura tecnológica do Banpará.

#### 4.5. E-MAIL E INTERNET

4.5.1. O e-mail é uma ferramenta institucional que deve ser utilizada apenas para comunicações eletrônicas relacionadas às atividades laborais, não sendo permitido seu uso para fins pessoais ou que não sejam de interesse do Banpará, visando com isso, assegurar o bom uso dos recursos do Banpará e evitando desperdício causado pelo fluxo de informações não relacionadas às tarefas laborais.

4.5.2. O acesso à Internet deve ser restrito, cabendo à quem tenha permissões de acesso, usá-la de forma consciente e ética, com fins exclusivamente voltados para as atividades laborais.

#### 4.6. Certificação Digital

4.6.1. O Banpará poderá fornecer, a seu exclusivo critério, certificado digital para um funcionário (pessoal e intransferível); para autenticar determinado endereço eletrônico; ou sistema, de acordo com a atividade bancária desenvolvida.

#### 4.7. Classificação da Informação

4.7.1. As informações de propriedade do Banpará ou de terceiros, utilizadas durante as atividades do Banco, devem ser classificadas de acordo com o nível de sensibilidade que representam para o negócio a fim de indicar a necessidade, prioridade e o nível esperado de proteção quando de seu tratamento pelos colaboradores.

4.7.2. O Gerente/Superintendente da unidade deverá ser o “proprietário da informação” e será responsável pela sua classificação e definição do grupo de acesso.

#### **4.7.3. Níveis de Classificação**

4.7.3.1. É a Categoria a ser definida para cada informação ou classe de informação, que estabelece a sensibilidade da informação em termos de preservação de sua confidencialidade.

4.7.3.2. De acordo com a ABNT NBR ISO IEC 27002:2005, item 7.2.1, deve-se evitar a criação de esquemas de classificação muito complexos utilizando diversos níveis, visto que poderá inviabilizar o processo de classificação e, conseqüentemente, o fluxo de informação. Sendo assim, o Banco optou por estabelecer 4 níveis de classificação, conforme abaixo:

**Nível I - (Pública);**  
**Nível II - (Interna);**  
**Nível III - (Restrita);**  
**Nível IV - (Confidencial).**

#### **4.7.4. Rotulação da Informação**

4.7.4.1. É a forma pela qual determinada informação será apresentada, de acordo com sua classificação. O processo de rotulação da informação deve estabelecer claramente o nível de classificação que foi atribuído para a informação bem como o grupo de acesso.

#### **4.7.5. Tratamento da Informação**

4.7.5.1. É o Conjunto de ações referentes ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo todas as etapas do seu ciclo de vida.

### **4.8. REGISTRO E MONITORAMENTO**

4.8.1. Todos os sistemas, as informações, os serviços e equipamentos disponibilizados pelo Banpará para os usuários desenvolverem suas atividades profissionais são de propriedade da Instituição e possuem caráter de ferramenta de trabalho, sendo expressamente proibida a utilização para fins particulares.

4.8.2. Assim, toda a infraestrutura tecnológica do Banco, bem como todos os dados trafegados e armazenados nesta infraestrutura, incluindo conta de e-mail corporativa e navegação em sites da Internet, está sujeita ao monitoramento, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança das informações a atender a requisitos legais e normativos do Banpará.

4.8.3. Todos os colaboradores do Banpará devem ter conhecimento de que o uso das informações e dos sistemas de informação do Banco pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação.

4.8.4. O usuário fica ciente da inexistência de expectativa da privacidade na utilização da infraestrutura tecnológica do Banpará.

4.8.5. O Banpará fará uso de câmeras de segurança instaladas em suas dependências com objetivo de garantir a segurança física do usuário e a segurança patrimonial do Banpará, ficando resguardada a dignidade humana do usuário, sendo vedada a instalação de câmeras de segurança nos banheiros e lavabos.

