AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 025/2022

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[1], licitação na modalidade Pregão Eletrônico para **Contratação de soluções tecnológicas especializadas de serviços em telecomunicações, contemplando fornecimento de Redes MPLS concomitante ao uso de tecnologia SD-WAN com implantação, configuração, gerenciamento e manutenção da rede de enlaces dedicados para transmissão de dados nos sites remotos, possibilitando conexão de dados através de diferentes tecnologias, incluindo 3G ou superior, visando fornecer conectividade e disponibilidade para as unidades do Banpará espalhadas pelo Estado do Pará e os datacenters localizados em Belém, assim como enlaces de conectividade à rede Internet com solução anti-DDoS nos sites centrais,** conforme especificações e condições exigidas no edital e demais anexos.

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

DATA: 30/11/2022

HORÁRIO: 10h (Horário de Brasília)

SISTEMA DE LICITAÇÕES: www.gov.br/compras

UASG: 925803

O edital da licitação estará disponível a partir de **08/11/2022**, podendo ser obtido: (i) Gratuitamente no site do BANPARÁ (www.banpara.b.br) e sites www.gov.br/compras e www.compraspara.pa.gov.br; ou, (ii) Na sede do BANPARÁ (Av. Presidente Vargas, n. 251, Ed. BANPARÁ – 1º andar, Comércio, Belém/PA) mediante depósito identificado do valor de R$ 0,25 (vinte centavos) por folha (Conta Corrente nº 800.002-6, Agência nº 0011 do BANPARÁ), não reembolsável, relativos aos custos de reprodução.

Belém - Pará, 08 de Novembro de 2022.

Soraya Rodrigues

Pregoeira

1 https://www.banpara.b.br/PortalImagens/3kpl3ekj/regulamento-de-licita%C3%A7%C3%B5es-e-contratos-do-banpar%C3%A1_v6.pdf?mode=pad&rnd=132851667259500000

PREGÃO ELETRÔNICO Nº 025/2022
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 n. 13.303/2016, do Regulamento de Licitações e Contratos do BANPARÁ (adiante denominado "Regulamento"), da Lei n. 10.520/2002 alterada pelas disposições do Decreto n. 10.024/2019, da Lei Complementar n. 123/2006 e da Lei Estadual n. 8.417/2016, do Decreto Estadual n. 2.121/2018, Lei n. 12.846/2013, e Código Civil Brasileiro, fará realizar licitação na modalidade Pregão Eletrônico, pelo critério de menor preço, conforme condições estabelecidas neste edital e seus anexos.

1. SUMÁRIO DA LICITAÇÃO

1.1. OBJETO: Constitui objeto da presente licitação a **Contratação de soluções tecnológicas especializadas de serviços em telecomunicações, contemplando fornecimento de Redes MPLS concomitante ao uso de tecnologia SD-WAN com implantação, configuração, gerenciamento e manutenção da rede de enlaces dedicados para transmissão de dados nos sites remotos, possibilitando conexão de dados através de diferentes tecnologias, incluindo 3G ou superior, visando fornecer conectividade e disponibilidade para as unidades do Banpará espalhadas pelo Estado do Pará e os datacenters localizados em Belém, assim como enlaces de conectividade à rede Internet com solução anti-DDoS nos sites centrais,** conforme especificações, exigências e condições estabelecidas no Edital e seus Anexos.

1.1.1. MODALIDADE: Pregão Eletrônico.

1.1.2. MODO DE DISPUTA: Aberto/Fechado.

1.1.3. CRITÉRIO DE JULGAMENTO: Menor preço, na forma estabelecida pelo artigo 51 do Regulamento.

1.1.4. CRITÉRIO DE VALORES: Valor máximo aceitável, observados os valores máximos por item.

1.1.5. SESSÃO PÚBLICA: Designada para o dia **30/11/2022**, às **10h** (horário de Brasília) no sistema de licitações www.gov.br/compras.

1.2. A adjudicação será **POR LOTE.**

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

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

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

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

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

2. CONDIÇÕES DE PARTICIPAÇÃO E CONTRATAÇÃO

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

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

a) Suspensão temporária de participação em licitação e impedimento de contratar, prevista no inciso III do artigo 87 da Lei nº 8.666/1993, aplicada pelo BANPARÁ;

b) Impedimento de licitar e contratar, prevista no artigo 7º da Lei nº 10.520/2002 ou no artigo 47 da Lei nº 12.462/2011, aplicada por qualquer órgão ou entidade integrante da Administração Pública do Estado do Pará;

c) Declaração de inidoneidade, prevista no inciso IV do artigo 87 da Lei nº 8.666/1993, aplicada por órgão ou entidade integrante da Administração Pública nacional, ou, a prevista no artigo 46 da Lei nº 8.443/1992, aplicada pelo Tribunal de Contas da União;

d) Proibição de contratar com o Poder Público aplicada com fundamento no artigo 12 da Lei nº 8.429/1992;

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 deste Edital**.

b) De cooperativas.

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

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

2.5. Esta licitação é de âmbito nacional.

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

3. PROCEDIMENTO DA LICITAÇÃO

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

a) Publicação do edital:

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

b) Credenciamento no sistema de licitações:

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

c) Eventual pedido de esclarecimento ou impugnação:

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

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

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

e) Cadastramento da proposta no sistema de licitações:

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

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

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

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

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

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

f) Avaliação das condições de participação:

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

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

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

g) Apresentação de lances:

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

i. A etapa de envio de lances na sessão pública durará **15** (**quinze) minutos** e, após isso, o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até

dez minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada.

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

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

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

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

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

h) Negociação:

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

i) Verificação de efetividade dos lances ou propostas:

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

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

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

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

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

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

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

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

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

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

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

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

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

j) Julgamento:

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

k) Habilitação:

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

l) Declaração de vencedor:

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

m) Interposição de recurso:

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

n) Adjudicação e homologação;

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

4. CREDENCIAMENTO E ACESSO AO SISTEMA DE LICITAÇÕES

4.1. Os interessados em participar deverão dispor de acesso no sistema de licitações www.gov.br/compras, no qual deverão realizar seu credenciamento e de

representante capacitado e habilitado a praticar os atos e transações inerentes à licitação.

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

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

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

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

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

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

4.8. Caberá ao licitante acompanhar as operações no sistema, antes, durante e após a sessão pública de lances, ficando responsável pelo ônus decorrente da perda de

negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

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

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

5. CONSULTAS, ADITAMENTOS E IMPUGNAÇÕES

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

5.1.1. Os pedidos de esclarecimentos e impugnações devem ser apresentados até às 23h59min (horário local) do **5º (quinto) dia útil** antes da data fixada para a ocorrência do certame, ou seja, até o dia **23/11/2022.**

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

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

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

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

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

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

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

6. APRESENTAÇÃO DA PROPOSTA NO SISTEMA DE LICITAÇÕES

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

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

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

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

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

6.2.4 Sua proposta foi elaborada de forma independente:

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

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

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

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

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

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

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

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

6.8 Quando o objeto licitado estiver enquadrado em algumas das vedações previstas no art. 17 da Lei Complementar nº 123/2016, os licitantes microempresas ou empresas de pequeno porte (ME/EPP) que forem optantes do Simples Nacional deverão formular suas propostas desconsiderando os benefícios tributários do regime a quem fazem jus.

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

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

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

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

6.10 No momento da inserção da proposta deverão ser inseridos em anexo os documentos de habilitação previstos **nos Itens 13 do Termo de Referência – Anexo I deste Edital e item 10 deste Edital**.

7 JULGAMENTO

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

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

ii. No caso de desconexão do(a) pregoeiro(a), no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

iii. Quando a desconexão do(a) pregoeiro(a) persistir por tempo superior a 10 (dez) minutos, a sessão da licitação eletrônica será suspensa e reiniciada somente após comunicação aos licitantes.

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

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

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

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

ii. Será permitida a apresentação de lances intermediários pelos licitantes, assim considerados os lances iguais ou superiores ao menor já ofertado, mas inferiores ao último lance dado pelo próprio licitante.

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

iv. Durante a fase de lances, o(a) pregoeiro(a) poderá excluir, justificadamente, lance cujo valor for considerado inexequível.

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

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

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

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

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

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

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

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

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

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

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

9 VERIFICAÇÃO DA EFETIVIDADE DOS LANCES E PROPOSTAS

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

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

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

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

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

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

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

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

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

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

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

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

9.7. O(a) pregoeiro(a) poderá negociar com o licitante autor da melhor proposta condições mais vantajosas, que poderão abranger os diversos aspectos da proposta, desde preço, prazos de pagamento e de entrega, sem que lhe caiba, a pretexto da

negociação, relativizar ou atenuar as exigências e condições estabelecidas no edital e nos seus documentos anexos.

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

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

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

- **a)** São vícios sanáveis, entre outros, os defeitos materiais atinentes à descrição do objeto da proposta e suas especificações técnicas, incluindo aspectos relacionados à execução do objeto, às formalidades, aos requisitos de representação, às planilhas de composição de preços, e, de modo geral, aos documentos de conteúdo declaratório sobre situações pré-existentes, desde que não alterem a substância da proposta;
- **b)** O(a) pregoeiro(a) não deverá permitir o saneamento de defeitos em propostas apresentadas com má-fé ou intenção desonesta, como aqueles contaminados por falsidade material ou intelectual ou que tentem induzir o(a) pregoeiro(a) a erro;
- **c)** O(a) pregoeiro(a) deverá conceder prazo adequado, recomendando-se 2 (dois) dias úteis, prorrogáveis por igual período, para que o licitante corrija os defeitos de sua proposta;
- **d)** O(a) pregoeiro(a) deverá indicar expressamente quais aspectos da proposta ou documentos apresentados junto à proposta devem ser corrigidos;
- **e)** A correção dos defeitos sanáveis não poderá importar alteração do valor final da proposta, exceto para oferecer preço mais vantajoso para o BANPARÁ;
- **f)** Se a proposta não for corrigida de modo adequado, o(a) pregoeiro(a) poderá conceder novo prazo para novas correções.

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

10 HABILITAÇÃO

10.1 O licitante autor da melhor proposta deve apresentar os documentos de habilitação exigidos neste item em formato digital por meio eletrônico,

exclusivamente no sistema **www.gov.br/compras** no momento de inserção da proposta de participação do presente pregão eletrônico.

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

10.2. O licitante deverá apresentar os seguintes documentos de **HABILITAÇÃO JURÍDICA**, que deverão estar acompanhados de todas as suas alterações ou da respectiva consolidação, quando for o caso, e deles deverá constar, **entre os objetivos sociais**, **a execução de atividades da mesma natureza do objeto desta licitação**:

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

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

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

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

10.3. QUALIFICAÇÃO TÉCNICA: o licitante deverá apresentar documentos de qualificação técnica conforme exigência **dos itens 13.1 e 13.2** do Termo de Referência, **ANEXO I** deste edital.

10.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA: O licitante deverá apresentar os documentos relativos à capacidade econômico-financeira exigidos **do item 13.3** do Termo de Referência, **ANEXO I** deste Edital.

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

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

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

b.1) No que se refere à certidão de regularidade fiscal emitida pela **fazenda pública municipal ou estadual**, quando for o caso, que, por ocasião da conferência da autenticidade online, ainda que dentro do prazo de validade, encontrar-se na situação "cassada", **o licitante poderá regularizá-la até o prazo final de análise dos documentos de habilitação.**

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

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

e) Certidão Negativa de Débitos Trabalhistas – CNDT.

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

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

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

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

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

10.7.1 Quando os documentos necessários à habilitação estiverem desatualizados no Sistema SICAF ou quando não estiverem nele

contemplados, deverão ser anexados no sistema Comprasnet junto com a documentação, conforme **item 10.1** acima.

10.8 Se o licitante desatender às exigências habilitatórias, o(a) pregoeiro(a) examinará a proposta e documentação do licitante subsequente, e assim, sucessivamente, até a apuração de documentação que atenda os termos do edital, cujo licitante será declarado vencedor.

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

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

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

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

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

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

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

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

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

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

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

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

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

11 RECURSOS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

251 – 1º andar – Bairro do Comércio – Belém/PA, CEP: 66.010-000, no horário de 9h as 16h (horário local).

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

12 ADJUDICAÇÃO E HOMOLOGAÇÃO

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

12.2 Na fase de homologação, a autoridade competente poderá:

a) Homologar a licitação;

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

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

i. O vício de legalidade for convalidável; ou

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

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

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

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

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

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

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

13 CONTRATAÇÃO

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

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

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

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

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

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

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

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

13.4 Todas as disposições sobre o contrato estão previstas na minuta do contrato, documento anexado ao edital - **ANEXO 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 2 (dois) anos, além das demais cominações legais cabíveis, nos seguintes casos:

a) Deixar de entregar a documentação exigida no certame;

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

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

d) Apresentar documentação falsa ou prestar declaração falsa;

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

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

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

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

a) Conduzir o processo administrativo;

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

c) Indicar a penalidade a que ele estará sujeito;

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

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

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

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

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

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

14.5. As penalidades referentes à inexecução do contrato estão estabelecidas na minuta do contrato - **ANEXO 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 2 (dois) funcionários designados.

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

15.9 Caso os atos lesivos apurados envolvam infrações administrativas à Lei n.8.666/1993, ao Regulamento ou outras normas de licitações e contratos da administração pública, e tenha ocorrido a apuração conjunta, o licitante também estará sujeito a sanções administrativas que tenham como efeito restrição ao direito de participar em licitações ou de celebrar contratos com a administração pública, a serem aplicadas no PAR.

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

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

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

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

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

16. DISPOSIÇÕES FINAIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16.18. Fazem parte integrante deste edital os seguintes anexos:

ANEXO I – TERMO DE REFERÊNCIA
ANEXO II – MODELO DE DECLARAÇÃO DE CONFORMIDADE AO ART.38 DA LEI Nº 13.303/2016
ANEXO III – MINUTA DE CONTRATO

Belém-PARÁ, 08 de Novembro de 2022.

Soraya Rodrigues
Pregoeira

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de soluções tecnológicas especializadas de serviços em telecomunicações, contemplando fornecimento de Redes MPLS concomitante ao uso de tecnologia SD-WAN com implantação, configuração, gerenciamento e manutenção da rede de enlaces dedicados para transmissão de dados nos sites remotos, possibilitando conexão de dados através de diferentes tecnologias, incluindo 3G ou superior, visando fornecer conectividade e disponibilidade para as unidades do Banpará espalhadas pelo Estado do Pará e os datacenters localizados em Belém, assim como enlaces de conectividade à rede Internet com solução anti-DDoS nos sites centrais, conforme especificações, exigências e condições estabelecidas neste Termo de Referência e seus Adendos.

2. MODALIDADE DA LICITAÇÃO

Considerando que o CONTRATANTE está sujeito à Lei nº 13.303/2016 e pelas razões apresentadas nas alíneas que seguem, adotou-se a modalidade pregão eletrônico para este processo licitatório, sendo que as normas da Lei nº 10.520/2002 serão aplicadas exclusivamente para a etapa externa da licitação, a partir da sua sessão pública de abertura até os atos de adjudicação e homologação.

2.1 JUSTIFICATIVA DA MODALIDADE DA LICITAÇÃO

1. O presente objeto caracteriza-se como serviço comum, com características e condições de fornecimento definidas objetivamente neste Termo de Referência, de acordo com a lei nº 10.520/2002 que define bens comuns como sendo “aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.
2. Os bens e serviços de tecnologia da informação são considerados benscomuns conforme acordão 1667/2017 do TCU no qual o relator Aroldo Cedrazdecidiu sobre a utilização de Pregão como meio de contratação de sistema de informática para a Casa da Moeda do Brasil (CMB), na decisão o relator define que “os padrões de desempenho e de qualidade do objeto estão objetivamente definidos por meio de especificações usuais no mercado, conforme detalhamento constante no termo de referência”, concluindo o voto considerando ”adequada a adoção da modalidade pregão, do tipo menor preço, para a contratação do objeto pretendido pela CMB”.
3. Em outro acórdão do TCU, 1548/2013, relatado por José Mucio Monteiro, cujo alvo de interposição foi a contratação pelo TSE de sistema de TI por meio de Pregão, o Tribunal decide por meio do voto do relator que “quanto à modalidade eleita para aquisição dos equipamentos, não vislumbro impedimentos ao emprego do pregão, uma vez que o objeto pretendido pode ser definido por meio de especificações objetivas e usuais no mercado. Do mesmo modo, os serviços de teste e integração desses componentes aos sistemas da Justiça Eleitoral, apesar de revestirem-se de caráter eminentemente técnico são

prestações comum nesse tipo de contratação e não possuem natureza intelectual ou criativa suficiente para desnaturar ou inviabilizar a utilização do pregão".

4. Portanto, a modalidade pregão, em sua forma eletrônica, será adotada para este processo de contratação, com fundamentação no Art. 33 do Regulamento de Licitações e Contratos do Banpará, pelo fato de o objeto poder ser definido e especificado com base em ampla pesquisa de mercado, realização de benchmark com bancos estaduais e nacionais. Dessa forma, ser plenamente especificado e seus padrões de desempenho facilmente qualificados neste Termo de Referência.
5. Não será vedada na presente licitação a participação de empresas consorciadas.
6. Na presente licitação, os Níveis Mínimos de Serviço são de total responsabilidade das CONTRATADAS, independentemente do acesso utilizado na última milha.
7. Podem participar deste Pregão as empresas cujo objeto social seja pertinente e compatível com o objeto desta licitação, inclusive as empresas reunidas em consórcio, que apresentem toda a documentação legalmente exigida para habilitação, além de atender às demais exigências constantes deste edital.
8. Em caso de participação de empresas em regime de consórcio, devem ser atendidas as exigências contidas nos itens que se seguem:
    a. As pessoas jurídicas que participarem organizadas em consórcio deverão apresentar, além dos documentos exigidos neste Edital, compromisso de constituição do consórcio, por escritura pública ou documento particular registrado em Cartório de Registro de Títulos e Documentos, discriminando a empresa líder, estabelecendo responsabilidade solidária com a indicação do percentual de responsabilidade de cada consorciada, bem como a etapa da participação na execução dos serviços, objeto da presente licitação, atendidas as condições previstas no Art. 51 do Decreto nº 7.581/2011.
    b. É vedada a participação de pessoa jurídica consorciada em mais de um consórcio ou isoladamente, bem como de profissional em mais de uma empresa, ou em mais de um consórcio.
    c. No consórcio de empresas brasileiras e estrangeiras, a liderança caberá, obrigatoriamente, a uma empresa brasileira.
    d. O prazo de duração do consórcio deve, no mínimo, coincidir com o prazo de conclusão do objeto licitado, até sua aceitação, por meio do Termo de Recebimento Definitivo.
    e. Os consorciados deverão apresentar compromisso de que não alterarão a constituição ou composição do consórcio, salvo aprovação pela Contratante, visando a manter válidas as premissas queasseguram a sua habilitação.
    f. Os consorciados deverão comprometer-se a apresentar, antes da assinatura do contrato decorrente desta licitação, o Instrumento de Constituição e o registro do Consórcio, subscrito por quem tenha competência em cada uma das empresas.
    g. Cada um dos consorciados deve apresentar a integralidade dos documentos sobre as condições econômicas e financeiras exigidos no edital.

3. JUSTIFICATIVA DA CONTRATAÇÃO

O BANPARÁ vem realizando amplos estudos na sua infraestrutura de TI visando torná-la cada vez mais capaz de disponibilizar os mecanismos necessários para que se possa trabalhar o negócio do Banco. Estes estudos prezam pela disponibilidade, confiabilidade e integridade dos dados do Banco, bem como desenvolver planos de contratações que estejam sempre à frente das demandas a fim de nunca termos escassez de recursos frente aos novos produtos e necessidades. Seguindo esta aderência ao negócio se faz necessária a contratação de Rede MPLS com tecnologia SD-WAN e links de Internet, os quais manterão os ambientes das redes WAN altamente necessários para a conectividade de toda a rede bancária implantada na capital e interior do Estado.

4. MODO DE DISPUTA:

Para esta contratação, será adotado o modo de disputa Aberto/Fechado.