4.8.6. Todas as atividades desenvolvidas com a utilização da infraestrutura do Banpará serão registradas, para os devidos fins, por um período de 03 (três) anos ou conforme requerido pela legislação vigente e aplicável. Essas atividades incluem, mas não se limitam a, acesso à rede, armazenamento de arquivos, informações, registros de envio e de recebimento de mensagens eletrônicas, acesso e navegação à Internet e impressão.

## 5. PAPÉIS E RESPONSABILIDADES

### 5.1. Todos os Colaboradores do Banpará:

5.1.1 Cumprir fielmente a Política de Segurança da Informação do Banpará;

5.1.2. Assinar o Termo de Confidencialidade, Zelo e Responsabilidade sobre os bens de informação do Banco do Estado do Pará AS, formalizando a ciência e o aceite da Política de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento.

5.1.3. Tratar as informações de acordo com sua classificação e com as diretrizes de tratamento estabelecidas pela organização;

5.1.4. Proteger as informações contra acessos indevidos; destruições acidentais ou propositais; e modificações ou divulgações não autorizadas pelo Banpará.

5.1.5. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Banpará;

5.1.6. Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual e do sigilo bancário;

5.1.7. Buscar orientação e esclarecimento da Superintendência de Gestão de Risco Operacional em caso de dúvidas relacionadas à segurança da informação;

5.1.8. Comunicar imediatamente à Superintendência de Gestão de Risco Operacional qualquer descumprimento ou violação desta Política.

### 5.2. Conselho de Administração

5.2.1 Aprovar a Política de Segurança da Informação e suas revisões anuais;

### 5.3. Diretoria Colegiada

5.3.1. Aprovar a Política de Segurança da Informação e suas revisões anuais;

5.3.2. Aprovar a nomeação dos proprietários da informação;

5.3.3. Tomar as decisões administrativas referentes aos casos de descumprimento da Política, encaminhados pelo Comitê de Segurança Física e Lógica.

### 5.4. Comitê de Segurança Física e Lógica

5.4.1. Apreciar as revisões e/ou propostas de alteração da Política de Segurança e Política de Continuidade de Negócios do Banpará.

5.4.2. Manter atualizada a Política de Segurança da informação.

### 5.5. Superintendência de Gestão de Risco Operacional

5.5.1. Prover ampla divulgação da Política de Segurança da Informação para todos os colaboradores do BANPARÁ;

5.5.2. Oferecer orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores do BANPARÁ;

5.5.3. Acompanhar a aplicação da política, estabelecer mecanismo de registro e controle de não conformidade a esta Política, comunicando ao Comitê de Segurança Física e Lógica.

5.5.4. Propor projetos e iniciativas relacionados ao aperfeiçoamento da política de segurança da informação do BANPARÁ, mantendo-a atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

## **5.6. Proprietário da Informação**

5.6.1. O proprietário da informação é o responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinada informação ou conjunto de informações pertencentes ao Banco ou sob a sua guarda.

## **5.7. Núcleo Jurídico**

5.7.1. Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas do Banco.

## **5.8. Diretorias, Núcleos, Superintendências e Gerências**

5.8.1. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

5.8.2. Assegurar que suas unidades possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

5.8.3. Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados;

5.8.4. Comunicar imediatamente eventuais casos de violação de segurança da informação à Superintendência de Gestão de Risco Operacional.

## **5.9. Superintendência de Desenvolvimento de Pessoas e Processos (Sudep)**

5.9.1. Colher a assinatura referente ao Termo de Confidencialidade, Zelo e Responsabilidade sobre os bens de informação do Banco do Estado do Pará SA dos diretores, funcionários, estagiários, terceirizados e prestadores de serviços, formalizando a ciência e o aceite da Política de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento e arquivando-o nos respectivos dossiês funcionais.

## **6. AVALIAÇÃO CONTÍNUA DOS RISCOS**

6.1. A Superintendência de Gestão de Risco Operacional deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação do Banco. A análise dos riscos deve atuar como ferramenta de orientação ao Comitê de Segurança Física e Lógica, principalmente, no que diz respeito à:

- a) Identificação dos principais riscos aos quais as informações do Banco estão expostas;
- b) Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas, etc.
- c) O escopo da análise/avaliação de riscos de segurança da informação pode ser de toda a organização, de partes da organização, de um sistema de informação específico, de componentes de um sistema específico, etc.

## **7. GESTÃO DA SEGURANÇA DA INFORMAÇÃO**

## 7.1. ESTRUTURA NORMATIVA

7.1.1. A estrutura normativa da Segurança da Informação do Banpará é composta por um conjunto de documentos classificados em 03 (três) níveis hierárquicos distintos:

- a) **Política de Segurança da Informação:** Constituída neste documento, está relacionada ao nível estratégico, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação, descreve o que deve ser feito.
- b) **Normas de Segurança da Informação:** Estão relacionadas ao nível tático, estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada, são as regras a serem adotadas.
- c) **Procedimentos de Segurança da Informação:** estão relacionados ao nível operacional, instrumentalizam o disposto nas Normas e na Política, descrevendo os procedimentos a realizar, permitindo a aplicação direta nas atividades do Banpará, definindo como serão implementadas as regras.



Figura 1 - **ESTRUTURA NORMATIVA DE SEGURANÇA DA INFORMAÇÃO.**

## 8. SEGURANÇA CIBERNÉTICA

**8.1.** O objetivo da segurança cibernética é manter as propriedades de segurança dos ativos da Organização contra riscos relevantes no ambiente cibernético através de controles que visem à prevenção e detecção de incidentes relacionados com o este ambiente.

**8.2.** O Banpará deverá adotar diversos procedimentos e controles para reduzir a vulnerabilidade a incidentes cibernéticos, abrangendo a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

8.2.1 Os procedimentos e os controles citados no item 8.2 devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.

**8.3.** O Banpará deverá implementar controles específicos para garantir a segurança das informações sensíveis.

**8.4.** O Banpará deverá manter o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição. Estes registros deverão abranger, inclusive, informações recebidas de prestadores de serviço;

<< DIRETRIZES PARA: >>

**8.5.** a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

**8.6.** a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;

**8.7.** a classificação dos dados e das informações quanto à relevância;

**8.8.** a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

<< FIM DAS DIRETRIZES >>

**8.9.** Deve ser disseminada na instituição uma cultura de segurança cibernética através de:

8.9.1 Implementação de programas de capacitação e de avaliação periódica de pessoal;

8.9.2 Prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros;

8.9.3 Comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

**8.10.** O Banco deverá manter um canal de comunicação com as demais instituições financeiras para compartilhamento de informações sobre os incidentes cibernéticos relevantes.

## **9. VIOLAÇÕES E SANÇÕES**

**9.1.** Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas poderão ser adotadas, sem prejuízo de ação civil e penal, se aplicáveis.

**ADENDO VIII**  
**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 IX  
MODELO DE ORDEM DE SERVIÇO**

ORDEM DE SERVIÇO – Nº

PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE  
DE VULNERABILIDADES DE SEGURANÇA

CONTRATO Nº

A presente ordem de serviço é celebrada em conformidade com o procedimento para PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE SEGURANÇA, 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:

<b>CONTATOS DA CONTRATANTE</b>		
Nome:		
Gerencia:	Unidade:	Matrícula:
Telefones de Contato:		

<b>CONTATOS DA CONTRATADA</b>
-------------------------------

Nome:		
Gerencia:	Unidade:	Matrícula:
Telefones de Contato:		

Belém, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_

CONTRATANTE

CONTRATADA

## **ADENDO X ACORDO DE PROTEÇÃO DE DADOS PESSOAIS**

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 PROTEÇÃO DE DADOS PESSOAIS, 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 SEGUINTE:

No desenvolvimento de quaisquer atividades relacionadas com a execução do presente Contrato, as Partes deverão observar o regime legal da proteção de dados pessoais, empenhando-se em proceder a todo o tratamento de dados pessoais que venha a mostrar-se necessário ao desenvolvimento do Acordo no estrito e rigoroso cumprimento da Lei, em especial à Lei Federal nº 13.709/18. Para tanto, as Partes obrigam-se a:

1. LICITUDE DO TRATAMENTO DE DADOS: A PRIMEIRA OUTORGANTE fará a coleta, conservação e tratamento de dados do SEGUNDO OUTORGANTE por imposição do cumprimento de obrigações legais, para cumprimento do presente contrato e ainda porque o SEGUNDO OUTORGANTE dá o seu consentimento.
2. RESPONSÁVEL PELO TRATAMENTO: A PRIMEIRA OUTORGANTE melhor identificada neste contrato será a Responsável pelo tratamento dos dados do SEGUNDO OUTORGANTE cujo processamento de dados será interno ficando a PRIMEIRA OUTORGANTE expressamente autorizada a caso assim o entenda efetuar esse processamento externamente.
3. COLETA DOS DADOS: Será efetuada pela SEGUNDA OUTORGANTE diretamente e presencialmente incluindo preenchimento de impressos pela PRIMEIRA OUTORGANTE.
4. FINALIDADES DO TRATAMENTO DOS DADOS: A PRIMEIRA OUTORGANTE fará o tratamento de dados de modo compatível com as finalidades para os quais tenham sido recolhidos.
5. DADOS PESSOAIS CONTIDOS NO REGISTRO: incluem nome, morada, contatos telefônicos e endereços eletrônicos, data de nascimento, gênero, filiação, estado civil, naturalidade, nacionalidade, composição do agregado familiar, identificação civil, identificação e enquadramento fiscal, autorização de residência, passaporte, currículo profissional, profissão, habilitações acadêmicas, formação profissional, agência, conta corrente, senhas e ainda dados biométricos.
6. COMUNICAÇÃO DOS DADOS A TERCEIROS: A PRIMEIRA OUTORGANTE vai comunicar ou transferir em parte ou na sua totalidade os dados pessoais do SEGUNDO OUTORGANTE a entidades públicas e ou privadas sempre que tal decorra de obrigação legal e ou seja necessário para cumprimento deste ou outros contratos ficando para tal expressamente autorizada pelo SEGUNDO OUTORGANTE.
7. PRAZO DE CONSERVAÇÃO DOS DADOS: A PRIMEIRA OUTORGANTE vai conservar os dados do SEGUNDO OUTORGANTE pelos prazos necessários a dar cumprimento à obrigações legais designadamente de 10 (dez) anos para cumprimento à obrigação legal de arquivo de toda a documentação de escrita comercial.
8. DIREITOS DO TITULAR DOS DADOS: O SEGUNDO OUTORGANTE poderá solicitar à PRIMEIRA OUTORGANTE e esta, salvo impedimento legal, vai salvaguardar os direitos do SEGUNDO OUTORGANTE de acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento, e o direito de se opor ao tratamento, bem como do direito à portabilidade dos dados. E ainda, o direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no cumprimento de obrigações legais ou com base no consentimento previamente dado. E também o direito de reclamação sobre o tratamento de dados junto da Comissão Nacional de Proteção de Dados.

9. **SEGURANÇA NO TRATAMENTO DOS DADOS:** Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, a PRIMEIRA OUTORGANTE aplica as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado.

10. **VIOLAÇÃO DE DADOS PESSOAIS:** Em caso de violação de dados pessoais a PRIMEIRA OUTORGANTE notifica esse fato à Autoridade Nacional de Proteção de Dados nos termos e condições previstos na lei. Se essa violação for suscetível de implicar um elevado risco para os direitos e liberdades do titular, comunica-lhe esse fato, nos termos e condições previstos na lei.

## ADENDO XI

### 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 *firewall* 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 infraestrutura 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 infraestrutura 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 Poisoning*.