5. CRITÉRIO DE JULGAMENTO:

O critério de julgamento será o de menor preço.

6. ESPECIFICAÇÃO DOS ITENS

LOTE	ITEM	OBJETO	MEIO DE TRANSMISSÃO	BANDA	QTDE
I	01	Enlace de Internet com Anti-DDoS	Fibra óptica	500mbps	2
	02	Concentrador	Fibra óptica	300mbps	2
	03	Enlace MPLS/SD-WAN	Fibra óptica	4mbps/10mbps	32
II	04	Concentrador	Fibra óptica	300mbps	2
	05	Enlace MPLS/SD-WAN	Satélite Banda Ku	4mbps uplink 1mbps downlink	50

A listagem completa das localidades dos links encontra-se nos ADENDOS I (LOTE I) e II (LOTE II).

6.1. Especificações exclusivas para o LOTE I.

6.1.1. Atendimento da última milha por meio de transmissão terrestre por meio guiado (fibra óptica, radiofrequência ou cabo de pares metálicos), conforme disposto no ADENDO I.

6.1.2. Ter latência de rede até 150ms (cento e cinquenta milissegundos).

6.2. Especificações exclusivas para o LOTE II.

6.2.1. Atendimento da última milha por meio de transmissão via satélite em banda KU, conforme disposto no ADENDO II.

6.2.2. Ter latência de rede de até 800ms (oitocentos milissegundos).

6.2.3. Os links satélites deverão ter banda mínima garantida de 50% das velocidades especificadas no ADENDO II.

6.3. Especificações comuns para os links dos LOTES 1 e 2.

6.3.1. Os concentradores de agência de ambos os lotes serão instalados nos datacenters localizados em Belém e possuirão tecnologia de fibra óptica.

6.3.2. Devem suportar a pilha de protocolos IP;

6.3.3. Suportar, além da transmissão de dados, também voz e imagem;

6.3.4. Permitir alteração (aumento ou diminuição) das velocidades contratadas, mediante solicitação de estudo de viabilidade técnica às CONTRATADAS.

6.3.5. Se a alteração de velocidade do item anterior implicar em troca de equipamentos ou inclusão de nova(s) interface(s) ou execução de serviço(s) por parte das CONTRATADAS, o(s) valor(es) do(s) mesmo(s) deve(m) se basear nas tabelas constantes dos ADENDOS I e II, que farão parte da proposta de preços do CONTRATADA.

6.3.6. Em caso de paralisação e/ou degradação de um enlace, o tempo de solução do problema deve observar o disposto nos ADENDOS I e II, sendo que não será admitida nova ocorrência, de mesma origem ou origem distinta, no intervalo de até 5 (cinco) dias corridos contados a partir da solução do primeiro problema;

6.3.7. Ter taxa de erro de pacotes mensal inferior a 10-6 (dez elevado a menos seis, equivalente a 0,0001%);

6.3.8. Ter taxa de perda de pacotes mensal inferior a 2% (dois por cento);

6.3.9. Serem permanentes, com capacidade de funcionar em tempo integral;

6.3.10. Serem automáticos, ou seja, uma vez que os equipamentos estejam configurados, basta ligá-los para que o enlace seja estabelecido;

6.3.11. Serem lógica e fisicamente independentes de qualquer outro enlace, tanto do BANPARÁ quanto de terceiros;

6.3.12. A rede de dados das CONTRATADAS deverão seguir as melhores práticas de projeto, implementação, operação, suporte e segurança de redes

de dados, segundo a série de documentos que compõem o BCP publicado pelo IETF;

6.3.13. A solução deve incluir todo o hardware e software necessários ao seu funcionamento, como roteadores, interfaces de roteadores, modems, antenas, cabos, conectores, adaptadores, parafusos e outros. Exemplo de itens que não precisam ser ofertados são os racks e os nobreaks, de propriedade do BANPARÁ.

6.3.14. Administrar os serviços e recursos utilizados na solução integrada da CONTRATANTE visando que as condições ideais de uso, bom funcionamento e operação dos recursos instalados sejam mantidos.

6.3.15. Responsabilizar-se pelos projetos, testes, instalação, configuração, operação, suporte técnico, manutenção e treinamento da solução fornecida pelas CONTRATADAS.

6.3.16. Garantir plena disponibilidade dos meios físicos utilizados para transmissão dos dados, bem como de suas conexões com os sites remotos da CONTRATANTE, de acordo com os critérios e padrões estabelecidos no Edital e neste Termo de Referência e seus ADENDOS.

6.3.17. Garantir plena disponibilidade dos meios físicos utilizados para transmissão dos dados, bem como de suas conexões com os sites principais da CONTRATANTE. Para tanto o Banco agendará periodicamente, de acordo com sua necessidade, testes de contingenciamento entre os links da Presidente Vargas e Municipalidade a fim de garantir a continuidade do negócio.

6.3.18. Oferecer manutenção e suporte técnico para os componentes do BACKBONE e os serviços da Rede fornecidos pelas CONTRATADAS.

6.3.19. Fornecer solução de comunicação integrada de Dados, Vídeo, Voz e Gerência dos pontos de interesse definidos pela CONTRATANTE.

6.3.20. Prover infraestrutura de Rede de Comunicação Digital composta de todas as funcionalidades necessárias ao bom funcionamento da rede, ter garantia de desempenho, baixo retardo e segurança.

6.3.21. Possibilitar melhorias qualitativas (disponibilidade, confiabilidade e escalabilidade) e de manutenção da rede de dados e ainda atender às necessidades de comunicação de dados, voz e vídeo da CONTRATANTE.

6.3.22. Fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos/recursos que forem necessários (roteadores, modems, meios de transmissão, terminais remotos satélite, cabeamento dos serviços, acessórios necessários) para o provimento dos serviços conforme solicitados neste Termo de Referência.

6.3.23. Os equipamentos/recursos serão de propriedade de cada CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos.

6.3.24. A infraestrutura de rede de cada CONTRATADA (backbones, POPs, equipamentos internos, roteadores CPE, enlaces, recursos de comunicação via satélite – segmento espacial e terrestre, dentre outros) deverá estar sempre dimensionada e preparada para suportar a totalidade dos serviços solicitados neste Termo de Referência, garantindo os níveis de desempenho especificados no mesmo.

6.3.25. As redes MPLS/SD-WAN deverão fazer QoS, fim a fim (CPE a CPE, incluindo a priorização dentro do backbone das CONTRATADAS), priorizando as aplicações conforme suas criticidades, que serão definidas pela CONTRATANTE após assinatura do contrato, em toda a rede MPLS da CONTRATANTE.

6.3.26. As redes MPLS/SD-WAN consistem das unidades listadas nos ADENDOS I e II, interligadas através de uma rede com arquitetura VPN IP/MPLS.

6.3.27. Caso solicitado pela CONTRATANTE, As CONTRATADAS deverão restringir a comunicação lógica de determinadas unidades prediais a um conjunto de unidades previamente definidas (restrição de acesso lógico a partir de faixas de endereçamento IP, portas TCP e UDP).

6.3.28. As CONTRATADAS deverão restringir a comunicação lógica de determinadas unidades prediais em até 15 (quinze) dias consecutivos, a partir da formalização de solicitação pela CONTRATANTE.

6.3.29. O limite de atuação das CONTRATADAS será a interface LAN do roteador que será conectado aos switches da CONTRATANTE.

6.3.30. As CONTRATADAS deverão providenciar a configuração lógica necessária para que a comunicação entre unidades prediais ocorra através da sua Rede de Acesso e backbone, em ambos os sentidos.

6.3.31. As CONTRATADAS deverão se comprometer com o atendimento dos futuros sites, a critério da CONTRATANTE, nas mesmas condições técnicas e de preço oferecidas à CONTRATANTE para o objeto deste Termo de Referência desde que haja viabilidade técnica.

6.3.32. A CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer unidade predial, de acordo com a lei 13.303/2016.

6.3.33. As redes MPLS/SD-WAN deverá transportar dados, vídeo e voz sobre o protocolo IP conforme modelo de QoS a ser definido entre a CONTRATANTE e as CONTRATADAS após assinatura do contrato.

6.3.34. As CONTRATADAS deverão prestar os serviços de comunicação de dados, por meio de VPN IP/MPLS conforme os seguintes padrões:

6.3.34.1. RFC 2547, BGP/MPLS VPNs

6.3.34.2. RFC 2447, Diff Serv Code Point

6.3.34.3. RFC 2917, A Core MPLSIP VPN Architecture;

6.3.34.4. Draft-ietf-l3vpn-rfc2547bis, BGP/MPLS IP VPNs.

6.3.35. A topologia lógica da rede VPN IP/MPLS criada será do tipo hub-spoke (estrela).

6.3.36. Os circuitos físicos de rede das CONTRATADAS deverão ser configurados com QoS e deverão utilizar os seguintes protocolos: MLPPP, PPP e ETHERNET.

6.3.37. As CONTRATADAS devem disponibilizar em todos os sites o protocolo de roteamento dinâmico BGP.

6.3.38. A rede de comunicação de dados deverá ter garantia de desempenho, segurança, e suporte a diversos protocolos e permitir a utilização de endereçamento IP privativo.

6.3.39. As soluções das CONTRATADAS deverão suportar a arquitetura DiffServ, incluindo DiffServ sobre redes MPLS conforme os seguintes padrões:

6.3.39.1. RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers;

6.3.39.2. RFC 2475, An Architecture for Differentiated Services;

6.3.39.3. RFC 2597, Assured Forwarding PHB Group;

6.3.39.4. RFC 2598, An Expedited Forwarding PHB;

6.3.39.5. RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Ser- vices.

6.3.40. De acordo com as prioridades e níveis de serviços requisitados, os diferentes tipos de tráfego que cursarão por meio dAs redes MPLS/SD-WAN deverão ser classificados nas classes de serviços (DiffServ), conforme descrito a seguir:

TIPO DE APLICAÇÃO	DESCRIÇÃO
a) Tempo Real Voz e Vídeo	Aplicações de voz e vídeo sensíveis a retardo (delay) e variações de retardo (jitter), que exigem priorização de tráfego e reserva de banda;
b) Missão Crítica	Aplicações interativas críticas para o negócio, que exigem entrega garantida, reserva de banda e tratamento prioritário;

c) Dados Alta Prioridade	Aplicações que necessitam de latência controlada – aplicações transacionais (ex: Base de Dados, SAP, PeopleSoft, Siebel, Financial, B2B, Supply Chain Management, Ariba, Microsoft SQL, DLSw+) e aplicações interativas (ex: Messenger, Net Meeting, Telnet, Citrix,PlaceWare);
d) Dados Média Prioridade	Aplicações que apresentam característica de rajada – Ex: Streaming de vídeo, E-mail (Lotus Notes, Outlook, SMTP, IMAP, etc), transferência de arquivos grandes (FTP), sincronização de base-de-dados, backups
e) Dados Baixa Prioridade	Aplicações não críticas com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato.
f) Gerenciamento	Aplicações de gerenciamento de redes e de sistemas que necessitam de uma banda mínima para atividades de suporte técnico;
g) Classe Default	Reservado

Tabela 1 – Classificação dos serviços

6.3.41. As políticas de QoS serão posteriormente definidas pelo CONTRATANTE em conjunto com AS CONTRATADAS para aplicação em cada site da rede, em até 20 dias úteis a contar das assinaturas do Contrato de Prestação do Serviço.

6.3.42. Em todos os circuitos de acesso deve ser habilitado o QoS, sendo obrigatório, no mínimo a definição de aplicações de baixa prioridade e de gerenciamento, as demais classes podem ser configuradas ou não de acordo com a necessidade e escolha das CONTRATADAS.

6.3.43. A CONTRATANTE poderá solicitar a qualquer momento a modificação nas configurações de QoS (classificadores, marcadores, escalonadores, policiamento, shaping, dentre outros) dos roteadores CPE, quando aplicável.

6.3.44. As CONTRATADAS deverão iniciar as configurações de QoS dos roteadores CPE e dos roteadores remotos em até 5 dias e terminar as configurações em até 30 dias consecutivos a partir da formalização de solicitação pela CONTRATANTE.

6.3.45. As CONTRATADAS deverão garantir o tráfego Real-Time na rede da CONTRATANTE.

6.3.46. As CONTRATADAS deverão garantir uma reserva máxima de banda de 97% para o tráfego das aplicações da CONTRATANTE em sua rede de acesso visando garantir a reserva de 3% para a classe default (supervisão da rede).

6.3.47. Padrões de endereçamento IP, roteamento e interconexão dAs redes MPLS/SD-WAN e Rede de Acesso:

6.3.48. A CONTRATANTE será responsável pelo mapa de endereçamento IP adotado nas redes MPLS/SD-WAN.

6.3.49. A CONTRATANTE poderá utilizar no interior de sua rede o plano de endereçamento IP que preferir. Entretanto, As CONTRATADAS deverão projetar e implementar a solução de forma a permitir a utilização do plano de endereços fornecido pela CONTRATANTE nas redes locais das unidades prediais.

6.3.50. A especificação da arquitetura de roteamento será definida pela CONTRATANTE, com a aprovação das CONTRATADAS.

6.3.51. As CONTRATADAS deverão projetar e implementar uma solução de roteamento que atenda aos requisitos de conectividade, balanceamento de tráfego e interconexão, baseada em roteamento dinâmico.

6.3.52. A solução de roteamento deverá ser projetada e implementada de forma escalável permitindo o crescimento da rede.

6.3.53. A solução de roteamento deverá permitir a convergência da rede em um tempo menor que 15 segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s) de backbone.

6.3.54. Os roteadores fornecidos devem:

6.3.54.1. Suportar o tráfego total do(s) enlace(s) a que estiver conectado utilizando, no máximo (considerando um período mínimo de amostragem de 5 minutos):

6.3.54.1.1. 70% (setenta por cento) da memória e 30% (trinta por cento) do processador nos roteadores concentradores (localizados nos dois sites centrais);

6.3.54.1.2. 80% (oitenta por cento) da memória e 60% (sessenta por cento) do processador nos roteadores CPE (localizados nos pontos remotos).

6.3.54.2. Ter capacidade de encaminhamento de pacotes compatível com o(s) enlace(s) a que estiver conectado;

6.3.54.3. Suportar configuração de, pelo menos, 3 (três) classes de serviço (QoS) baseados em protocolo, endereço de origem/destino ou porta TCP/UDP de origem/destino;

6.3.54.4. Suportar configuração de, pelo menos, 3 (três) classes de banda mínima garantida baseado em protocolo, endereço de origem/destino ou porta TCP/UDP de origem/destino;

6.3.54.5. Suportar configuração de, pelo menos, 10 (dez) filtros de pacotes baseados em protocolo, endereço de origem/destino ou porta TCP/UDP de origem/destino;

6.3.54.6. Suportar CIDR;

6.3.54.7. Disponibilizar um usuário com acesso somente de leitura a todas as suas configurações dos CPEs e Concentradores;

6.3.54.8. Disponibilizar informações através do protocolo SNMP versão 2v ou superior;

6.3.54.9. Suportar a configuração de traps SNMP;

6.3.54.10. Disponibilizar pelo menos uma interface RJ-45 com suporte ao padrão 802.3u ou superior para interligação à rede do BANPARÁ;

6.3.54.11. Disponibilizar pelo menos uma interface de rede WAN com suporte aos protocolos de camada de enlace PPP, Frame relay ou HDLC;

6.3.54.12. Estar, sempre que necessário, com as versões de firmware atualizadas, sem custo adicional ao BANPARÁ;

6.4. Serviço De Balanceamento Seguro De Circuitos De Agências

6.4.1. As CONTRATADAS deverão fornecer a solução SD-WAN para cada unidade listada nos ADENDOS I e II, de acordo com o LOTE que tiver conquistado, considerando os circuitos atualmente utilizados pela CONTRATANTE, sendo eles:

6.4.1.1. MPLS das CONTRATADAS.

6.4.1.2. Enlaces de outras operadoras.

6.5. Características específicas dos Concentradores SD-WAN (válidas para os dois LOTES)

6.5.1. Throughput de, no mínimo, 20 Gbps com a funcionalidade de reconhecimento e controle de aplicação habilitada, com tamanho do pacote HTTP 64K;

6.5.2. Suporte a, no mínimo, 4 milhões conexões simultâneas;

6.5.3. Suporte a, no mínimo, 300 mil novas conexões por segundo;

6.5.4. Throughput de, no mínimo, 20 Gbps de VPN IPSec;

6.5.5. Estar licenciado para, ou suportar sem o uso de licença, 2.000 mil túneis de VPN IPSEC Site-to-Site simultâneos;

6.5.6. Suportar no mínimo 3.9 Gbps de throughput de Inspeção SSL;

6.5.7. Deve possuir, pelo menos:

6.5.8. 16 interfaces 1000Base-T com conectores RJ-45;

6.5.9. 16 interfaces 1000Base-X com conectores SFP;

6.5.10. 2 portas USB.

6.5.11. Deve possui armazenamento interno, no mínimo, de 480GB em SSD;

6.5.12. Deve possuir fonte redundante “Hot Swappable”;

6.5.13. Estar licenciado, sem custo adicional, 10 sistemas virtuais lógicos (Contextos) por equipamento;

6.6. Características Específicas da Solução Remota SD-WAN (válidas para os dois LOTES)

6.6.1. Throughput de, no mínimo, 950 Mbps com a funcionalidade de reconhecimento e controle de aplicação habilitada, com tamanho do pacote HTTP 64K;

6.6.2. Suporte a, no mínimo, 900 mil conexões simultâneas;

6.6.3. Suporte a, no mínimo, 15 mil novas conexões por Segundo;

6.6.4. Throughput de, no mínimo, 75 Mbps de VPN IPSec;

6.6.5. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;

6.6.6. Suportar no mínimo 125 Mbps de throughput de Inspeção SSL;

6.6.7. Deve possuir, pelo menos:

6.6.8. 5 interfaces 1000Base-T com conectores RJ-45;

6.6.9. 1 porta USB.

6.6.10. Estar licenciado, sem custo adicional, 5 sistemas virtuais lógicos (Contextos) por appliance;

6.7. Características gerais comuns para os Concentradores SD-WAN e para as Soluções Remotas SD-WAN

6.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

6.7.2. O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;

6.7.3. Os dispositivos devem possuir suporte a 4094 VLAN Tags 802.1q;

6.7.4. Os dispositivos devem possuir suporte a agregação de links 802.3ad e LACP;

6.7.5. Os dispositivos devem possuir suporte a Policy based routing ou policy based forwarding;

6.7.6. Os dispositivos devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

6.7.7. Os dispositivos devem possuir suporte a DHCP Relay;

6.7.8. Os dispositivos devem possuir suporte a DHCP Server;

6.7.9. Os dispositivos devem suportar sFlow;

6.7.10. Os dispositivos devem possuir suporte a Jumbo Frames;

6.7.11. Os dispositivos devem suportar sub-interfaces ethernet logicas;

6.7.12. Deve suportar NAT dinâmico (Many-to-1);

6.7.13. Deve suportar NAT dinâmico (Many-to-Many);

6.7.14. Deve suportar NAT estático (1-to-1);

6.7.15. Deve suportar NAT estático (Many-to-Many);

6.7.16. Deve suportar NAT estático bidirecional 1-to-1;

6.7.17. Deve suportar Tradução de porta (PAT);

6.7.18. Deve suportar NAT de Origem;

6.7.19. Deve suportar NAT de Destino;

6.7.20. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

6.7.21. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

6.7.22. Deve suportar NAT64 e NAT46;

6.7.23. Deve implementar o protocolo ECMP;

6.7.24. Deve implementar balanceamento de link por hash do IP de origem;

6.7.25. Deve implementar balanceamento de link por hash do IP de origem e destino;

6.7.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

6.7.27. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

6.7.28. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis

estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

6.7.29. Enviar log para sistemas de monitoração externos, simultaneamente;

6.7.30. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

6.7.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

6.7.32. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

6.7.33. Suportar OSPF graceful restart;

6.7.34. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

6.7.35. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

6.7.36. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;

6.7.37. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

6.7.38. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

6.7.39. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

6.7.40. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

6.7.41. A configuração em alta disponibilidade deve sincronizar: Sessões;

6.7.42. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas NAT, QOS e objetos de rede;

6.7.43. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

6.7.44. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

6.7.45. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

6.7.46. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

6.7.47. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

6.7.48. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

6.7.49. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

6.7.50. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

6.8. Características Complementares de SD-WAN

6.8.1. A solução SDWAN deverá ser capaz de suportar no mínimo 04 links, que podem ser contratados pelo Banco junto a outras operadoras, com velocidades de no mínimo 50Mbps, sendo de tecnologias MPLS, 3G ou superior e novas tecnologias a serem implementadas.