## 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 XII

### 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

- a) 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.
- b) Autenticar somente as pessoas que podem utilizar os sistemas corporativos da instituição;
- c) Garantir a utilização de informações sensíveis e confidenciais, somente por pessoas autorizadas, de acordo com o seu perfil funcional;
- d) 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 multissessão.

**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 autenticuem-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:

- Usuário de rede;
- Login do Usuário;
- Grupo (perfil) do usuário;
- Operação;
- Contexto ();
- Endereço IP e porta lógica que realizou as transações;
- Nome de máquina (Hostname);
- A data e hora de evento do usuário, sendo (recomendável o uso do relógio do sistema e

não o do host);

- MAC Address;
- Geolocalização;
- 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:

- 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;
- Perfil do usuário;
- 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 à 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.

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 à 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 segunda 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 Cryptographic Architecture) para garantia de sigilo de comunicação.
- iii. Deverá suportar, no mínimo, os algoritmos de criptografia definidos no padrão JCA (Java Cryptographic Architecture) 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 modificá-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 XIII****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://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

## ANEXO II

**MODELO DE DECLARAÇÃO – CONFORMIDADE AO ART.38 DA LEI Nº 13.303/2016****DECLARAÇÃO DE 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) suspensão 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 III – 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, nº 251, Bairro Comércio, CEP. 66.010-000, Belém-PA, inscrito no Ministério da Fazenda sob o CNPJ nº 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**

1.1. O presente contrato tem como objeto contratação de ....., conforme especificações, exigências e condições estabelecidas **no termo de referência e demais anexos deste edital**.

**1.2. A CONTRATAÇÃO DEVERÁ CONSIDERAR QUE O OBJETO A SER ADQUIRIDO E DEVE CONTER TODAS AS ESPECIFICAÇÕES DEFINIDAS NO TERMO DE REFERÊNCIA (Anexo I do Edital e Adendo 1 deste contrato).**

1.3. O presente contrato decorre do processo nº 1677/2019, realizado pelo edital da licitação nº ...../.....

**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/ Especificações Técnicas e Detalhamentos

Adendo 2 –Proposta/Detalhamentos dos Preços

Adendo 3 – 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, contado** da assinatura do Contrato, prorrogável na forma da Lei. O prazo da garantia independe do prazo da vigência contratual.

**4. CLÁUSULA QUARTA – VALOR DO CONTRATO**

4.1. Como contrapartida à execução do objeto do presente contrato, o BANPARÁ deve pagar à CONTRATADA o valor total de ....., conforme os valores da tabela abaixo e nas condições estabelecidas no Termo de Referência:

ITEM	DESCRIÇÃO	QUANTIDADE (A)	UNIDADE	PRODUTOS /SERVIÇOS	
				VALOR UNITÁRIO (B)	SUBTOTAL A x B
1	Testes de Invasão em redes no padrão de redes sem fio IEEE 802.11 ( <b>Wireless</b> ) e Rede de Área Local ( <b>LAN</b> ) do tipo Externos e/ou Internos.	1000	Horas	R\$	R\$
2	Serviço de Teste de invasão em sistemas no padrão Red Team (in loco), Blackbox, GreyBox e WhiteBox.	1500	Horas	R\$	R\$
3	Curso preparatório para EXIN ETHICAL HACKING e CompTIA PenTest+ - Curso preparatório tanto para certificação EXIN Ethical Hacking Foundation quanto para a certificação CompTIA PenTest+	2	Turmas	R\$	R\$
<b>TOTAL PRODUTOS / SERVIÇOS</b>					<b>R\$</b>

4.2. O valor contratado inclui todos os impostos e taxas vigentes na Legislação Brasileira para a execução do objeto desta contratação, e, também, todos os custos diretos e indiretos inerentes, tais como os a seguir indicados, porém sem se limitar aos mesmos: despesas com pessoal (inclusive obrigações sociais, viagens e diárias), despesas administrativas, administração, lucro e outras despesas necessárias a boa realização do objeto desta contratação, isentando o BANPARÁ de quaisquer ônus adicionais.