6.8.2. Devem ser baseados em equipamentos físicos (appliances). Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

6.8.3. O appliance SD-WAN deverá ser fornecido com bandeja ou suporte para montagem em rack.

6.8.4. Além das interfaces utilizadas para os circuitos do(s) provedor(es) deve possuir pelo menos 1 (uma) interface GigabitEthernet (10/100/1000Base-T), que serão utilizadas na rede interna da CONTRATANTE.

6.8.5. Deve possuir capacidade de agregar e balancear, no mínimo, 2 (dois) circuitos de dados utilizando uma interface dedicada para cada circuito.

6.8.6. O Contratante poderá solicitar a instalação de circuitos adicionais (3G/4G/5G/ADSL ou similar) de outros fornecedores, sem custos adicionais, uma vez que os equipamentos SD-WAN deverão suportar conexões adicionais.

6.8.7. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

6.8.8. A solução deve prover gerência centralizada.

6.8.9. A solução deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

6.8.10. A solução deve ser escalável, suportando, no mínimo, todos os dispositivos da solução em uma mesma comunidade VPN neste contexto.

6.8.11. Solução deve ser capaz de prover uma arquitetura onde haja comunicação Matriz x Agência através de links MPLS ou acesso de internet local.

6.8.12. A solução deve suportar aos seguintes requisitos mínimos:

6.8.12.1. IPv6

6.8.12.2. VRRP ou Equivalente

6.8.12.3. VRF

6.8.12.4. BGP

6.8.12.5. OSPF

6.8.12.6. RIPv1

6.8.12.7. Dynamic Multipath

6.8.12.8. Policy Based Routing

6.8.12.9. Reconhecimento em camada 7 totalmente segregado da camada 4.

6.8.13. O reconhecimento de aplicações, deve ser atualizado de forma dinâmica e totalmente transparente para o no dispositivo.

6.8.14. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.

6.8.15. A solução, em sua modalidade física e/ou virtual, deve considerar os seguintes itens:

6.8.15.1. 802.1Q

6.8.15.2. BFD ou BGP

6.8.16. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv4 e quando requisitado possuir suporte a IPv6 mesmo que seja necessária substituição do equipamento, com o ônus das CONTRATADAS.

6.8.17. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

6.8.18. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes (Packet Loss), onde seja possível configurar um valor de limite (Threshold) para cada um destes itens, onde poderá ser utilizado como fator de decisão nas regras de SD-WAN.

6.8.19. A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores/destinos.

6.8.20. A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links.

6.8.21. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal

recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.

6.8.22. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

6.8.23. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

6.8.24. A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento.

6.8.25. A solução deve permitir a consulta via SNMPv2/v3 referente aos seguintes dados:

6.8.25.1. Estado atual dos links SD-WAN

6.8.25.2. Latência

6.8.25.3. Jitter

6.8.25.4. Packet Loss

6.8.25.5. Pacotes enviados / Pacotes Recebidos

6.8.25.6. Link Bandwitdth

6.8.26. A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:

6.8.26.1. Número de Sessões,

6.8.26.2. Volume de Tráfego,

6.8.26.3. IP de Origem e Destino e

6.8.26.4. Transbordo de Link (Spillover)

6.8.27. A Solução deve apresentar compatibilidade com modens USB (3G/4G/5G), onde estes sejam capazes de funcionar como circuito Ativo Ativo em relação à saída principal de internet, e alternativamente funcionar em uma arquitetura Ativo x Standby, onde apenas seja acionado na eventualidade de falha no link principal.

6.8.28. Solução deve ser capaz de suportar uma arquitetura de transporte Multicast IPv4 e IPv6 através de tuneis VPN.

6.8.29. Solução deve possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados:

6.8.29.1. Local

6.8.29.2. Integrada a servidor TACACS+ ou RADIUS

6.8.29.3. Integrada a servidor Ldap ou RADIUS

6.8.30. A Alta Disponibilidade provida pela solução de SD-WAN, independente em suas modalidades físicas ou virtual, deverá suportar balanceamento ativo – ativo, ativo – passivo, distribuído geograficamente.

6.8.31. A solução SD-Wan deve oferecer Troubleshooting em console de linha de comando ou gráfica, onde seja possível:

6.8.31.1. Executar Packet sniffer do tráfego interessante, filtrando por IP e Porta;

6.8.31.2. Realizar debug detalhado das fases de negociação de uma VPN;

6.8.32. A Solução SD-Wan deve oferecer visualização gráfica de:

6.8.32.1. Aplicações mais utilizadas com respectiva largura de banda

6.8.32.2. Shapping de Tráfego SD-WAN

6.8.32.3. IPs de Destino mais utilizados com respectivo número de Sessões e Largura de Banda associados

6.9. Reconhecimento e Controle de Aplicações

6.9.1. Os dispositivos deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

6.9.2. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

6.9.3. Deve possibilitar a diferenciação de tráfegos possuindo granularidade de controle/políticas para os mesmos;

6.10. QoS e Traffic Shaping

6.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda.

6.11. VPN

6.11.1. Suportar IPSec VPN;

6.11.2. Suportar SSL VPN;

6.11.3. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

6.11.4. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

6.11.5. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

6.11.6. A funcionalidades de VPN devem ser atendidas com ou sem o uso de agente;

6.12. Solução de Gerenciamento Centralizado

6.12.1. Deve permitir gerenciar dispositivos e possuir capacidade ampliação de até 300 dispositivos gerenciados;

6.12.2. Deve ser fornecido em appliance físico;

6.12.3. Deve possuir fonte redundante “Hot Swap”.

6.12.4. Gerar alertas automáticos via Email;

6.12.5. Gerar alertas automáticos via SNMP;

6.12.6. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

6.12.7. Deve permitir que todos os controladores/concentradores sejam controlados de forma centralizada utilizando apenas um servidor de gerência;

6.12.8. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador a leitura das licenças nos appliances através dessa ferramenta.

6.12.9. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

6.12.10. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

6.12.11. Deve permitir criar fluxos de aprovação na solução de gerência, onde as CONTRATADAS possam criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação da CONTRATANTE;

6.12.12. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

6.12.13. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

6.12.14. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados (remotos), tais

como hostname, serial, IP de gerência, licenças, horário do sistema, features ativadas e versão do firmware;

6.12.15. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

6.12.16. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

6.12.17. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

6.12.18. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;

6.12.19. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

6.12.20. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

6.12.21. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

6.12.22. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

6.12.23. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

6.13. Solução de Gerenciamento de Eventos e Relatórios

6.13.1. Deve suportar receber logs de todos os dispositivos ativados na rede;

6.13.2. Deve ser fornecido em virtual appliance ou appliance físico; deve possuir capacidade de armazenamento, no mínimo, de 2 TB;

6.13.3. Para appliance físico, deve possuir, no minimo, 6 portas 1000Base-T com conectores RJ-45;

6.13.4. Em ambiente virtual, deverá ser compatível com ambiente VMware ESXi 5.5 e 6.0, Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e Citrix XenServer 6.0+;

6.13.5. Possuir capacidade de receber ao menos 10 GBytes de logs diários;

6.13.6. Possuir ao menos 10 TB de espaço em disco;

6.13.7. Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.

6.13.8. Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);

6.13.9. Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;

6.13.10. Suportar SNMP versão 2 e versão 3 na solução de relatórios;

6.13.11. Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

6.13.12. Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios;

6.13.13. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

6.13.14. Autenticação integrada a servidor Radius;

6.13.15. Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela;

6.13.16. Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas;

6.13.17. Autenticação integrada ao Microsoft Active Directory;

6.13.18. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

6.13.19. Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos;

6.13.20. Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;

6.13.21. Possuir mecanismo para que logs antigos sejam removidos conforme determinação da CONTRATANTE;

6.13.22. Permitir a importação e exportação de relatórios;

6.13.23. Deve possuir a capacidade de criar relatórios nos formatos HTML, PDF, XML e CSV;

6.13.24. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

6.13.25. Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar;

6.13.26. A solução deve possuir relatórios pré-definidos, devendo ser possível a customização dos mesmos;

6.13.27. Possuir envio automático de logs para um servidor FTP externo a solução;

6.13.28. Possibilitar a duplicação de relatórios existentes e editá-los logo após;

6.13.29. Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;

6.13.30. Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;

6.13.31. Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios;

6.13.32. Possibilitar mecanismo "Drill-Down" para navegação nos relatórios em realtime;

6.13.33. Dever ser possível fazer download dos arquivos de logs recebidos;

6.13.34. Deve possuir agendamento para gerar e enviar automaticamente relatórios;

6.13.35. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;

6.13.36. Permitir o envio de maneira automática de relatórios por email;

6.13.37. Deve permitir a escolha do email a ser enviado para cada relatório escolhido;

6.13.38. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;

6.13.39. Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados;

6.13.40. Deve ser possível definir filtros nos relatórios;

6.13.41. Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;

6.13.42. Permitir que relatórios criados sejam no idioma português;

6.13.43. Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros;

6.13.44. Deve permitir o envio automático de relatórios criados a um servidor de SFTP ou FTP externo a solução;

6.13.45. Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;

6.13.46. Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;

6.13.47. Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado;

6.13.48. Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios;

6.13.49. Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs;

6.13.50. A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes;

6.13.51. Deve possuir a informação da quantidade de logs armazenados e estatística de tempo de retenção restante;

6.13.52. Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios;

6.13.53. Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar;

6.13.54. Deve permitir ver em tempo real os logs recebidos;

6.13.55. Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

6.13.56. Deve possuir relatório de PCI DSS Compliance;

6.13.57. Deve possuir relatório de utilização de aplicações SAAS;

6.13.58. Deve possuir relatório de VPN;

6.14. Requisitos técnicos mínimos dos links de conectividade à rede Internet:

6.14.1. Declaração, emitida pelas CONTRATADAS, de que sua própria rede de dados e o link de Conectividade à internet com solução anti-DDoS oferecido ao Banpará atendem aos pré-requisitos mínimos de segurança física e lógica para evitar qualquer tipo de ação (ataque ou invasão), intencional ou não, que prejudique a disponibilidade, a confidencialidade ou a confiabilidade dos dados transmitidos;

6.14.2. Disponibilizar 2 (dois) enlaces para transmissão de dados para Conectividade a Internet nos sites indicados pelo BANPARÁ, com as seguintes funcionalidades:

6.14.2.1. Suporte à pilha de protocolos IP;

6.14.2.2. Taxa de Transmissão (Velocidade) simétrica (nos dois sentidos) mínima de 500 Mbps para cada enlace;

6.14.2.3. Meio físico de acesso: fibra ótica;

6.14.2.4. Protocolo de acesso: Ethernet ou Fast Ethernet;

6.14.3. A título de melhoria qualitativa das conexões à Internet, será permitido alteração (aumento ou diminuição) de velocidade e aumento do número de links. Se houver necessidade de troca ou adição de equipamento(s) ou execução de serviço(s) de reconfiguração lógica ou física, o(s) mesmo(s) poderão incidir em custos ao Banpará, resguardados os limites da Lei 13.303/2016;

6.14.4. Ter disponibilidade diária superior a 99,7% (noventa e nove e sete décimos por cento), equivalente a pouco mais de 4 minutos de indisponibilidade por dia;

6.14.5. Ter disponibilidade mensal superior a 99,9% (noventa e nove e nove décimos por cento), equivalente a pouco mais de 43 minutos de indisponibilidade por mês;

6.14.6. Ter latência de rede inferior a 75 (setenta e cinco) ms;

6.14.7. Ter taxa de erro inferior a 1% (um por cento);

6.14.8. Ter taxa de perda de pacotes inferior a 1% (um por cento);

6.14.9. Ser permanente, com capacidade de funcionar em tempo integral;

6.14.10. Ser automático, ou seja, uma vez que os equipamentos estejam configurados, basta ligá-los para que o enlace seja estabelecido;

6.14.11. Ser lógica e fisicamente independentes de qualquer outro enlace, tanto do Banpará quanto de terceiros;

6.14.12. Interligar o Banpará diretamente ao centro de roteamento das CONTRATADAS;

6.14.13. Seguir as melhores práticas de projeto, implementação, operação, suporte e segurança, segundo a série de documentos que compõem o Best Current Practices;

6.14.14. Vir acompanhado de todo o hardware que se faça necessário ao seu funcionamento, como roteador (que deve ser compatível com rack padrão EIA-310-D já existente, de propriedade do Banpará), cabos, conectores, e parafusos. Esses equipamentos devem ser de propriedade das CONTRATADAS e estar dentro da garantia de suporte do fabricante;

6.14.15. Interligar o Banpará à Internet utilizando-se exclusivamente da rede de dados das CONTRATADAS, sem utilização de redes de dados de terceiros;

6.14.16. Fornecimento de circuitos com conectividade direta a rede INTERNET através de acessos dedicados, portas IP exclusivas com protocolo de roteamento BGP, garantindo a disponibilidade do serviço entre os sites, e solução anti-DDoS aplicada no backbone das CONTRATADAS a partir da velocidade de 1 Gbps.

6.15. Requisitos complementares dos enlaces das Redes MPLS:

6.15.1. As CONTRATADAS deverão fornecer todos os equipamentos necessários à prestação do serviço de transmissão de dados bidirecional quando via satélite, tais como: antena, modem satélite, cabeamento, conectores, infraestrutura da base da antena e etc, até os equipamentos que permitam a integração com a rede local da CONTRATANTE.

6.15.2. Caberá às CONTRATADAS elaborar as especificações e o dimensionamento, bem como o fornecimento, instalação e manutenção dos equipamentos necessários à prestação dos serviços solicitados.

6.15.3. A transmissão e recepção dos sinais de dados via satélite poderão ser realizadas diretamente das dependências da CONTRATANTE e/ou através de compartilhamento de estação terrena das CONTRATADAS. Em caso de compartilhamento de estação terrena das CONTRATADAS deverão ser utilizado acesso dedicado e exclusivo entre esta e o site central da CONTRANTANTE até a integração com sua rede local.

6.15.4. Todas as especificações devem estar plenamente disponíveis nos equipamentos entregues, sem a necessidade de quaisquer outras aquisições.

6.15.5. Para os links que utilizem tecnologia satélite, as características técnicas mínimas a serem contratadas são:

6.15.5.1. Cobertura em todo o território do Estado do Pará;

6.15.5.2. Operação em banda Ku, conforme ADENDO II;

6.15.5.3. Disponibilidade anual, para:

6.15.5.3.1. Links que utilizem tecnologia de fibra óptica ou par metálico: 99,7%;

6.15.5.3.2. Links que utilizem tecnologia de satélite em Banda Ku: 99,5%;

6.15.5.4. Simultaneidade das conexões na HMM: no mínimo 80% (vinte porcento) dos sites remotos.

6.15.6. Excetuando-se os links de satélite, todos os demais links devem possuir simetria de velocidade.

6.15.7. As CONTRADADAS deverão possuir atendimento operacional e de recuperação no Brasil 24 horas por dia, 7 dias por semana e em língua portuguesa;

6.15.8. As CONTRATADAS deverão fornecer o segmento espacial e equipamentos para o perfeito funcionamento do contingenciamento das redes MPLS/SD-WAN da CONTRATANTE;

6.16. Informações complementares quanto ao serviço Anti-DDoS (links de Internet).

6.16.1. As CONTRATADAS deverão disponibilizar em seu backbone proteção contra ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS e DDOS, considerando os requisitos mínimos a seguir:

6.16.2. Serviços deverão ter pró-atividade para solução e prevenção de incidentes e ataques;

6.16.3. Monitorar disponibilidade e performance de todos os links de dados existentes nesse termo de referência em regime 24x7 utilizando profissionais de forma dedicada;

6.16.4. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pelas CONTRATADAS.

6.16.5. A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

6.16.6. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

6.16.7. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

6.16.7.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

6.16.7.2. Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

6.16.7.3. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

6.16.7.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

6.16.7.5. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS.

6.16.8. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pelas CONTRATADAS.

6.16.9. As CONTRATADAS devem possuir dois centros de limpeza nacional cada um com capacidade de mitigação de 1GB, centro de limpeza internacional com capacidade de mitigação de 30GB.

6.16.10. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole.

6.16.11. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

6.16.12. As CONTRATADAS devem disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

6.16.13. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.

6.16.14. Em momentos de ataques DOS e DDOS, todo tráfego limpo deve ser reinjetado na infraestrutura da CONTRATANTE através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDOS das CONTRATADAS e o CPE do CONTRATANTE.

6.16.15. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.

6.16.16. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual

6.16.17. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas das CONTRATADAS.

6.16.18. AS CONTRATADAS têm um prazo de até 15 minutos para iniciar a mitigação de ataques de DDOS.

6.16.19. As CONTRATADAS deverão disponibilizar uma Solução de Monitoração de acompanhamento contra ataques, que contemple Quadro Sinóptico, em aplicação web, para visualização da ocupação de banda do link Internet e níveis de severidade dos ataques.

6.16.20. Os alertas, que deverão fornecer, no mínimo, as seguintes funcionalidades:

6.16.20.1. Visualização de informações on-line, de forma gráfica, da banda consumida no ataque;

6.16.20.2. Acompanhamento do nível de importância do ataque, o percentual do nível de severidade do ataque, o consumo de banda do ataque e tipo do ataque e classificação.

6.16.20.3. Origem de ataques, com identificação do endereço IP e porta de origem.

6.16.20.4. Destino de ataques, com identificação do endereço IP e porta de destino.

6.16.20.5. Protocolo de transporte do alerta.

6.16.20.6. Cada alerta deverá ter um número de identificação que facilite sua consulta.

6.16.20.7. Informar a data de início e fim do acompanhamento do alerta

6.16.20.8. Volume de ataques sumarizados por hora, dia, semana e mês.

6.16.20.9. Relatório por tipos de ataques em PDF.

6.16.21. O Portal de monitoração das CONTRATADAS deverão possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

6.16.22. Disponibilizar usuários a serem definidos pela CONTRATANTE com acesso (somente de leitura) a todos os módulos da aplicação;

6.16.23. O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da CONTRATANTE.

6.16.24. As CONTRATADAS deverão:

6.16.24.1. Implementar, em sua rede de dados, os pré-requisitos mínimos de segurança para evitar qualquer tipo de ação (ataque ou invasão), intencional ou não, que prejudique a disponibilidade, a confidencialidade ou a confiabilidade dos dados transmitidos;

6.16.24.2. Possuir centro de roteamento no Brasil;

6.16.24.3. Possuir pelo menos 1 (um) servidor DNS que, a critério do Banpará, poderá ter uma cópia de sua base de dados DNS, para aumentar a disponibilidade do serviço (servidor secundário);

6.16.24.4. Possuir pelo menos 2 (dois) servidores DNS para consulta reversa dos endereços IP alocados ao Banpará (DNS reverso);

6.16.24.5. Possuir pelo menos 2 (dois) caminhos diferentes (sem ponto único de falha) para fora do estado do Pará;

6.16.24.6. Ter em seu quadro funcional técnicos para prestar os serviços relacionados aos enlaces e aos equipamentos. Esses técnicos, em caso de atendimento dentro das dependências do Banpará, deverão sempre se apresentar com uniforme e crachá do respectivo empregador. As CONTRATADAS devem sempre manter atualizada a lista de técnicos junto do Banpará;

6.16.24.7. Fornecer serviços de gerência pró-ativa dos enlaces, de forma a detectar e/ou corrigir, em tempo integral, qualquer anormalidade que venha a ocorrer nos enlaces ou nos equipamentos do licitante vencedor, não sendo necessário que o Banpará entre em contato para comunicar uma anormalidade;

6.16.24.8. No caso de qualquer anormalidade, o Banpará deve ser avisado sobre a mesma, em no máximo em 15 (quinze) minutos, através de um dos telefones divulgados no ato de assinatura do contrato e/ou e-mail corporativo;

6.16.24.9. Os dados referentes ao monitoramento podem trafegar pelos próprios enlaces fornecidos, através de VPNs com criptografia, alta prioridade (QoS alto) e tráfego máximo de 10 (dez) Kbps.

6.16.24.10. Emitir relatório mensal contendo, por exemplo, taxa de utilização, percentual de disponibilidade, horários de início e término de falhas, ativações, desativações, remanejamentos e mudanças de configuração;

6.16.24.11. Possuir equipes técnicas sediadas na região metropolitana de Belém e nas cidades de Marabá e Santarém;

6.16.24.12. Negociar com o Banpará, com antecedência mínima de 5 (cinco) dias corridos, qualquer interrupção programada em algum de seus enlaces de dados;

6.16.24.13. Disponibilizar um bloco CIDR de, pelo menos, 128 (cento e vinte e oito) endereços IP contínuos, de acordo com as orientações do IAB, que deve atender aos dois enlaces simultaneamente;

6.16.24.14. Executar os serviços de alteração de velocidade conforme demanda da CONTRATANTE (item 8.2.5) em até 30 (dias) dias úteis após solicitação feita por um dos canais disponibilizados (itens 8.4.12);

6.16.24.15. Limitar sua atuação à interface de rede local de seu roteador CPE.

6.16.24.16. Cancelar o faturamento dos links para os quais for solicitada desativação a partir do dia seguinte à respectiva solicitação de desativação.

6.16.25. Caberá às CONTRATADAS elaborar as especificações e o dimensionamento de infraestrutura, fornecer roteador e backbone para atender a rede da CONTRATANTE, bem como instalar, configurar, testar, operar, prestar suporte técnico, manter e fornecer equipamentos.

7. DA TOPOLOGIA

7.1. As topologias da rede de enlace de dados MPLS e dos links de Internet constam no ADENDO III

7.2. Todos os enlaces das redes de dados MPLS devem ligar as unidades a pelo menos um dos dois data center do BANPARÁ (localizados na cidade de Belém nos endereços: R. Municipalidade, 1036 e Pres. Vargas, 251) através de topologia ponto-a-ponto ou ponto-multiponto. Neste último caso, cada enlace separadamente deve atender aos requisitos técnicos.

7.3. A chegada dos enlaces da rede de dados MPLS poderá ser distribuída entre os dois data centers (como forma de aumentar a disponibilidade, devendo as CONTRATADAS disponibilizar estrutura física (facilidade) e lógica (configuração de equipamento) nos dois locais.

7.4. A largura de banda dos enlaces dos data centers referente à Rede MPLS deve ser igual ou superior a 80% (oitenta por cento) da soma das larguras de banda de todos pontos remotos, devendo ser adequado sempreque for necessário.

8. CRITÉRIOS DE SUSTENTABILIDADE

8.1. As CONTRATADAS se comprometem a atender às diretrizes da Política de Responsabilidade Socioambiental do Banpará – PRSA do Banpará, disponível em https://www.banpara.b.br/socioambiental/politica-rsa/, considerando os requisitos:

8.2. 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. 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.

8.4. 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.

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

8.6. 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.

8.7. Desenvolver suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados 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.

8.8. Atender à Política Nacional de Resíduos Sólidos (Lei 12.305/2010), observando quanto ao descarte adequado e ecologicamente correto.

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

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

8.11. Adotar práticas e métodos voltados para a preservação da confidencialidade e integridade, atentando à Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018.

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

9. CRITÉRIO DE JULGAMENTO

Conforme definido nos incisos I a VI do Artigo 42 da Lei n. 13.303/2016, o regime a ser adotado para a contratação do objeto deste Termo de Referência é empreitada por preço global.

10. EXECUÇÃO DOS SERVIÇOS

10.1 As CONTRATADAS deverão, no ato de assinatura do contrato, apresentar:

10.1.1 Projeto de implantação dos serviços contratados, contendo as ações e respectivos prazos;

10.2.2 Lista com o(s) número(s) de telefones e o endereço eletrônico definido para contatos;

10.3.3 Lista dos técnicos, seus ou de subcontratados, aptos a efetuar atendimentos locais.

10.2 Dentre as atividades iniciais, citamos:

10.2.1 Instalação física do hardware fornecido;

10.2.2 Configuração dos roteadores fornecidos (SNMP, VPNs, syslog e outros);

10.3 Os enlaces devem estar ativos dentro dos prazos definidos para instalação no Item 15 deste Termo de Referência.

10.4 O prazo de conclusão da homologação da solução é de 10 (dez) dias corridos;

11. NÍVEIS MÍNIMOS DE SERVIÇO

11.1. Considera-se um enlace como disponível quando o mesmo pode trafegar dados nos dois sentidos e quando os níveis de “taxa de erro”, “taxa de perda de pacotes” e “latência de rede” estão todos dentro dos limites definidos no item 11.1 deste Termo de Referência, considerando um período de 5 (cinco) minutos.

11.2. O percentual de disponibilidade é calculado pela fórmula DE=(1440*D-Ti)*100/(1440*D), onde “Ti” é a quantidade de minutos em que o enlace ficou indisponível e “D” é a quantidade de dias considerados.

11.3. Para efeito de cálculo, deve sempre ser considerado o intervalo entre 00:00 e 23:59 no horário de Belém.

11.4. Serão desconsideradas, para efeito de cálculo de indisponibilidade, as paralisações ocasionadas pelo BANPARÁ ou por motivo de força maior.

11.5. O percentual de disponibilidade mínimo será de 99,7% para links terrestres e 99,5% para links satélite.

11.6. Os valores mensais totais referentes às glosas aplicadas por descumprimento dos tempos de SLA (ADENDOS I e II) e de ativação de links, deverão ser abatidos na fatura do mês subsequente, após validação da apuração do responsável técnico do BANPARÁ.

11.7. Serão aplicadas glosas nos valores dos enlaces contratados em caso de descumprimento de prazos definidos nos cronogramas de ativação acordados entre o Banpará e as CONTRATADAS, conforme abaixo.

11.8. Para os enlaces de Rede de dados MPLS:

11.8.1. De 5% (cinco por cento) do valor da mensalidade do respectivo enlace para cada dia ou fração de dia de atraso, limitado a 75 (setenta e cinco) dias, nos casos abaixo:

11.8.1.1. Após 60 (sessenta) dias corridos da assinatura do contrato, caso a solução não seja entregue para homologação, no caso de enlaces com tecnologia satélite;

11.8.1.2. Após 30 (trinta) dias corridos da assinatura do contrato, caso a solução não seja entregue para homologação, no caso de enlaces com tecnologia terrestre.

11.8.2. De 3% (três por cento) do valor mensal do respectivo enlace para cada dia ou fração de dia de atraso, limitado a 30 (trinta) dias, nos casos abaixo:

11.8.2.1. Após 60 (sessenta) dias corridos da notificação formal, caso não tenha sido realizada a ativação de um novo enlace, no caso de enlaces com tecnologia satélite;

11.8.2.2. Após 30 (trinta) dias corridos da notificação formal, caso não tenha sido realizada a ativação de um novo enlace, no caso de enlaces com tecnologia terrestre;

11.8.2.3. Após 60 (sessenta) dias corridos da notificação formal, caso não tenha sido realizada a alteração de velocidade de um enlace, no caso de enlaces com tecnologia satélite;

11.8.2.4. Após 30 (trinta) dias corridos da notificação formal, caso não tenha sido realizada a alteração de velocidade de um enlace, no caso de enlaces com tecnologia terrestre;

11.8.3. De 1% (um por cento) do valor mensal do respectivo enlace para cada dia ou fração de dia de atraso, limitado a 30 (trinta) dias, nos casos abaixo:

11.8.3.1. Após 5 (cinco) dias úteis da notificação formal, caso um serviço/equipamento tenha sido executado/entregue com defeito ou fora das especificações sem que tenha sido realizada a correção/substituição do mesmo;

11.8.3.2. Após 5 (cinco) dias úteis da notificação formal, caso não tenha sido realizada a troca de equipamento que apresente 3 (três) falhas ou problemas semelhantes em um período de até 3 (três) meses;

11.8.3.3. Após 2 (dois) dias úteis do encerramento de um chamado técnico sem que o respectivo relatório de solução tenha sido disponibilizado;

11.8.4. De 5% (cinco por cento) do valor mensal do respectivo enlace para cada hora ou fração de hora corrida, limitado a 36 (trinta e seis) horas, após 30 (trinta) minutos corridos quando de uma falha em um Data center do BANPARÁ sem que os enlaces MPLS a ele conectados sejam remanejados ao outro Data center;

11.8.5. De 5% (cinco por cento), para os enlaces MPLS, do valor mensal do respectivo enlace para cada hora ou fração de hora corrida, após o limite de tempo de solução estabelecido nos ADENDOS I e II, limitado a 72 (setenta e duas) horas;

11.8.6. De 1% (um por cento) do valor mensal do respectivo enlace para cada caso de não cumprimento do tempo mínimo entre períodos de indisponibilidade;

11.8.7. De 0,1% (um décimo por cento) do valor global do contrato para cada dia ou fração de dia de atraso, limitado a 75 (setenta e cinco) dias, após 15 (quinze) dias corridos após a assinatura do contrato, na entrega dos documentos a seguir: projeto de implantação dos serviços contratados, contendo as ações e respectivos prazos; lista com o(s) número(s) de telefones e o endereço eletrônico de recorrência para as devidas aberturas de chamados técnicos.

11.9. Para os enlaces de Rede de Conectividade Internet:

11.9.1. No caso de atraso injustificado, execução parcial ou inexecução do contrato, as CONTRATADAS ficarão sujeitas, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e comprovados, a critério da Administração, e ainda garantida prévia e ampla defesa, à aplicação das glosas abaixo, cumulativamente ou não, com as demais penalidades previstas neste instrumento:

11.9.1.1. De 0,1% (um décimo por cento) do valor global do contrato para cada dia ou fração de dia de atraso nos casos abaixo:

11.9.1.1.1. Após 60 (sessenta) dias corridos da assinatura do contrato, caso não seja realizada a homologação da solução neste prazo;

11.9.1.1.2. Após 5 (cinco) dias úteis da notificação formal, caso um serviço ou equipamento tenha sido executado ou entregue com defeito ou fora das especificações contratadas sem que tenha sido realizada a substituição do mesmo;

11.9.1.1.3. Após 5 (cinco) dias úteis da notificação formal, caso não tenha sido realizada a troca de equipamento que apresente 3 (três) falhas ou problemas semelhantes em até 3 (três) meses;

11.9.1.1.4. Após 30 (trinta) dias corridos da notificação formal, caso não tenha sido realizada a alteração de velocidade dos enlaces;

11.9.1.1.5. Após 2 (dois) dias úteis, caso não tenha sido realizada a substituição de funcionário das CONTRATADAS.

11.9.1.2. De 1% (um por cento) do valor mensal para cada anormalidade/indisponibilidade detectada pelo CONTRATANTE antes que o mesmo seja avisado pelo CONTRATADO;

11.9.1.3. De 1% (um por cento) do valor mensal para cada hora ou fração de hora corrida após 24 (vinte e quatro) horas corridas do encerramento de um chamado técnico sem que o respectivo relatório de solução tenha sido disponibilizado;

11.9.1.4. De 5% (cinco por cento) do valor mensal do enlace para cada hora ou fração de hora corrida, após o limite de tempo de solução estabelecido nos ADENDOS I e II, limitado a 72 (setenta e duas) horas

11.10. Em caso de indisponibilidade de um enlace além do limite permitido, conforme SLA informado nos ADENDOS I e II, deixará de ser cobrado o valor relativo a este período de tempo.

12. DAS DEFINIÇÕES DO ACORDO DE NÍVEL DE SERVIÇO (SLA)

12.1. Métricas e Definições das redes de enlace de dados MPLS e de Conectividade à Internet:

12.1.1. Disponibilidade dos enlaces: é o percentual de tempo em que um enlace ficou disponível para uso;

12.1.2. Taxa de erro: é o percentual de pacotes enviados com erro em relação ao total de pacotes enviados;

12.1.2.1. É calculado pela fórmula Te=E*100/T, onde “E” é a quantidade de pacotes enviados com erro e “T” é o total de pacotes enviados.

12.1.2.2. A taxa de erro de pacotes mensal deverá ser inferior a 10-6 (dez elevado a menos seis, equivalente a 0,0001%);

12.1.3. Taxa de perda de pacotes: é o percentual de pacotes não transmitidos devido a algum problema no enlace;

12.1.3.1. É calculado pela fórmula Tpp=P*100/T, onde “P” é a quantidade de pacotes perdidos e “T” é o total de pacotes enviados.

12.1.3.2. A taxa de perda de pacotes mensal deverá ser inferior a 2% (dois por cento).

12.1.4. Latência de rede: é o tempo gasto entre a transmissão do primeiro bit de um pacote até a recepção do último bit do mesmo pacote, pelo próximo elemento da rede, em um único sentido de tráfego;

12.1.4.1. É calculado pela fórmula L=T/(5*2), onde “T” a soma dos tempos que 5 pacotes ICMP gastam para ir e voltar. Os pacotes usados no teste devem ser do tipo 8 (echo request) e tamanho de 32 bytes. O intervalo entre pacotes deve ser no máximo 1 segundo e o tempo máximo de espera (timeout) é de 5 segundos;

12.1.4.2. Para maior exatidão no teste, o mesmo deve ser executado a partir de um equipamento o mais próximo possível do limite de atuação das CONTRATADAS (do ponto de vista de topologia de rede), salvando-se a saída dos comandos digitados para posterior cálculo;

12.1.4.3. Pacotes que excederem o timeout serão considerados, para efeito de cálculo, como tendo tempo de resposta de 10 segundos.

12.1.5. Velocidade (Taxa de Transmissão): É a quantidade de bits que podem ser transmitidos durante um segundo;

12.1.5.1. É calculado pela fórmula V=(X+C)/T, onde “X” é tamanho em bits de um arquivo transmitido por FTP entre dois computadores situados cada um em cada ponta do enlace, “T” é o tempo em segundos gasto nessa transmissão e “C” é o tamanho em bits dos cabeçalhos dos protocolos em uso (camada física, camada de enlace, IP e FTP);

12.1.5.2. Para maior exatidão no teste, deve-se assegurar que nenhuma outra transmissão é feita nesse enlace durante esse período, embora se aceite uma variação de até 5% para mais ou para menos.

12.2. Observações:

12.2.1. Os testes referentes à latência de rede e velocidade podem ser realizados a cada 15 minutos, a critério do BANPARÁ. Em caso de não conformidade com os valores estabelecidos, o BANPARÁ deve repetir o teste, em conjunto com AS CONTRATADAS, como forma de garantir a transparência do processo;

12.2.2. Os valores necessários para o cálculo de taxa de erro e taxa de perda de pacotes são acumulados automaticamente pelos roteadores CPE e devem ser consultados a cada 5 (cinco) minutos e armazenados para efetuar o cálculo. O mesmo ocorre com os valores referentes a uso de processador e memória dos roteadores CPE.

12.2.3. Deve-se sempre calcular as métricas de cada um dos enlaces separadamente.

13. REQUISITOS DE HABILITAÇÃO

13.1. ATESTADO DE CAPACIDADE TÉCNICA:

13.1.1. As LICITANTES deverão apresentar atestado de capacidade técnica expedido por pessoa jurídica de direito público ou privado que certifiquem a qualidade técnico-operacional do serviço similar em pontos e tecnologia aplicada aos do objeto desta licitação, prestados à declarante pelas LICITANTES.

13.2. DOCUMENTOS TÉCNICOS

13.2.1. As LICITANTES deverão apresentar os seguintes documentos técnicos:

13.2.1.1. Termo de Autorização de SCM – Serviço de Comunicação Multimídia expedido pela ANATEL. A não apresentação desta licença se caracteriza como um item de desclassificação.

13.2.1.2. Declaração, emitida pela própria EMPRESA, de que possui pelo menos 1 (um) centro de roteamento no Brasil;

13.2.1.3. Outorga, emitida pela ANATEL em nome das LICITANTES, de SCM ainda em validade, atestando que é empresa licenciada para comercializar serviços de redes de transporte de dados, pelo menos no Estado do Pará;

13.2.1.4. Declaração, emitida pelo fornecedor de segmento espacial, de que o(s) satélite(s) utilizado(s) tem vida útil, no mínimo, igual ao prazo de contratação;

13.2.1.5. Termo de Direito de Exploração ainda em validade em nome da LICITANTE ou de empresa subcontratada fornecedora de segmento espacial;

13.2.1.6. Atestado, emitida por pessoa jurídica de direito público ou privado, com a sua respectiva ART, expedida pelo CREA, atestando a qualidade técnico-operacional dos serviços prestados pelas LICITANTES, compatíveis em porte e tecnologia aos do objeto desta licitação;

13.2.1.7. Declaração, emitida pelas LICITANTES, de atendimento integral das exigências deste edital, ao qual dará pleno conhecimento. Não

serão admitidas quaisquer alegações posteriores de desconhecimento das características e condições especiais que possam dificultar ou a impedir a execução dos trabalhos.

13.2.1.8. Declaração das LICITANTES de que atenderá às exigências mínimas relativas à implantação das instalações, equipamentos e pessoal técnico essencial para o cumprimento do objeto da licitação.

13.2.2. As LICITANTES assumem todos os custos de preparação e apresentação de suas propostas e a CONTRATANTE não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

13.2.3. Todas as documentações de Qualificação Técnica exigidas neste Termo de Referência deverão ser apresentadas em original ou cópia autenticada em cartório. No caso de opção pela apresentação da documentação em cópia autenticada em cartório, toda documentação (sem exceção) deve ser devidamente autenticada. A apresentação da documentação (em parte ou na totalidade) em cópia simples incidirá na imediata desclassificação das LICITANTES.

13.3. QUALIFICAÇÃO ECONÔMICO FINANCEIRA:

13.3.1. Na habilitação econômico-financeira, as LICITANTES deverão apresentar os seguintes documentos:

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

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

13.3.1.3. Para Sociedades Anônimas, cópia autenticada da publicação do balanço em diário oficial ou jornal de grande circulação da sede da empresa Licitante;

13.3.1.4. 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;

13.3.1.5. 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 2003/2021 da RFB e alterações, apresentarão documentos extraído do Sistema Público de Escrituração Digital – SPED na seguinte forma:

13.3.1.6. 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;

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

13.3.1.8. Balanço e Demonstração do Resultado do Exercício extraídos do Sistema Público de Escrituração Digital – SPED.

13.3.1.9. Índices de Liquidez Corrente (LC), de Liquidez Geral (LG) e de Solvência Geral (SG) superiores a 1 (um).

13.3.1.9.1. 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:

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

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

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

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

13.3.2. 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.

13.3.3. 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.

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

13.4. VISITA TÉCNICA:

13.4.1. As LICITANTES poderão realizar vistoria no site central do BANPARÁ para obter a declaração de vistoria. A visita será realizada até 05 (cinco) dias úteis antes da data de abertura prevista no Edital e será assinada conjuntamente com o representante do CONTRATANTE.

13.4.2. A DECLARAÇÃO DE VISTORIA, constante no ADENDO IX, será fornecida pela SUPRO/GETEL, após a realização da vistoria, as quais devem ser agendadas previamente junto à área, pelos telefones (91) 3348-3027/3348-3049, de 2ª a 6ª feira, no horário das 14:00 às 18:00 horas, nos endereços: Rua Municipalidade, 1036, Umarizal e Av. Presidente Vargas, 251, Campina, ambos localizados no município de Belém/PA.

13.4.3. As LICITANTES que não realizarem vistoria deverão preencher e entregar o ADENDO X – DECLARAÇÃO DE ATENDIMENTO ÀS EXIGÊNCIAS MÍNIMAS.