## 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 03 (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.

5.2. 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:

- a.1. Estatuto Social e ata de posse da diretoria da Instituição Financeira;
- a.2. Quando Procuradores, encaminhar as procurações devidamente autenticadas, com poderes específicos para representar a Instituição Financeira;
- a.3. Balanços Patrimoniais e Demonstração de Resultado dos últimos dois anos, acompanhado das notas explicativas e respectivos pareceres do Conselho de Administração e Auditores Independentes;
- a.4. 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 *síte* do Banco Central do Brasil ([www.bcb.gov.br](http://www.bcb.gov.br)).

**b) Caução em dinheiro**, valor **depositado** pela CONTRATADA, no Banco ....., Agência ....., Conta-Corrente nº ....., 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.

- 5.3. 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.

5.4. A inobservância do prazo fixado nesta Cláusula para apresentação da garantia acarreta a aplicação de multa de 0,2% (dois décimos por cento) sobre o valor total do contrato, por dia de atraso, limitada a 5% (cinco por cento) sobre o valor total do contrato.

- 5.5. 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.

- 5.6. 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 03 (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 nº 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).

6.3. 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.

6.4. 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.

6.5. 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.

6.6. 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.

6.7. 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.

6.8. 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.

6.8.1. 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.

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

6.9. 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.

6.9.1. 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.

6.10. 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.

6.11. 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.

6.11.1. 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.

6.12. 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.

6.13. 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.

6.14. 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 - .....

6.15. 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.

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

6.17. As partes estão obrigadas a comunicarem uma a outra, com 05 (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 05 (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, anexo I deste edital.

## **8. CLÁUSULA OITAVA – CONDIÇÕES DE FATURAMENTO E PAGAMENTO**

8.1. O pagamento é condicionado ao recebimento parcial ou definitivo e deve ser efetuado mediante a apresentação de Nota Fiscal/Fatura pela CONTRATADA à unidade de gestão de contrato do BANPARÁ, que deve conter o detalhamento do objeto executado, o número deste contrato, a agência bancária e contracorrente, aberta ou mantida no Banpará S/A, conforme dispõe o Decreto do Estado do Pará nº 877/2008, na qual deve ser depositado o respectivo pagamento.

8.1.2. O pagamento será realizado nas condições estabelecidas no Termo de Referência (Anexo I do edital), a contar do recebimento, condicionado à apresentação à unidade de gestão de contrato do BANPARÁ da Nota Fiscal/Fatura.

8.1.3. 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.

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

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

8.4. É vedado o pagamento antecipado.

8.5. É permitido ao 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 – SUBCONTRATAÇÃO**

9.1. A CONTRATADA, desde que com a prévia e expressa autorização do gestor do contrato do BANPARÁ, pode subcontratar parcela do objeto deste contrato, desde que não se refira a parcela sobre a qual o BANPARÁ exigiu atestado de capacidade técnica durante o processo licitatório. A subcontratação pode abranger aspectos acessórios e instrumentais de tais parcelas.

9.1.1. A subcontratação não exonera a CONTRATADA de todas as suas obrigações, atinentes à integralidade do contrato.

9.1.2. O pagamento, se assim requerido formal e expressamente pela CONTRATADA, pode ser realizado diretamente pelo BANPARÁ à subcontratada.

## **10. CLÁUSULA DEZ – DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO**

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

10.1.1. 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.

10.1.2. 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**.

10.2. 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 estejam, porventura, depender com pagamentos desta natureza.

## **11. CLÁUSULA ONZE – ALTERAÇÕES INCIDENTES SOBRE O OBJETO DO CONTRATO**

11.1. 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.