13.4.4. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento dos serviços a serem executados e das características e condições especiais, que venham a dificultar ou a impedir a execução dos trabalhos.

14. DAS AMOSTRAS OU PROVA DE CONCEITO:

Na presente contratação não serão utilizadas amostras nem serão realizadas provas de conceito.

15. DA ADJUDICAÇÃO DO OBJETO

A adjudicação do objeto desta contratação será por lote.

15.1. DA JUSTIFICATIVA PELA FORMA DE ADJUDICAÇÃO:

A adjudicação do objeto será por LOTE, não sendo possível realizar a adjudicação por item devido à natureza interdependente dos itens.

16. DAS CONDIÇÕES DE CONTRATAÇÃO

16.1 As LICITANTES deverão possuir e comprovar que em seu quadro de técnicosou de seus prestadores de serviço existem profissionais com os seguintes conhecimentos:

16.1.1. Experiência mínima de 5 anos em suporte em redes de dados comprovados através de atestado, exigência que se faz necessária para evitar a participação na instalação e manutenção de equipamentos de alta complexidade tecnológica por pessoas leigas, buscando a atuação de profissionais com competência na área de Redes de Dados.

16.1.2. Conhecimento em comunicação satélite e MPLS, comprovados através de atestado de capacitação técnica ou certificação em produto que contenha esta funcionalidade.

16.1.3. Conhecimento em Gestão de Equipes de Suporte e Metodologias de Atendimento de Help Desk, comprovados através de certificação ITIL V3.

16.2. As CONTRATADAS deverão também ter pelo menos um funcionário ou um de seus prestadores de serviço que atenda os seguintes requisitos:

16.2.1. Formação de nível superior na área de Engenharia, Ciências da Computação, Tecnólogo em Processamento de Dados, Administração ou outro curso superior com extensão na área de informática, com carga horária

mínima de 360 horas, comprovada mediante diploma e/ou certificado fornecido por instituição reconhecida pelo Ministério da Educação.

16.3. A empresa que for contratada para fornecer o serviço referente ao LOTE-II, ou seu fornecedor, deverá apresentar:

16.3.1. Declaração de que possui estação de satélite TERRENA no território brasileiro, atendida por circuito satélite dedicado em Banda Ku, citando o seu endereço e apresentando documento que comprove a propriedade ou a locação do referido imóvel (IPTU).

16.4. Tais declarações anteriormente citadas são necessárias uma vez que, devido às características logísticas do Estado do Pará, algumas unidades do Banpará provavelmente serão atendidas inicialmente apenas por links de tecnologia de transmissão via satélite.

17. DA GARANTIA

17.1 DA GARANTIA CONTRATUAL:

17.1.1. As CONTRATADAS devem apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do BANPARÁ, contado da assinatura do instrumento de contrato ou documento equivalente, comprovante de prestação de garantia, podendo optar por caução em dinheiro, seguro-garantia ou fiança bancária.

17.1.2. A garantia, qualquer que seja a modalidade escolhida, deve assegurar o pagamento de prejuízos advindos do não cumprimento do objeto do contrato e multas moratórias e compensatórias aplicadas pelo BANPARÁ à contratada;

17.1.3. A garantia deve assegurar o cumprimento pelas CONTRATADAS de obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pelas CONTRATADAS.

17.1.4. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa a ser definida em edital e/ou contrato;

17.1.5. O atraso superior a 25 (vinte e cinco) dias na apresentação da garantia autoriza o BANPARÁ a:

17.1.5.1. Promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações, aplicando, se for o caso, a hipótese de

dispensa de licitação prevista no inciso VI do Artigo 29 da Lei n. 13.303/2016; ou

17.1.5.2. Reter o valor da garantia dos pagamentos eventualmente devidos ao contratado até que a garantia seja apresentada.

17.1.6. O BANPARÁ executará a garantia na forma prevista na legislação que rege a matéria.

17.2 DA GARANTIA DO OBJETO:

17.2.1. As CONTRATADAS deverão prestar a garantia técnica dos serviços e equipamentos entregues a contar da data do recebimento definitivo até o fim da vigência contratual.

17.2.2. As CONTRATADAS deverão entregar e manter os serviços com alto nível de qualidade, uma vez que ela própria será responsável por corrigir todas as falhas em seus serviços e equipamentos enquanto perdurar sua relação contratual com a área requisitante, fornecendo total garantia técnica à solução.

18. DOS PRAZOS

18.1 Em até 15 (QUINZE) dias corridos após a assinatura do contrato, para efeito de Homologação da Solução, as CONTRATADAS devem apresentar: o projeto de implantação dos serviços contratados, contendo as ações e respectivos prazos; a lista com o(s) número(s) de telefone(s) e endereços eletrônicos definidos, assim como a lista inicial dos técnicos, seus ou de subcontratados, aptos a efetuar atendimentos locais;

18.2 Até 75 (SETENTA E CINCO) dias corridos contados a partir da data da assinatura do contrato para a instalação da solução, no caso de enlaces com tecnologia satélite;

18.3 Até 60 (SESSENTA) dias corridos contados a partir da data da assinatura do contrato para a instalação da solução, no caso de enlaces com tecnologia terrestre;

18.4 Até 75 (SETENTA E CINCO) dias corridos após solicitação formal para a ativação de um novo enlace, no caso de enlaces com tecnologia satélite, mediante resposta positiva do estudo de viabilidade técnica das CONTRATADAS;

18.5 Até 60 (SESSENTA) dias corridos após solicitação formal para a ativação de um novo enlace, no caso de enlaces com tecnologia terrestre,

mediante resposta positiva do estudo de viabilidade técnica das CONTRATADAS;

18.6 Até 30 (TRINTA) dias corridos após solicitação formal para a alteração de velocidade, no caso de enlaces com tecnologia satélite, mediante resposta positiva do estudo de viabilidade técnica das CONTRATADAS;

18.7 Até 30 (TRINTA) dias corridos após solicitação formal para a alteração de velocidade, no caso de enlaces com tecnologia terrestre, medianteresposta positiva do estudo de viabilidade técnica das CONTRATADAS;

18.8 Até 3 (TRÊS) dias úteis após notificação formal caso um serviço/equipamento tenha sido executado/entregue com defeito ou fora das especificações para que seja realizada a correção/substituição do mesmo;

18.9 Até 3 (TRÊS) dias úteis após notificação formal para substituição de equipamento que apresente 3 (três) ou mais falhas semelhantes em um período de até 3 (três) meses;

18.10 Em até 2 (DOIS) dias úteis após o encerramento de um chamado técnico para a disponibilização de relatório detalhando quaisquer problemas ocorrido na solução e sua respectiva solução;

18.11 Em até 1 (UMA) hora após a ocorrência de falha em um dos concentradores instalados nos Data centers do BANPARÁ, ou seja, caso aconteça um sinistro em um Data center, as CONTRATADAS deverão fazer o remanejamento do trafego para o outro Data center em até uma hora. Entretanto, o chaveamento deverá se dar de forma automática para o concentrador backup.

18.12 Observações:

18.12.1 Dentre as atividades iniciais, citamos a instalação física do hardware fornecido e a configuração dos roteadores fornecidos (SNMP, VPN,syslog e outros);

18.12.2 Cada enlace MPLS deve ser homologado separadamente em até 24 horas corridas após a entrega por parte das CONTRATADAS;

18.12.3 O enlace MPLS será considerado homologado se estiver configurado de acordo com as especificações técnicas;

18.12.4 Quando houver necessidade de remanejar enlaces MPLS de um Data center para outro, deve ser dado prioridade para os enlaces com maior largura de banda.

19. DA ENTREGA

19.1 A entrega da solução deverá ocorrer conforme prazos descritos no Item 17 deste Termo de Referência, dentro do horário comercial.

19.2 O local das instalações fica definido conforme ADENDOS I e II.

19.3 No caso dos links de parceiros constantes do LOTE I, o endereço será definido junto à CONTRATADA após a realização da licitação.

19.4 No caso de novas unidades que venham a ser criadas no futuro, o Banpará definirá seu endereço e o informará à contratada.

20. DO RECEBIMENTO DO OBJETO

O prazo de recebimento para cada um dos lotes será de 120 dias a contar da assinatura dos respectivos contratos, conforme cronograma definido entre o BANPARÁ e as CONTRATADAS.

21. DA VIGÊNCIA DO(S) CONTRATO(S) DECORRENTE(S) DO PROCESSO LICITATÓRIO

21.1 Os contratos vinculados a este termo de referência terão vigência de 12(doze) meses, podendo ser prorrogados até o limite previsto no art. 71 da Lei n. 13.303/2016.

21.2 Em caso de prorrogação do prazo de vigência, os valores contratados serão repactuados conforme o IPCA (Índice Nacional de Preços ao ConsumidorAmplo) acumulado dos 12 meses anteriores ao mês da assinatura do aditivo contratual.

22 OBRIGAÇÕES DAS PARTES

22.1 OBRIGAÇÕES DO CONTRATANTE

22.1.1 Adicionalmente às responsabilidades estabelecidas nos demais tópicos constantes deste Termo de Referência, incumbe ao CONTRATANTE observar os seguintes requisitos:

22.1.1.1 Cumprir os prazos e obrigações financeiras estabelecidas no Edital, desde que cumpridas todas as formalidades e exigências por parte da CONTRATADA.

22.1.1.2 Convocar a CONTRATADA a participar das reuniões.

22.1.1.3 Designar gestor que efetuará sua representação perante a CONTRATADA para determinação, avaliação, acompanhamento e aprovação dos serviços por ela realizados.

22.1.1.4 Colocar à disposição da CONTRATADA, os equipamentos mínimos e documentação necessários para a realização das atividades, quando estas forem executadas nas instalações do CONTRATANTE.

22.1.1.5 Prestar os esclarecimentos que venham a ser solicitados pela CONTRATADA, no que diz respeito ao contrato.

22.1.1.6 Comunicar oficialmente à CONTRATADA quaisquer falhas verificadas no cumprimento do contrato.

22.1.1.7 Apresentar à CONTRATADA processos de trabalho, políticas e normas internas necessários para a adequada execução do objeto da contratação.

22.1.1.8 Acompanhar as atividades de implantação, de forma a reter informações críticas para a continuidade do sistema implantado.

22.1.1.9 Gerenciar e fiscalizar a execução do contrato, de forma a garantir o fiel cumprimento de suas cláusulas.

22.1.1.10 Fornecer a infraestrutura necessária de TI e o sob sua responsabilidade para a adequada execução do contrato.

22.1.1.11 Recusar recebimento de qualquer bem ou serviço que estiver em desacordo com as condições e as especificações estabelecidas no contrato, chamado técnico e na OS de solicitação.

22.1.1.12 Emitir termos circunstanciados de recebimento provisório, de recebimento parcial, de recebimento definitivo ou de recusa de serviços relacionados ao objeto contratado.

22.1.1.13 Aplicar à CONTRATADA, se necessário, as sanções administrativas e contratuais cabíveis, garantida ampla defesa e contraditório.

22.1.1.14 Manter o histórico de gerenciamento do contrato nos autos do processo de fiscalização, contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato, por ordem cronológica.

22.1.1.15 Liberar as garantias prestadas pela CONTRATADA nos tempos contratualmente previstos.

22.1.1.16 Exercer o acompanhamento, gestão e fiscalização do contrato, anotando em registro próprio as ocorrências detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, encaminhando os apontamentos à autoridade competente para as providências cabíveis.

22.1.1.17 Comunicar as CONTRATADAS por escrito de eventuais ocorrências, imperfeições, falhas e/ou irregularidades detectadas no curso da execução do contrato, fazendo constar na comunicação, expressamente, as medidas e prazos máximos para as correções e regularizações.

22.1.1.18 Pagar às CONTRATADAS o valor resultante da execução do contrato, conforme prazos contratados.

22.1.1.19 Efetuar as retenções tributárias devidas sobre o valor da fatura das CONTRATADAS, em conformidade com as normas fiscais pertinentes.

22.2 OBRIGAÇÕES DA CONTRATADA

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

22.2.2 Cumprir os prazos e obrigações estabelecidas no Edital.

22.2.3 Nomear coordenador do contrato para representá-la durante o período de vigência contratual.

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

22.2.5 Observar as normas e procedimentos internos do CONTRATANTE no que se refere à segurança (Política de Segurança) e sigilo dos dados manuseados, bem como no que é pertinente à documentação, sobre os quais se obriga a dar ciência a seus funcionários que tiverem acesso às dependências do CONTRATANTE, e aos que possuírem acesso remoto, caso haja necessidade.

22.2.6 Observar todas as normas e procedimentos internos do CONTRATANTE, os quais poderão ser atualizados a qualquer momento pelo CONTRATANTE.

22.2.7 Colocar nos prazos contratados os profissionais à disposição do CONTRATANTE para execução dos serviços.

22.2.8 Disponibilizar ao contratante e manter atualizada a relação nominal dos profissionais que atuarão no projeto em contato direto com o CONTRATANTE, incluindo CPF, perfil profissional, papel no projeto, acompanhada dos respectivos comprovantes de qualificação técnica.

22.2.9 Manter os profissionais devidamente identificados por meio de crachá, quando em trabalho nas dependências do CONTRATANTE.

22.2.10 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.

22.2.11 Cuidar para que o Coordenador do Contrato mantenha permanente contato com a unidade responsável pela fiscalização do contrato, adotando as providências requeridas à execução dos serviços pelos profissionais, e comande, coordene e controle a execução dos serviços contratados.

22.2.12 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.

22.2.13 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 seus empregados não manterão qualquer vínculo empregatício com o CONTRATANTE.

22.2.14 Assumir a responsabilidade, sem qualquer espécie de solidariedade por parte do CONTRATANTE, por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus profissionais durante a execução deste contrato, ainda que acontecido em dependência do CONTRATANTE.

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

22.2.16 Planejar, desenvolver, implantar, executar e manter os serviços de acordo com os níveis de serviço estabelecidos no contrato.

22.2.17 Responsabilizar-se por eventuais prejuízos provocados por ineficiência, negligência, erros ou irregularidades cometidas na execução dos serviços objeto deste contrato, bem como, nas instalações e demais bens de propriedade do CONTRATANTE.

22.2.18 Reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados nos quais se verificar vícios, defeitos ou incorreções.

22.2.19 É vedada a subcontratação para a execução dos serviços objeto desta contratação.

22.2.20 É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização do CONTRATANTE.

22.2.21 Observar os prazos apresentados no cronograma de execução do serviço, bem como o prazo de entrega deste.

22.2.22 Dar ciência ao CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade verificada na execução dos serviços.

22.2.23 Fornecer ao CONTRATANTE, no ato da homologação dos serviços, os Manuais de Usuário, Técnico e Operacional (Produção), contendo os seguintes documentos: diagrama entidade-relacionamento, dicionário de dados, diagrama de classes, diagrama de componentes, diagrama de atividades, diagrama de sequência, diagrama de casos de uso, descrição dos casos de uso, procedimentos para instalação, diagrama de implantação, interfaces utilizadas de outros sistemas, interfaces disponibilizadas para outros sistemas. A lista de documentos apresentada neste item diz respeito à visão macro do que é desejável receber pelo CONTRATANTE durante a execução de um projeto, porém pode variar, isto é, não ser necessária em sua totalidade, sendo que tal situação será definida no escopo de cada projeto, de acordo com a complexidade envolvida.

22.2.24 A homologação da solução será vinculada à entrega dos Manuais Técnicos escritos na Língua Portuguesa.

22.2.25 Manter sempre atualizados os manuais técnicos, de usuário e de produção, quando o sistema, objeto deste contrato, sofrer alguma alteração.

22.2.26 Manter durante o curso do contrato e após o seu término, o mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às atividades do CONTRATANTE, das quais venha a ter conhecimento ou às quais venha a ter acesso por força do cumprimento do contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento da obrigação assumida por eventuais perdas e danos e sujeitando-se às cominações legais, nos

termos da Lei 4.595 de 31/12/1964 e demais leis, permitindo, ainda, que o CONTRATANTE, a qualquer tempo, fiscalize o seu uso.

22.2.27 Colaborar com o CONTRATANTE no desenvolvimento de qualquer procedimento de auditoria que este decida realizar na área de tecnologia, permitindo que auditores, sejam eles internos ou externos, a área de segurança de TI ou outros prepostos designados pelo CONTRATANTE tenham amplo acesso a dados, informações, equipamentos, instalações, profissionais e documentos que julguem necessários à conclusão de seu trabalho.

22.2.28 Colaborar com o CONTRATANTE, quando solicitado, com informações de sua responsabilidade, necessárias para a execução de tarefas vinculadas a projetos em cujas características relacionadas à integração entre sistemas exijam conhecimento de mais de uma empresa prestadora de serviços de TI;

22.2.29 Caso seja detectado qualquer problema na homologação do objeto do contrato, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções, sem qualquer ônus para o CONTRATANTE.

22.2.30 A homologação da solução e emissão do Termo de Recebimento Definitivo da Ordem de Serviço ocorrerá após a conclusão e aceitação de todos os testes do serviço pelo CONTRATANTE.

22.2.31 Responsabilizar-se, dentro dos limites do vínculo empregatício, pelos empregados que colocar à disposição do CONTRATANTE, observadas as legislações trabalhistas e a Lei Previdenciária Social.

22.2.32 Não ceder ou dar em garantia, a qualquer título, no todo ou em parte, os créditos de qualquer natureza, decorrentes ou oriundos deste contrato, salvo com autorização prévia e por escrito do CONTRATANTE.

22.2.33 Manter a guarda dos equipamentos e demais bens de propriedade do CONTRATANTE, quando utilizados, permitindo que este, a qualquer tempo, fiscalize o seu uso.

22.2.34 Garantir a segurança e qualidade do software em suas características operacionais, de manutenção e adaptabilidade a novos ambientes e assegurar que o software produzido seja eficiente quanto ao desempenho e consumo de hardware.

22.2.35 Fornecer treinamento, conforme estabelecido neste Termo de Referência.

22.2.36 Informar ao CONTRATANTE, no ato da apresentação da proposta ou em um prazo não superior a 24 horas, contadas a partir de quando o CONTRATANTE solicitar que sejam executadas nas suas instalações, os equipamentos mínimos e documentação necessários para a realização das atividades, inclusive para execução de testes integrados e/ou homologação.

22.2.37 Providenciar as próprias licenças de software necessárias para execução dos serviços, tais como licenças de ferramentas de desenvolvimento e outras. O CONTRATANTE poderá solicitar comprovação dos registros de licenciamento.

22.2.38 Atualizar as versões de documentos, de códigos-fontes e demais artefatos produzidos a cada alteração nos sistemas objeto deste termo de referência, fazendo uso da ferramenta de controle de versão disponibilizada pelo CONTRATANTE.

22.2.39 Providenciar, às suas custas, link de comunicação para acesso aos recursos computacionais necessários à execução dos serviços contratados, quando não fornecido pelo CONTRATANTE.

22.2.40 Manter em suas dependências e às suas custas, ambiente computacional adequado à execução dos serviços contratados;

22.2.41 Executar os serviços objeto da presente contratação, observando as melhores práticas preconizadas pela ITIL (Information Technology Infrastructure Library) e os requisitos estabelecidos para gestão do ciclo de vida da Solução.

22.2.42 Assegurar a transferência de todas as obrigações contratuais ao sucessor, em caso de venda, fusão, cisão, incorporação por novos controladores ou associação da contratada com outrem.

22.2.43 Substituir, sempre que solicitado pelo CONTRATANTE, profissional cuja atuação, permanência e/ou comportamento sejam considerados prejudiciais, inconvenientes, insatisfatórios às normas de disciplina do CONTRATANTE ou ao interesse do serviço público, haja vista o CONTRATANTE estar indiretamente ligado ao Estado; ou ainda, incompatíveis com o exercício das funções que lhe foram atribuídas.

22.2.44 Adotar as providências necessárias para exclusão do CONTRATANTE da lide na hipótese de haver ação judicial envolvendo terceiros, cujo objeto

refira-se a serviço prestado ou bem fornecido ao CONTRATANTE. Não obtendo êxito na exclusão, e, se houver condenação, reembolsar ao CONTRATANTE, no prazo de dez dias úteis, a contar da data do efetivo pagamento, as importâncias que tenha sido o CONTRATANTE obrigado a pagar.

22.2.45 Permitir o acompanhamento, pelo CONTRATANTE, de todas as atividades realizadas no escopo do serviço de implantação, de forma a absorver informações críticas de negócio e possibilitar a condução, de forma emergencial, dos serviços de sustentação da Solução.

22.2.46 É vedada a contratação, pela CONTRATADA, para atuar no âmbito do presente contrato, de empregado ativo no quadro do contratante.

22.2.47 Observar e adequar o sistema objeto deste documento às evoluções tecnológicas realizadas pelo CONTRATANTE nos sistemas operativos que abrigam as soluções, sem ônus algum ao CONTRATANTE.

22.2.48 Fornecer serviços de gerência pró-ativa da Rede de enlaces de dados, de forma a detectar e/ou corrigir, no menor tempo possível, qualquer anormalidade que venha a ocorrer nos enlaces ou nos equipamentos fornecidos, diminuindo a necessidade de que o BANPARÁ entre em contato para comunicar uma anormalidade.

22.2.49 No caso de uma anormalidade que não possa ser corrigida de imediato, o BANPARÁ deve ser avisado sobre a mesma, no máximo em 30 (trinta) minutos, através de um dos telefones divulgados no ato da assinatura do contrato e de e-mail corporativo;

22.2.50 Os dados referentes ao monitoramento podem, a critério do CONTRATADA e sem custo adicional ao BANPARÁ, trafegar por enlaces dedicados ponto-a-ponto ou pelos próprios enlaces fornecidos. Neste último caso, os dados devem ser transmitidos através de VPNs com alta prioridade (QoS alto) e tráfego máximo de 3% (três por cento) da banda total do enlace ou 10 (dez) Kbps, o que for maior;

22.2.51 O serviço de gerência pró-ativa também deve monitorar e armazenar, por um período mínimo de 90 dias, informações relativas a tráfego (até o nível de protocolo de aplicação), latência de rede, perda de pacotes e taxa de erro.

22.2.52 Ativar os enlaces (e instalar todo o hardware necessário) que lhe for solicitado nos pontos definidos pelo BANPARÁ. Caberá ao BANPARÁ

apenas os custos de quaisquer obras necessárias (instalação elétrica, cabeamento de LAN, adequações de engenharia civil e outros);

22.2.53 Negociar com o BANPARÁ, com antecedência mínima de 5 (cinco) dias corridos, qualquer interrupção programada em algum de seus enlaces de dados. Caso as partes não cheguem a um consenso em relação a data/horário de paralisação, estará configurada paralisação não-programada;

22.2.54 Limitar sua atuação à interface de rede local (LAN) do(s) seu(s) roteador(es).

22.2.55 Disponibilizar obrigatoriamente telefone gratuito nacional para:

22.2.56 Abertura e acompanhamento de chamados técnicos;

22.2.57 Abertura e acompanhamento de solicitações de serviços.

22.2.58 Disponibilizar site web com autenticação por meio de usuário/senha e/ou certificado digital para:

22.2.59 Abertura reativa, acompanhamento e encerramento de chamados técnicos;

22.2.60 A exigência dessa ferramenta não exime as CONTRATADAS da responsabilidade de abrir chamados de forma proativa.

22.2.61 Abertura, acompanhamento e encerramento de solicitações de serviços;

22.2.62 Verificação de utilização dos enlaces, com exibição de gráficos diários, semanais, mensais e anuais, com amostragem mínima de 5 minutos;

22.2.63 Emissão de relatórios de disponibilidade diária, semanal e mensal dos enlaces;

22.2.64 Emissão de relatórios contendo informações sobre os chamados técnicos, solicitações de serviços e anormalidades ocorridas;

22.2.65 Emitir relatório mensal contendo taxa de utilização, percentual de disponibilidade, horários de início e término de falhas, ativações, desativações, remanejamentos e mudanças de configuração;

22.2.66 Verificação do estado geral dos enlaces.

22.2.67 Seguir rigorosamente, tanto em suas redações atuais quanto em qualquer redação futura, das quais se obriga a dar ciência a seus funcionários, prepostos e mandatários que, ora estiverem alocados nas dependências do BANPARÁ, ora possuírem acesso remoto:

22.2.68 Lei nº 13.709/2018 – Lei Geral de Proteção de Dados;

22.2.69 Termo de Confidencialidade, Zelo e Responsabilidade Sobre Informação do Banco do Estado do Pará (ADENDO IV)

22.2.70 Diretrizes Para Utilização de Desenvolvimento Seguro – ADENDO V;

22.2.71 Diretrizes Para Utilização de Nuvem – ADENDO VI;

22.2.72 Recomendações e Padrões de Segurança Tecnológica Mínima – ADENDO VII;

22.2.73 Requisitos de Segurança Para Controle De Acesso e Auditoria Nos Sistemas Corporativos – ADENDO VIII.

22.2.74 Retirar, sem quaisquer ônus ao BANPARÁ, os equipamentos que porventura forem disponibilizados, dos locais em que foram instalados, em até 30 (trinta) dias consecutivos, quando do término do contrato ou desativação do enlace ou equipamento. A não retirada desses equipamentos, no prazo estabelecido, desde que não tenha havido qualquer impedimento causado pelo BANPARÁ, isenta o mesmo de qualquer responsabilidade sobre estes e lhe confere o direito de dar-lhes a destinação que melhor lhe aprouver, independentemente de qualquer comunicação ao CONTRATADA.

22.2.75 Manter rigorosa observância das políticas institucionais e dos normativos internos e externos do Banco, principalmente quanto segurança da informação e continuidade de negócios.

22.2.76 Cumprir de modo integral os contratos firmados com o Banco, observando os normativos vigentes relacionados ao serviço contratado.

22.2.77 Cumprir com todas obrigações trabalhistas, apresentando à Contratante todas as certidões e/ou documentos comprovando que a empresa não permite a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal, 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 e 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.

22.2.78 Comunicar as ocorrências referentes a risco operacional (falha, inadequação ou deficiência) que ocasionou a interrupção do serviço contratado. As comunicações devem ser feitas por e-mail à GEROP – Gerência de Risco Operacional e Continuidade de Negócios (gerop@banparanet.com.br), com cópia à GETEL – Gerência de Telecomunicações (getel@banparanet.com.br) e à GEMON – Gerência de Monitoramento

(gemon@banparanet.com.br), ou a qualquer outro endereço eletrônico que a CONTRATANTE venha a especificar durante a vigência dos contratos, assim como aos responsáveis discriminados no plano de continuidade, mesmo que as situações de risco operacional tenham sido contornadas antes de causarem algum impacto negativo nas operações do Banpará.

22.2.79 Responsabilizar-se pelos prejuízos provocados diretamente ao Banco ou a terceiros, por culpa ou dolo, na execução dos serviços.

22.2.80 Responsabilizar-se por eventuais danos causados por ineficiência, negligência, erros ou irregularidades praticadas durante a prestação dos serviços.

22.2.81 Responsabilizar-se por eventuais danos socioambientais causados direta ou indiretamente a terceiros, por seus empregados ou administradores.

22.2.82 Manter confidencialidade quanto às informações mantidas nos equipamentos, documentos e/ou materiais manipulados por seus empregados, em conformidade com a Política Institucional de Segurança da Informação e com a Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

22.3 As CONTRATADAS devem desenvolver para a solução contratada, em conjunto com a CONTRATANTE, em até 180 dias após o início do contrato, um Plano de Continuidade de Negócios que deverá estar de acordo com o art. 20, inciso III e IV da Resolução Bacen nº 4.557/17, devendo conter no mínimo:

22.3.1 Objetivo e escopo;

22.3.2 Papéis e responsabilidades dos envolvidos na ativação e execução do plano de continuidade;

22.3.3 Condições para a ativação de planos;

22.3.4 Autoridade responsável;

22.3.5 Interdependências (internas e externas) e suas interações;

22.3.6 Procedimentos de implementação do plano de continuidade;

22.3.7 Controle de versão.

22.4 O plano de contingência deve contemplar os requisitos de segurança da informação definidos pelo Banpará e considerar:

22.4.1 Condições para ativação dos planos, os quais devem descrever os processos a serem seguidos e discriminar quem ou qual departamento

deverá acompanhar o acionamento do plano, preferencialmente que seja o gestor do contrato.

22.4.2 Procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio;

22.4.3 Procedimentos de recuperação que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infraestrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário, bem como discriminar os responsáveis que devem ser acionados para execução das transferências de atividades de negócio ou serviços de infraestrutura. Caso, o serviço seguir um modelo que não dependa da infraestrutura interna da CONTRATANTE, este requisito não se faz necessário;

22.4.4 Procedimentos operacionais temporários para seguir durante a conclusão de recuperação e restauração;

22.4.5 Procedimentos que descrevam as ações a serem adotadas quando do restabelecimento das operações;

22.4.6 Designação das responsabilidades individuais, informando o responsável pela execução dos itens do plano, além da designação de suplentesquando necessário;

22.5 As CONTRATADAS devem apresentar documentos (como certificados, planos de continuidade e relatórios de testes), sujeito à aprovação da área CONTRATANTE, que comprovem que realiza uma gestão de continuidade de negócios consistente, bem como apresentar evidências dos testes realizados (através de relatórios), no mínimo uma vez ao ano ou quando solicitado pela CONTRATANTE. Caso no momento da contratação as CONTRATADAS não tenham uma gestão de continuidade implantada corporativamente, deve ser dado a mesma um prazo de no máximo 180 dias para a implantação da mesma.

22.6 As CONTRATADAS devem se adequar continuamente aos padrões de normativos da CONTRATANTE, para assegurar que possíveis mudanças de regulamentações estejam perfeitamente em conformidade com os serviços e ações das CONTRATADAS.

22.7 As CONTRATADAS devem obrigatoriamente manter o controle de versionamento do sistema e sua documentação e deve disponibilizar acesso

ao Banpará a qualquer momento durante a vigência do contrato. Caso as CONTRATADAS não mantenha o controle de versão a mesma será responsabilizada por prejuízos causados ao Banco decorrentes de versão de aplicação ou documentação falhas que não podem ser retornadas a versão anterior estável.

22.8 As CONTRATADAS deverão realizar a transferência de tecnologia e de técnicas empregadas, com intuito de capacitar o corpo técnico da área tecnológica do Banco que serão responsáveis pela manutenção dos sistemas, contemplando todos os dados, documentação e conhecimento pertinentes à operação, à sustentação e à manutenção da solução.

22.9 As CONTRATADAS deverão apresentar Anotação de Responsabilidade Técnica expedida pelo CREA de qualquer unidade da federação, que dispõe de circuitos exclusivos com o exterior, de no mínimo 5 (cinco) Gbps (Gigabits por segundo), correspondendo a somatória de banda de todos os circuitos. Essa saída deve ser composta por uma ou mais conexões ponto-a-ponto entre o backbone IP do provedor e do sistema autônomo (AS-Autonomous System) remoto, sem backbones intermediários;

22.10 As CONTRATADAS deverão comprovar através de Anotação de Responsabilidade Técnica expedida pelo CREA de qualquer unidade da federação, que pode se conectar com, no mínimo, 4 (quatro) AS/provedores diferentes dos Estados Unidos da América (EUA), da Europa ou da África;

22.11 As CONTRATADAS deverão comprovar através de Anotação de Responsabilidade Técnica expedida pelo CREA de qualquer unidade da federação, que o seu backbone IP possui saída com destino a outros provedores de backbone IP Nacionais, com banda mínima de 5 (cinco) Gbps;

22.12 As CONTRATADAS deverão comprovar através de Anotação de Responsabilidade Técnica expedida pelo CREA de qualquer unidade da federação, que o backbone IP do provedor deve ser capaz de prover trânsito nacional e internacional para o SISTEMA AUTÔNOMO (AS), com suporte ao protocolo BGP-4;

23 DAS SANÇÕES ADMINISTRATIVAS

23.1 Pela inexecução total ou parcial do contrato a CONTRATANTE poderá, garantida a prévia defesa, aplicar às CONTRATADAS as seguintes sanções:

23.1.1 Advertência;

23.1.2 Multa, na forma prevista no instrumento convocatório ou no contrato;

23.1.3 Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

23.2 As sanções administrativas devem ser aplicadas diante dos seguintes comportamentos das CONTRATADAS e contratados:

23.2.1 Dar causa à inexecução parcial ou total do contrato;

23.2.2 Deixar de entregar a documentação exigida para o certame, salvo na hipótese de inversão de fases prevista;

23.2.3 Não manter a proposta, salvo se em decorrência de fato superveniente, devidamente justificado;

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

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

23.2.6 Apresentar documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

23.2.7 Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

23.2.8 Comportar-se com má-fé ou cometer fraude fiscal;

23.2.9 Praticar atos ilícitos visando a frustrar os objetivos da licitação.

23.3 Sem prejuízo de outras sanções previstas no instrumento convocatório ou no contrato, as CONTRATADAS sujeitam-se à aplicação das seguintes multas:

23.3.1 Igual ao valor do prejuízo financeiro comprovado de forma direta (indisponibilidade de informações dentro de um determinado prazo legal ou perda de negócios, por exemplo) e/ou estimado de forma indireta (imagem da instituição, por exemplo). A presente multa é a título de cláusula penal, razão pela qual não prejudica a aplicação das demais multas previstas.

23.3.2 De 10% (dez por cento) do valor global do contrato, independentemente de qualquer outra providência de ordem legal, nos casos de rescisão por culpa das CONTRATADAS, o que caracteriza a inexecução da obrigação assumida.

23.3.3 De 1% (um por cento) do valor da fatura/nota fiscal do mês anterior para cada dia ou fração de dia, limitado a 30 (trinta) dias, em que houver

descumprimento de qualquer das exigências estabelecidas neste edital, salvo os casos anteriores, para os quais já existem penalidades especificadas.

24. DO PAGAMENTO

24.1 O pagamento de cada enlace iniciará somente após o ateste técnico do funcionamento do referido enlace realizado pela SUPRO/GETEL.

24.2 O pagamento às CONTRATADAS será realizado mediante validação da respectiva fatura/nota fiscal pela Comissão de fiscalização, respeitando-se o prazo previsto no item seguinte.

24.3 O objeto de cobrança terá que ter sido previamente validado e/ou conferido. Assim, para que o respectivo pagamento se efetive, deverá a Nota Fiscal/Fatura ser apresentada ao BANPARÁ com antecedência mínima de 15 (quinze) dias do vencimento, ficando este isento de responsabilidade por atrasos na apresentação das faturas por parte das CONTRATADAS.

24.4 Nenhum pagamento será efetivado sem que a Comissão de fiscalização ateste que o objeto contratado está integralmente sendo entregue/disponibilizado e/ou cumprido pelas CONTRATADAS.

24.5 A realização de qualquer pagamento pelo Banco fica condicionada a apresentação dos seguintes documentos atualizados, caso os anteriormente apresentados estejam vencidos: CND emitida pelo INSS; Certidão de Regularidade da Receita Federal e da PGFN; CND do FGTS expedida pela CEF; prova de regularidade para com as fazendas Estadual e Municipal do domicílio da sede das CONTRATADAS.

24.6 A devolução da Nota fiscal/Fatura não servirá de pretexto ao descumprimentode quaisquer das obrigações das CONTRATADAS.

24.7 Havendo necessidade de realização de serviços por profissionais disponibilizados pelas CONTRATADAS, quaisquer despesas necessárias (como passagens, deslocamentos, estadias, refeições e outros), serão arcadas pelas CONTRATADAS.

24.8 Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

24.9 Sem prejuízo ao pagamento das glosas estipuladas no contrato, o BANPARÁ poderá suspender quaisquer pagamentos devidos à CONTRATADA, sem incorrer em ônus adicionais, sempre que Comissão de fiscalização constatar a ocorrência de atrasos, inconsistências no faturamento e/ou descumprimentos na execução do objeto contratado, retomando-os tão logo tais atrasos sejam completamente eliminados, nos termos de parecer desta Comissão.

24.10 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário e órgãos administrativos, atribuídos ao BANPARÁ, oriunda de problemas na execução do contrato por parte das CONTRATADAS, serão repassadas a estas e deduzidas do pagamento realizado pelo BANPARÁ.

24.11 No preço apresentado pelas CONTRATADAS já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do BANPARÁ, por eventuais autuações.

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

24.13 No caso de atraso no pagamento das faturas ou outros documentos de cobrança emitidos pelas CONTRATADAS, sem que haja culpa da mesma, 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 seguintes ao do vencimento até a data da efetiva liquidação do débito.

25 FISCALIZAÇÃO DO CONTRATO

25.1 A gestão e fiscalização dos requisitos técnicos a serem medidos ficará a cargoda SUPRO/GETEL e dar-se-á mediante o tempo máximo de atendimento de cada unidade do Banco interligada pela rede contratada. As listagens dos tempos de atendimento por unidade constam nos ADENDOS I e II deste Termo de Referência.

25.2 A medição da disponibilidade informada no item 10 – NÍVEIS MÍNIMOS DE SERVIÇO será efetuada através do portal de gerenciamento que cada CONTRATADA disponibilizará ao Banco. A equipe técnica da SUPRO/GETEL será responsável pela homologação da entrega de cada circuito mediante teste de continuidade. Em caso do não atingimento do referido índice de disponibilidade, apurado pela equipe técnica da SUPRO/GETEL, ocorrerá a glosa dos valores dos circuitos afetados, conforme Item 10 deste Termo de Referência.

25.3 FISCALIZAÇÃO TÉCNICA

25.3.1 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 serviço contratado.

25.3.2 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.

25.3.3 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.

25.3.4 O BANPARÁ, através de funcionário ou comissão, doravante designado como FISCALIZAÇÃO, efetuará a fiscalização e o acompanhamento da execução do objeto contratado, podendo a qualquer tempo exigir às empresas CONTRATADAS que forneçam os elementos necessários ao esclarecimento de dúvidas relativas ao fornecimento, tais como demonstrativos de custos, notas fiscais, relatórios, etc.

25.3.5 Os bens e/ou serviços fornecidos, bem como o material utilizado na sua execução, estarão sujeitos à aceitação da FISCALIZAÇÃO, a quem caberá direito de recusa caso os mesmos não sejam executados de acordo com as especificações constantes do Termo de Referência, ou caso se constate, nos mesmo, existências de vícios ou defeitos.

25.3.6 O aceite dos serviços será formalizado pela FISCALIZAÇÃO através do aceite ou atesto na respectiva nota fiscal. Não obstante o Aceite/Atesto, as CONTRATADAS serão responsáveis pela perfeita execução do objeto contratado, nos termos da legislação civil, penal e profissional, pelo que a fiscalização da execução dos serviços não diminui ou substitui a responsabilidade da empresa, decorrente das obrigações pactuadas.

25.3.7 Quaisquer tolerâncias, concessões ou liberalidades da FISCALIZAÇÃO para com as CONTRATADAS, quando não formalizadas mediante termo aditivo, não constituirão precedentes invocáveis e não terão o poder de alterar as obrigações estabelecidas.

25.3.8 A fiscalização técnica dos contratos deve avaliar constantemente a execução do seu objeto e sua qualidade, verificando, dentre outros aspectos, o cumprimento dos seus resultados e cronograma, a utilização dos materiais, técnicas e recursos humanos exigidos para a execução dos contratos, devendo determinar a correção de falhas ou faltas por parte das CONTRATADAS, bem como informar ao gestor do contrato sobre providências, que importem disposição sobre o contrato, com as respectivas justificativas.

25.3.9 A fiscalização técnica do contrato será exercida pela Superintendência de Produção – Gerência de Telecomunicações (SUPRO/GETEL), a quem incumbirá acompanhar a execução do fornecimento do serviço, determinando às CONTRATADAS as providências necessárias ao regular cumprimento das obrigações pactuadas.

25.4 FISCALIZAÇÃO ADMINISTRATIVA

25.4.1 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 Termo de Referência, 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.