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

- a) a aplicação dos limites deve ser realizada separadamente para os acréscimos e para as supressões, sem que haja compensação entre os mesmos;
- b) deve ser mantida a diferença, em percentual, entre o valor global do contrato e o valor orçado pelo **BANPARÁ**, salvo se o fiscal técnico do contrato apontar justificativa técnica ou econômica, que deve ser ratificada pelo gestor do contrato;

11.3. A alteração qualitativa não se sujeita aos limites previstos nos § 1º e 2º do artigo 81 da Lei nº 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.

11.4. As alterações incidentes sobre o objeto devem ser:

1. 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;
2. as justificativas devem ser ratificadas pelo gestor do contrato do **BANPARÁ**; e
3. submetidas à área jurídica e, quando for o caso, à área financeira do **BANPARÁ**;

11.5. 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**.

11.6. 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.

## **12. CLÁUSULA DOZE – EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO**

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

1. Reajuste: instrumento para manter o equilíbrio econômico-financeiro do contrato diante de variação de preços e custos que sejam normais e previsíveis, relacionadas com o fluxo normal da economia e com o processo inflacionário, devido ao completar 01 (um) ano a contar da data da proposta;
2. 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.

12.2. 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.

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

1. dos fatos imprevisíveis ou previsíveis, porém com consequências incalculáveis;
2. 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
3. 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.

12.4. 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.

12.5. 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.

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

12.7. 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.

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

## **13. CLÁUSULA TREZE – RESCISÃO**

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

13.2. A parte que pretende a rescisão deve avaliar e responder motivadamente a manifestação referida no subitem precedente no prazo de 05 (cinco) dias úteis, comunicando a outra parte, na forma prevista neste contrato, considerando-se o contrato rescindido com a referida comunicação.

13.3. 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.

13.4. 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.

13.5. 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.

#### **14. CLÁUSULA CATORZE – SANÇÕES ADMINISTRATIVAS**

14.1. 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 02 (dois) anos, que podem ser cumuladas com multa.

14.2. 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.

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

- a) se não se caracterizar má-fé, a pena base deve ser de 06 (seis) meses;
- b) caracterizada a má-fé ou intenção desonesta, a pena base deve ser de 01 (um) ano e a pena mínima deve ser de 06 (seis) meses, mesmo aplicando as atenuantes previstas.

14.4. 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.

14.5. 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 nº 8.420/2015.

14.5.1. 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 nº 13.303/2016.

14.6. 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.

14.7. 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.

14.8. 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.

14.9. 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.

## **15. CLÁUSULA QUINZE – 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) 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 nº 12.846/2013, Decreto nº 8.420/2015, Lei nº 8.666/1993, ou de quaisquer outras leis ou regulamentos aplicáveis, ainda que não relacionadas no presente contrato.

15.2. 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 estimativa;
- 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).

15.3.1. 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.

15.4. 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.

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

15.6. 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 02 (dois) servidores designados.

15.7. 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 nº 12.846/2013.

15.7.1. Caso os atos lesivos apurados envolvam infrações administrativas à Lei nº 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.

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

15.9. 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.

15.10. O PAR e o sancionamento administrativo obedecerão às regras e parâmetros dispostos em legislação específica, notadamente, na Lei nº 12.846/2013 e no Decreto nº 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.

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

15.12. As disposições deste subitem se aplicam quando o licitante se enquadrar na definição legal do parágrafo único do artigo 1º da Lei nº 12.846/2013.

15.13. 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.

## 16. CLÁUSULA DEZESSEIS – PUBLICIDADE E CONFIDENCIALIDADE

16.1. 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.

## 17. CLÁUSULA DEZESSETE – POLÍTICA DE RELACIONAMENTO E ANTICORRUPÇÃO

17.1. A CONTRATADA assumem 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](http://www.banpara.b.br)), bem como no termo de compromisso que integra o presente contrato.

17.2. 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 05 (cinco) dias a contar de sua solicitação.

## 18. CLÁUSULA DEZOITO – 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.....

Nome:

CPF:

2ª.....

Nome:

CPF:

**ADENDO 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 nº 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 anti-suborno, 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 nº 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)