25.4.2 A fiscalização administrativa do contrato será exercida pela Superintendência de Produção – Gerência de Telecomunicações (SUPRO/GETEL), a quem incumbirá acompanhar os pagamentos, prazos, obrigações e encerramento do mesmo.

25.4.3 As CONTRATADAS deverão possuir o seguinte ator agindo para a execução contratual:

25.4.4 Preposto – Funcionário representante das CONTRATADAS, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativasreferentes ao andamento contratual.

26 DISPOSIÇÕES GERAIS

26.1 Não obstante as CONTRATADAS sejam as únicas e exclusivas responsáveis pela execução do objeto contratado, o BANPARÁ reserva-se o direito de exercer a mais ampla e completa fiscalização dos serviços contratados.

26.2 Havendo mudança de endereço dos data centers, as CONTRATADAS deverão executar a mudança dos acessos de dados para os novos endereços a serem definidos pela CONTRATANTE.

26.3 Deverá constar no contrato a permissão de acesso do Banco Central do Brasil a termos firmados, documentação e informações referentes aos serviços prestados e a dependência do contratado.

26.4 As partes obrigam-se, durante o curso do contrato e após o seu término, ao mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às respectivas atividades, das quais venha a ter conhecimento ou às quais venha a ter acesso por força do cumprimento do contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento da obrigação assumida por eventuais perdas e danos e sujeitando-se às cominações legais, nos termos das Leis 13.709 de 14.08.2018, 4.595 de 31.12.1964 e demais leis correlatas;

26.5 Todo e qualquer recurso computacional utilizados pelas CONTRATADAS, necessários para o atendimento do objeto do contrato, deverão ser devidamente legalizados, em conformidade com as leis de Software (nº 9.609/98) e do Direito Autoral (nº 9.610/98);

26.6 Para se garantir o fiel cumprimento de todas as cláusulas e condições do contrato, as CONTRATADAS deverão optar por uma das modalidades de garantia previstas nos incisos de I a III, do parágrafo primeiro, do art. 56, da Lei nº 8.666/93, ou dos dispositivos legais correlatos da Lei nº 13.303/2016.

ADENDO I – MODELO DE PROPOSTA DE PREÇOS – LOTE I

CARTA DE APRESENTAÇÃO DE PROPOSTA

Ao BANCO DO ESTADO DO PARÁ S.A.
Av. Presidente Vargas, n. 251, Ed. BANPARÁ – 1º andar
Comércio, Belém/PA, CEP 66.010-000

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

Objeto do LOTE 01:

LOTE	ITEM	OBJETO	MEIO DE TRANSMISSÃO	BANDA	QTDE	VLR MENSAL	VLR ANUAL
I	01	Enlace de Internetcom Anti-DDoS	Fibra óptica	500mbps	2		
	02	Concentrador	Fibra óptica	300mbps	2		
	03	Enlace MPLS/SD-WAN	Fibra óptica	4mbps/ 10mbps	32		

Prezados senhores,

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

1. Propõe-se o Valor Total de R$ .....(. .....).

A tabela completa com localidade, endereço, coordenadas geográficas, tecnologia, velocidade e tempo de reparo consta no ANEXO I a este ADENDO.

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

3. Junta-se detalhamento da proposta.

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

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

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

( ) Não é optante do Simples Nacional.

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

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, esta proposta constituirá um compromisso da empresa..... , observadas as condições do edital. Caso esta proposta não venha a ser aceita para contratação, o BANPARÁ fica desobrigado de qualquer responsabilidade referente à presente proposta.

7. Os pagamentos serão efetuados em conformidade com as condições estabelecidas no termo de referência e na minuta do contrato.

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

BANCO: 037 .....
AGÊNCIA: .....
CONTA CORRENTE: .....

IMPORTANTE: Caso não seja informado desde já, nos campos acima citados, a agência e conta aberta no Banco do Estado do Pará, em cumprimento ao art. 2º do Decreto Estadual n.º 877/2008 de 31/03/2008, **O LICITANTE VENCEDOR DEVERÁ APRESENTAR A SEGUINTE DECLARAÇÃO:**

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

9. Por fim, declara conhecer e aceitar as condições constantes do edital do Pregão Eletrônico n. ...../. ..... e de seus anexos.

.....
(Local e Data)

.....
(Representante legal)

ANEXO I ao modelo de proposta de preços – LOTE I

LINKS INTERNET										
	TIPO	**Município**	**Unidade**	**Endereço**	**Coordenadas**	**Tecnologia**	**Veloc.**	**Tempo de Reparo (hora)**	**Valor Mensal**	**Valor Anual**
1	MATRIZ	BELÉM	MUNICIPALIDADE	R. Municipalidade, 1036 - Umarizal, Belém - PA, 66050-350	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	500 MBPS	1		R$ -
2	MATRIZ	BELÉM	PRESIDENTE VARGAS	Av. Pte. Vargas, nº 251 - Campina - 66.010-000	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	500 MBPS	1		R$ -
								TOTAL	R$ -	R$ -

LINKS CONCENTRADORES MPLS										
	TIPO	**Município**	**Unidade**	**Endereço**	**Coordenadas**	**Tecnologia**	**Velocidade**	**Tempo de Reparo (hora)**	**Valor Mensal**	**Valor Anual**
1	MATRIZ	BELÉM	MUNICIPALIDADE	R. Municipalidade, 1036 - Umarizal, Belém -PA, 66050-350	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	300 MBPS	1		R$ -
2	MATRIZ	BELÉM	PRESIDENTE VARGAS	Av. Pte. Vargas, nº 251 - Campina - 66.010-000	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	300 MBPS	1		R$ -
								TOTAL	R$ -	R$ -

LINKS MPLS/SDWAN										
	TIPO	**Município**	**Unidade**	**Endereço**	**Coordenadas**	**Tecnologia**	**Veloc.**	**Tempo de Reparo (hora)**	**Valor Mensal**	**Valor Anual**
1	Agência	BARCARENA	VILA DOS CABANOS	Av. Cônego Jerônimo Pimentel, s/n - Quadra 290 - Lote 25	1°30'58.9"S 48°41'51.8"W	FIBRA OPTICA	10MBPS	6		
2	PAE	BELÉM	SEMA UTINGA	R. do Utinga - Curió Utinga, Belém - PA, 66610-010	1°25'25.8"S 48°26'43.9"W	FIBRA OPTICA	10MBPS	2		R$ -

3	PAE	BELÉM	PROPAZ	Trav. Celso Malcher, 920 - Terra Firme - Belém/PA	1°27'26.8"S 48°27'00.7"W	FIBRA OPTICA	10MBPS	2		R$ -
4	Agência	ITAITUBA	ITAITUBA-CIDADE ALTA	Rua Décima Quinta, nº 835 - Bela Vista - 68.180-420	4°15'35.8"S 55°59'12.7"W	FIBRA OPTICA	10MBPS	6		R$ -
5	Agência	ITAITUBA	ITAITUBA	Av. Dr Hugo de Mendonça, nº 852 - Centro - 68.180-000	4°16'32.0"S 55°59'03.6"W	FIBRA OPTICA	10MBPS	6		R$ -
6	Agência	MOCAJUBA	MOCAJUBA	Rua Manoel de Souza Furtado, nº 872 - Centro - 68.420-000	2°35'00.5"S 49°30'16.8"W	FIBRA OPTICA	10MBPS	8		R$ -
7	Agência	MONTE ALEGRE	MONTE ALEGRE	Trav. Dr. Carlos Arnóbio Franco, nº 250 - Centro	1°59'57.7"S 54°04'16.7"W	FIBRA OPTICA	10MBPS	12		R$ -
8	Agência	NOVA TIMBOTEUA	NOVA TIMBOTEUA	Av. Barão do Rio Branco, n° 1966 - Centro 68.730-000	1°12'27.2"S 47°23'35.9"W	FIBRA OPTICA	10MBPS	6		R$ -
9	Agência	NOVO PROGRESSO	NOVO PROGRESSO	Rua Aymoré, s/n - Centro - 68.193-000	7°02'37.7"S 55°24'52.7"W	FIBRA OPTICA	10MBPS	12		R$ -
10	Agência	OEIRAS	OEIRAS	Rua Magalhães Barata, nº 862 - Centro - 68.470-000	2°00'15.8"S 49°51'22.5"W	FIBRA OPTICA	10MBPS	12		R$ -
11	Agência	PACAJÁ	PACAJA	Rua 24 de Janeiro, 260 - Centro - CEP 68485-000	3°50'11.1"S 50°38'11.0"W	FIBRA OPTICA	10MBPS	12		R$ -
12	Agência	PORTO DE MOZ	PORTO DE MOZ	Rua Rui Barbosa, nº 1554 - Centro - 68.330-000	1°45'12.2"S 52°14'17.6"W	FIBRA OPTICA	10MBPS	12		R$ -
13	Agência	SANTANADO ARAGUAIA	SANTANA DO ARAGUAIA	Rua Adão Franco, nº 15, Q 7, Lote 1 - Centro	9°20'09.6"S 50°20'22.7"W	FIBRA OPTICA	10MBPS	12		R$ -
14	Agência	Terra Alta	Terra Alta	Av. Magalhães Barata Nº 500-A, Setor 1 – Qd 4 – Lote 7; Centro; CEP: 68773-000	1°02'23.4"S 47°54'38.5"W	FIBRA OPTICA	10MBPS	6		R$ -
15	PAE	TUCURUÍ	HOSPITAL REGIONAL DE TUCURUI	Av. Dos Amazônidas, s/n - Vila Permanente,Tucuruí - PA, 68455-464	3°49'42.8"S 49°40'25.6"W	FIBRA OPTICA	10MBPS	6		R$ -
16	Agência	VIGIA	VIGIA	Av. Boulevard Melo Palheta, s/n - Centro - 68.780-000	0°51'12.2"S 48°08'43.4"W	FIBRA OPTICA	10MBPS	6		R$ -
17	Agência	VISEU	VISEU	Rua Major Olímpio, nº 366 - Centro - 68.620-000	1°12'19.4"S 46°08'21.5"W	FIBRA OPTICA	10MBPS	12		R$ -

18	Plano de Expansão	SANTA CRUZ DO ARARI	Santa Cruz do Arari	Rua Benjamim Gaioso iglesias S/Nº	0°39'53.8"S 49°10'19.5"W	FIBRA OPTICA	10MBPS	12		R$ -
19	Plano de Expansão	QUARIPURU	QUARIPURU	Rua Conego Siqueira Mendes Nº 468; Bairro Marambaia; CEP: 68709-000	0°53'37"S 47°00'15.9"W	FIBRA OPTICA	10MBPS	6		R$ -
20	Plano de Expansão	BAGRE	BAGRE	Tv. Evaristo de Mendonça, s/n. CEP: 68.475-000	1°53'59.9"S 50°12'31.6"W	FIBRA OPTICA	10MBPS	12		R$ -

21	Plano de Expansão	OURÉM	OURÉM	R. Padre Lazaro Moretti, s/n. CEP: 68.640-000	1°33'04.3"S 47°06'51.6"W	FIBRA OPTICA	10MBPS	6		R$ -
22	Plano de Expansão	INHANGAPI	INHANGAPI	Av. Hernane Lameira, s/n, Rod. PA 422, Lote 7, Bairro Vila Nova. CEP: 68.770-000	1°25'58.7"S 47°54'28.7"W	FIBRA OPTICA	10MBPS	6		R$ -
23	Plano de Expansão	IRITUIA	IRITUIA	R. Siqueira Campos, s/n. CEP: 68.655-000	1°46'19.5"S 47°26'21.3"W	FIBRA OPTICA	10MBPS	6		R$ -
24	Plano de Expansão	SANTARÉM NOVO	SANTARÉM NOVO	Tv. Paes de Carvalho S/Nº; entre R. Frei Daniel e Av. Francisco Martins de Oliveira	0°55'48.4"S 47°23'52.6"W	FIBRA OPTICA	10MBPS	6		R$ -
25	Plano de Expansão	SÃO SEBASTIÃO DA BOA VISTA	SÃO SEBASTIÃO DA BOA VISTA	Av. 18 de Novembro S/Nº	1°43'01.8"S 49°31'55,8"W	FIBRA OPTICA	10MBPS	12		R$ -
26	Plano de Expansão	SÃO FRANCISCO DO PARÁ	SÃO FRANCISCO DO PARÁ	Tv. Padre Inácio Magalhães, S/Nº, Esquina com R. Ricardo Rodrigues	1°10'18,6"S 47°47'5"W	FIBRA OPTICA	10MBPS	6		R$ -
27	Plano de Expansão	SÃO DOMINGOS DO ARAGUAIA	SÃO DOMINGOS DO ARAGUAIA	Tv. Serafim S/Nº; Entre Av. Duque de Caxias e Av. Jarbas Passarinho	5°32'13.0"S 48°43'58.3"W	FIBRA OPTICA	10MBPS	6		R$ -
28	Plano de Expansão	SÃO JOÃO DO ARAGUAIA	SÃO JOÃO DO ARAGUAIA	Av. Belém S/Nº Entre R. Boa Vista e a Rod. Pedro Carneiro (PA 405)	5°21'46.2"S 48°47'33.3"W	FIBRA OPTICA	10MBPS	6		R$ -
29	Plano de Expansão	PLACAS	PLACAS	Em prospecção	3°52'02.7"S 54°13'01.0"W	FIBRA OPTICA	10MBPS	12		R$ -
30	Plano de Expansão	AVEIRO	AVEIRO	Em prospecção	3°36'20.1"S 55°19'45.7"W	FIBRA OPTICA	10MBPS	12		R$ -
31	Plano de Expansão	URUARÁ	URUARÁ	Em prospecção	3°42'56.0"S 53°44'24.4"W	FIBRA OPTICA	10MBPS	12		R$ -
32	Plano de Expansão	SÃO DOMINGOS DO CAPIM	SÃO DOMINGOS DO CAPIM	Em prospecção	1°40'33.5"S 47°46'23.2"W	FIBRA OPTICA	10MBPS	6		R$ -
								TOTAL	R$ -	R$ -

ADENDO II – MODELO DE PROPOSTA DE PREÇOS – LOTE II

CARTA DE APRESENTAÇÃO DE PROPOSTA

Ao BANCO DO ESTADO DO PARÁ S.A.
Av. Presidente Vargas, n. 251, Ed. BANPARÁ – 1º andar
Comércio, Belém/PA, CEP 66.010-000

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

Objeto do LOTE 02::

LOTE	ITEM	OBJETO	MEIO DE TRANSMISSÃO	BANDA	QTDE	Vlr Mensal	Vlr Anual
II	04	Concentrador	Fibra óptica	300mbps	2		
	05	Enlace MPLS/SD-WAN	Satélite Banda Ku	4mbps uplink 1mbps downlink	50		

Prezados senhores,

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

1. Propõe-se o Valor Total de R$ .....(.....).

A tabela completa com localidade, endereço, coordenadas geográficas, tecnologia, velocidade e tempo de reparo consta no ANEXO I a este modelo de proposta comercial.

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

3. Junta-se detalhamento da proposta.

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

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

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

( ) Não é optante do Simples Nacional.

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

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, esta proposta constituirá um compromisso da empresa....., observadas as condições do edital. Caso esta proposta não venha a ser aceita para contratação, o BANPARÁ fica desobrigado de qualquer responsabilidade referente à presente proposta.

7. Os pagamentos serão efetuados em conformidade com as condições estabelecidas no termo de referência e na minuta do contrato.

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

BANCO: 037 .....
AGÊNCIA: .....
CONTA CORRENTE: .....

IMPORTANTE: Caso não seja informado desde já, nos campos acima citados, a agência e conta aberta no Banco do Estado do Pará, em cumprimento ao art. 2º do Decreto Estadual n.º 877/2008 de 31/03/2008, **O LICITANTE VENCEDOR DEVERÁ APRESENTAR A SEGUINTE DECLARAÇÃO:**

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

9. Por fim, declara conhecer e aceitar as condições constantes do edital do Pregão Eletrônico n. ...../..... e de seus anexos.

.....
(Local e Data)

.....
(Representante legal)

ANEXO I ao modelo de proposta de preços - LOTE II

LINKS CONCENTRADORES MPLS										
	TIPO	Município	Unidade	Endereço	Coordenadas	Tecnologia	Veloc.	Tempo de Reparo	Valor Mensal	Valor Anual
1	MATRIZ	BELÉM	MUNICIPALIDADE	R. Municipalidade, 1036 - Umarizal, Belém - PA, 66050-350	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	300 MBPS	1		R$ -
2	MATRIZ	BELÉM	PRESIDENTE VARGAS	Av. Pte. Vargas, nº 251 - Campina - 66.010-000	1°26'59.1"S 48°29'50.4"W	FIBRA ÓPTICA	300 MBPS	1		R$ -
								TOTAL	R$ -	R$ -

LINKS MPLS/SDWAN											
	TIPO	Município	Unidade	Endereço	Coordenadas	Tecnologia	Velocidade (Downlink)	Velocidade (Uplink)	Tempo de Reparo	Valor Mensal	Valor Anual
1	Agência	ABEL FIGUEIREDO	ABEL FIGUEIREDO	Rua Costa e Silva, nº 484 - Centro - 68.527-000	4°56'59.8"S 48°23'54.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
2	Agência	ACARÁ	ACARÁ	Tv. Manoel Paiva da Mota, nº 66 - Centro - 68.690-000	1°57'45.2"S 48°12'00.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
3	Agência	AFUÁ	AFUÁ	Tv. Mariano Cândido de Almeida, nº 61 - Centro - 68.890-000	0°09'26.1"S 50°23'27.3"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
4	Agência	ÁGUA AZUL DO NORTE	ÁGUA AZUL DO NORTE	Av. Paulo Guimarães, nº149 - Centro - 68.533-000	6°48'16.2"S 50°29'25.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
5	Agência	ANAJÁS	ANAJÁS	Rua Manoel Vieira, s/n - Centro - 68.810-000	0°59'05.4"S 49°56'19.5"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
6	Agência	BANNACH	BANNACH	Av. Antonia Soller, s/n - Lote 30 e 31 -	7°21'02.7"S 50°24'13.6"W	SATÉLITE -	4 MBP	1MBPS	10		R$

				centro 68.388-000		Banda KU	S				

7	Plano de Expansão	BELTERRA	BELTERRA	Em prospecção	2°38'21.6"S 54°56'03.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
8	Agência	BOM JESUS DO TOCANTINS	BOM JESUS DO TOCANTINS	Rua Expedito Nogueira, nº 540 - Centro - 68.525-000	5°02'45.6"S 48°36'03.5"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
9	Agência	BREJO GRANDE DO ARAGUAIA	BREJO GRANDE DO ARAGUAIA	Av. 13 de Maio, 277- Centro - 68.521-000	5°42'06.2"S 48°24'12.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
10	Agência	BREU BRANCO	BREU BRANCO	Av. Getúlio Vargas, nº 894 - Centro - 68.488-000	3°46'26.5"S 49°34'04.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	2		R$
11	Agência	BREVES	BREVES	Tv. Mário Curica, nº 326 - Centro - 68.800-000	1°41'12.1"S 50°29'08.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
12	Agência	CACHOEIRA DO ARARI	CACHOEIRA DO ARARI	Rua Sete de Setembro n° 761 - Centro - 68.840-000	1°00'58.9"S 48°57'40.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
13	Agência	CACHOEIRA DO PIRIÁ	CACHOEIRA DO PIRIÁ	Rua São Marcos n° 43 - Piçarreira - 68.617-000	1°45'44.1"S 46°32'40.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
14	Plano de Expansão	CHAVES	CHAVES	Em prospecção	0°09'55.0"S 49°59'14.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
15	Agência	CUMARU DO NORTE	CUMARU DO NORTE	Rua Maranhão, nº 07, Quadra 53 - Centro - CEP 68.398-000.	7°48'42.4"S 50°46'02.8"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
16	Agência	CURRALINHO	CURRALINHO	Av. Jarbas Passarinho, n° 100 - Marambaia - 68.815-000	1°48'39.5"S 49°47'53.2"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
17	Agência	CURUÁ	CURUÁ	Rua 3 de Dezembro, nº 7 - Santa Terezinha - 68.210-000	1°53'21.8"S 55°07'06.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
18	PAB	DOM ELISEU	ITINGA (DOM ELISEU)	Rod. BR 010 - KM 1481 - Posto Fiscal da SEFA - 68.633-000	4°26'15.4"S 47°32'09.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
19	Agência	FLORESTA DO ARAGUAIA	FLORESTA DO ARAGUAIA	Av. Sete de Setembro, nº 2196, Quadra 132 - Lote 11	7°33'46.0"S 49°42'18.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
20	Plano de Expansão	GURUPÁ	GURUPÁ	Em prospecção	1°24'26.3"S 51°38'47.2"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
21	Agência	JACAREACANGA	JACAREACANGA	Tv. Tenente Fernandes, 04, Quadra 106, Lote 09 - Centro - 68195-000	6°13'12.3"S 57°45'25.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$

22	Agência	JURUTI	JURUTI	Praça da República, s/n - Centro - 68.170-000	2°09'13.8"S 56°05'36.2"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
23	Plano de Expansão	MÃE DO RIO	MÃE DO RIO	Em prospecção	2°03'13.0"S 47°33'05.6"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$

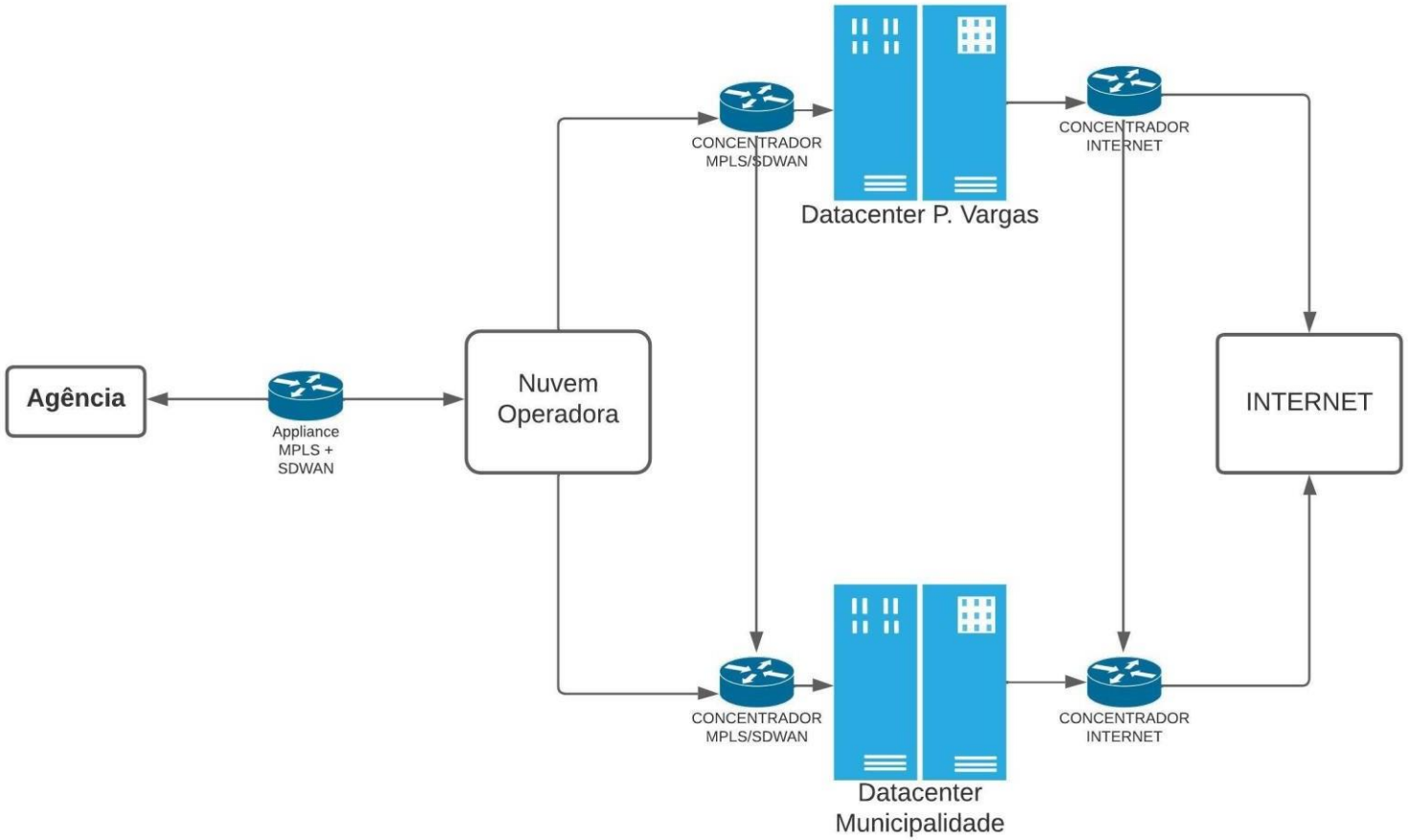
24	Agência	MAGALHÃES BARATA	MAGALHÃES BARATA	Rua Doutor Lauro Sodré, s/n - Centro 68.722.000	0°47'56.2"S 47°36'07.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
25	Agência	MELGAÇO	MELGAÇO	Rua Marechal Rondon, nº 64, Quadra 02 - Lote 35	1°48'27.0"S 50°42'53.5"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
26	Agência	MOCAJUBA	MOCAJUBA	Rua Manoel de Souza Furtado, nº 872 - Centro - 68.420-000	2°35'00.5"S 49°30'16.8"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
27	Agência	MOJUÍ DOS CAMPOS	MOJUÍ DOS CAMPOS	Av. Castelo Branco, s/n - Centro - 68.129-000	2°40'55.4"S 54°38'33.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
28	Agência	MONTE ALEGRE	MONTE ALEGRE	Trav. Dr. Carlos Arnóbio Franco, nº 250 - Centro	1°59'57.7"S 54°04'16.7"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
29	Plano de Expansão	NOVA ESPERANÇA DO PIRIÁ	NOVA ESPERANÇA DO PIRIÁ	Em prospecção	2°16'20.4"S 46°58'03.8"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
30	PAB	NOVA IPIXUNA	NOVA IPIXUNA	Avenida Brasil Nº 04. Setor 12. Quadra 77. Lote 129.	4°55'14.7"S 49°04'31.2"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
31	Agência	NOVO PROGRESSO	NOVO PROGRESSO	Rua Aymoré, s/n - Centro - 68.193-000	7°02'37.7"S 55°24'52.7"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
32	Plano de Expansão	NOVO REPARTIMENTO	NOVO REPARTIMENTO	Em prospecção	4°14'59.7"S 49°56'54.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
33	Agência	ÓBIDOS	ÓBIDOS	Rua Deputado Raimundo Chaves, nº 18	1°55'01.7"S 55°30'54.8"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
34	Agência	ORIXIMINÁ	ORIXIMINÁ	Tv. Carlos Maria Teixeira, s/n - Centro - 68.270-000	1°45'20.8"S 55°51'32.6"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
35	Agência	OURILÂNDIA DO NORTE	OURILÂNDIA DO NORTE	Av. Piauí, n° 1218, Quadra 67- Lotes 24 e 25 - setor 3	6°45'22.4"S 51°04'27.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
36	Agência	PALESTINA DO PARA	PALESTINA DO PARA	Av. Marechal Rodon, nº 29 - Centro - 68.535-000	5°44'29.0"S 48°19'05.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
37	Plano de Expansão	PEIXE BOI	PEIXE BOI	Em prospecção	1°11'37.9"S 47°19'02.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
38	agencia	PIÇARRA	PIÇARRA	Rua Maria Lucia Pimentel, nº 274 - CEP	6°26'45.5"S 48°51'53.2"W	SATÉLITE -	4 MBP	1MBPS	6		R$

				68575-000		Banda KU	S				
39	Plano de Expansão	PORTEL	PORTEL	Em prospecção	1°56'16.7"S 50°49'01.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
40	Agência	PRAINHA	PRAINHA	Rua 15 de Novembro, S/N - Centro	1°48'07.4"S 53°28'44.0"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$

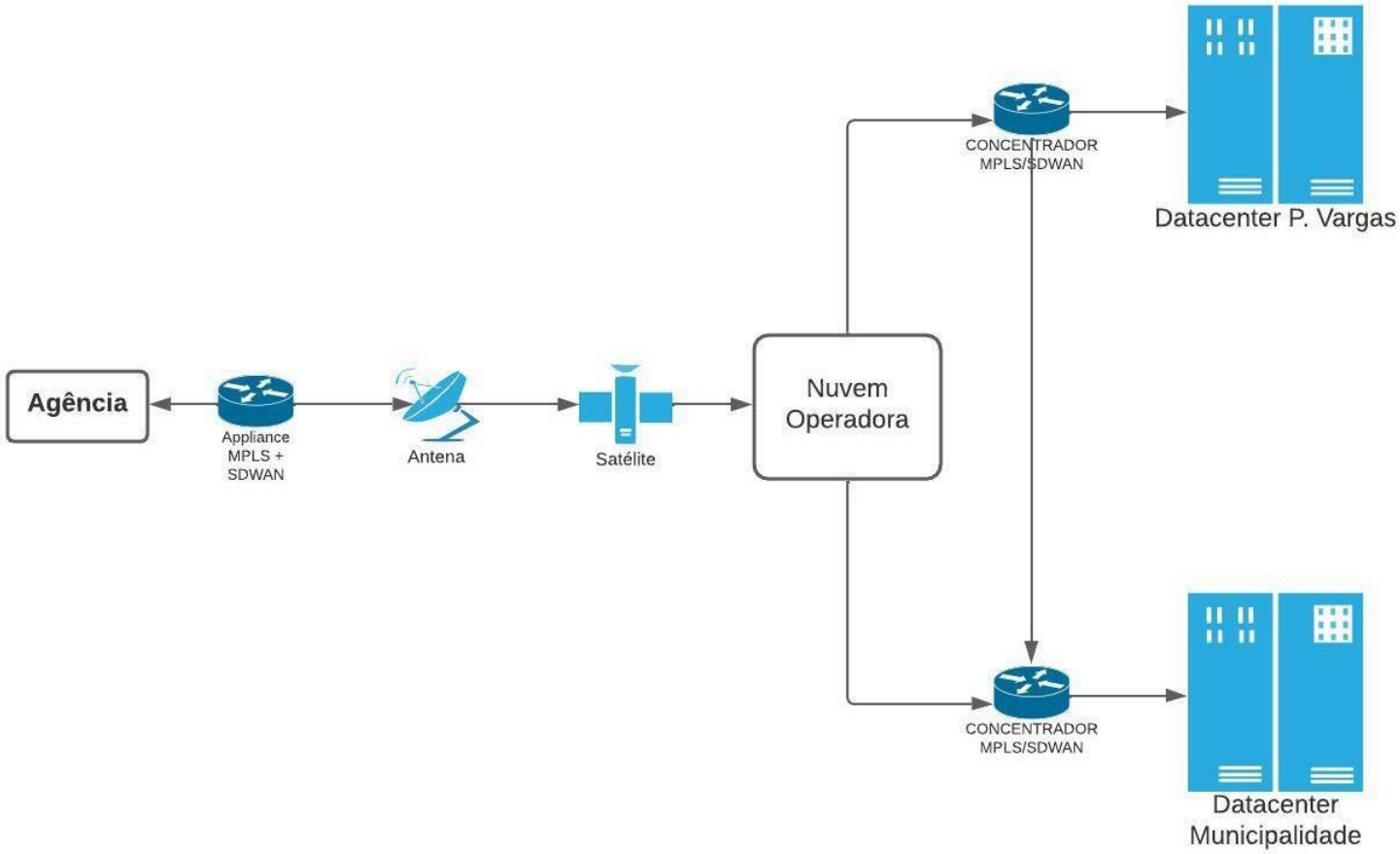
41	Agência	SANTANA DO ARAGUAIA	SANTANA DO ARAGUAIA	Rua Adão Franco, nº 15, Q 7, Lote 1 - Centro	9°20'09.6"S 50°20'22.7"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
42	Agência	SÃO FELIX DO XINGU	SÃO FELIX DO XINGU	Rua América, nº 3486 - Lote 19, Qd 161, Setor 2 - Rodoviário	6°38'29.4"S 51°58'58.3"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
43	Agência	SÃO GERALDO DO ARAGUAIA	SÃO GERALDO DO ARAGUAIA	Av. José Bonifácio, nº 1202 - Centro - 68.570-000	6°23'40.9"S 48°33'33.6"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
44	Plano de Expansão	SÃO JOÃO DA PONTA	SÃO JOÃO DA PONTA	Em prospecção	0°51'13.6"S 47°55'22.9"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
45	Agência	SENADOR JOSE PORFÍRIO	SENADOR JOSE PORFÍRIO	Rua Marechal Assunção, nº 100 - Centro - 68.360-000	2°35'22.7"S 51°57'03.1"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
46	Agência	TERRA SANTA	TERRA SANTA	Rua Nossa Senhora das Graças nº 100 - Centro - 68.285-000	2°06'35.9"S 56°29'33.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	12		R$
47	Agência	TRAIRÃO	TRAIRÃO	Rua Magalhães Barata n° 19 - Bela Vista - 68.198-000	4°42'08.4"S 55°59'38.5"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	8		R$
48	Agência	TUCUMÃ	TUCUMÃ	Av. Pará, nº 819 - Centro - 68.385-000	6°44'55.3"S 51°09'29.7"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	10		R$
49	Agência	ULIANOPÓLIS	ULIANOPÓLIS	Rua João Buzzi, n°87 - Centro 68.632-000	3°45'09.7"S 47°29'49.6"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
50	Plano de Expansão	URUARÁ	URUARÁ	Em prospecção	3°42'56.0"S 53°44'24.4"W	SATÉLITE - Banda KU	4 MBPS	1MBPS	6		R$
									TOTAL	R$	R$ -

ADENDO III -
TOPOLOGIAS

TOPOLOGIA LOTE I



TOPOLOGIA – LOTE II



ADENDO IV - TERMO DE CONFIDENCIALIDADE, ZELO E RESPONSABILIDADE SOBRE INFORMAÇÃO DO BANCO DO ESTADO DO PARÁ S.A.

Pelo presente termo se confidencialidade, zelo e responsabilidade, considerando que os bens de informação a mim disponibilizados por força de processo licitatório do BANPARÁ são de propriedade deste e devem ser utilizados com o único e exclusivo objetivo de permitir a adequada prestação dos serviços a serem contratados e, ciente dos cuidados necessários à preservação e proteçãode todos os bens de informação da instituição, inclusive em relação ao dever de sigilo, comprometo-mea:

I – Seguir as diretrizes da política de segurança e proteção dos bens de informação do BANPARÁ, sobpena de responsabilização penal ou civil cabíveis;

II - Utilizar os bens de informação disponibilizados por força exclusivamente para fins da adequada prestação dos serviços a serem contratados, estritamente em observância aos interesses do BANPARÁ;

III - 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 pessoasnão autorizadas;

IV – Manter, a qualquer tempo e sob as penas da 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;

V – Instalar e utilizar nos ambientes computacionais disponibilizados pelo BANPARÁ somentesoftwares desenvolvidos, adquiridos ou autorizados expressamente pelo BANPARÁ em pretensocontrato resultante do processo licitatório.

Declaro, ainda, para os devidos fins de direito, que me responsabilizo e obrigo a fazer com que quaisquer de meus representantes, empregados, consultores e demais colaboradores que vierem a ter acesso a quaisquer dados e informações confidenciais cumpram as obrigações constantes deste Termo.

Belém,____de_____de 2022.

_____

Nome:
Documento de Identidade:

ANEXO V - DIRETRIZES PARA UTILIZAÇÃO DE DESENVOLVIMENTO SEGURO

1. METODOLOGIA

O conteúdo deste documento é resultante de uma criteriosa pesquisa em diversas fontes reconhecidas e confiáveis por seus trabalhos, sobretudo no que tange à normatização, processos e diretrizes de segurança.

ISO/IEC 15408:2008
Common Weakness Enumeration (CWE)
OWASP Secure Coding Practices

2. PREMISSAS

2.1 Integrar o sistema a solução de Cyberark (cofre de senha) para utilização de credenciais genéricas.

2.2 Os ambientes de desenvolvimento, homologação e produção devem ser logicamente isolados, respeitando ainda o controle de acesso estabelecido internamente;

2.3 Os sistemas devem possuir recursos para realizar o registro de eventos e/ou atividades, corroborando com os critérios para a geração de logs descritos na Política de Segurança e ANEXO XX - NORMA DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS;

2.4 O sistema deve possuir capacidade de tolerância a falhas e retorno a operação. Inclui-se aqui uma atenção às mensagens para o tratamento de erros na interface do usuário;

2.5 Inspeções periódicas por amostragem no código deverão ser realizadas para verificar o atendimento aos requisitos de segurança e à ausência de códigos maliciosos com uso de ferramenta de teste, como o OWASP Zed Attack Proxy Project ou Sonar, que analisa o comportamento da aplicação e aponta possíveis vulnerabilidades de segurança. O relatório da análise desse tipo de ferramenta deve ser apresentado como requisito de validação de segurança do sistema, sendo que 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 para avaliação e verificação das fragilidades;

2.6 Sistema publicado na DMZ passará por teste de intrusão em fase piloto e somente será expandido para produção após regularizar todas as falhas de segurança encontradas.

2.7 Os ambientes de produção e homologação devem ser gerenciados pela equipe de infraestrutura e corretamente configurado para receber atualizações, *patches* e avaliações periódicas, de forma a assegurar maior segurança para os processos suportados pela aplicação;

2.8 Os aplicativos só devem passar do ambiente de homologação para a produção após a conclusão bem sucedida dos testes funcionais e de segurança (análise de vulnerabilidades);

2.9 Para funções triviais em que seja realizado o reaproveitamento de código, utilizar sempre componentes já testados, validados e aprovados em outros projetos.

2.10 Deve ocorrer atualização de componente para caso que a versão atual seja descontinuada pelo fabricante para versão atualizada do mesmo.

2.11 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.

2.12 Sistema deve prevenir os seguintes ataques **Erro! Fonte de referência não encontrada.**: 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

3. ORIENTAÇÕES TÉCNICAS PARA O DESENVOLVIMENTO DE SISTEMAS

Nesta seção serão abordadas instruções a respeito de métodos gerais de programação, ponderando, sobretudo, os aspectos de segurança que envolvem o uso dos sistemas. Por desconsiderar as tecnologias e ferramentas empregadas, o presente conteúdo não direciona seus dados a tal ou tal linguagem.

3.1. GERENCIAMENTO DE ARQUIVOS

3.1.1. Solicitar autenticação antes de permitir que seja feito o upload de arquivos;

3.1.2. Limitar os tipos de arquivos que podem ser enviados para aceitar somente os tipos necessários ao propósito do negócio (trabalhar com o modelo de *white list*). Validar os arquivos através da verificação dos cabeçalhos, uma vez que extensões de arquivos são facilmente modificadas;

3.1.3. Não salvar arquivos no mesmo diretório de contexto da aplicação, principalmente se esta for web. Preferencialmente, utilizar servidores de conteúdo ou bases de dados específicas;

3.1.4. Nos diretórios onde serão recebidos arquivos de upload, desativar privilégios de execução de binários, scripts ou arquivos de linguagens específicas, tais como: ASP, PHP, Perl, etc.

3.1.5. Não enviar caminhos de diretórios ou de arquivos em requisições. Utilizar mecanismos de mapeamento desses recursos para índices definidos em uma lista pré-definida de caminhos;

3.1.6. Nunca devolver o caminho absoluto do arquivo para o cliente da aplicação ou usuário final;
3.1.7. Quando necessário referenciar outros aplicativos, não utilizar nome relativos e sim o caminho absoluto do sistema. Por exemplo, ao invés de regedit.exe, utilizar %systemroot%\regedit.exe;
3.1.8. Ao realizar chamadas de outros aplicativos, utilizar mecanismos de verificação de integridade por *checksum* ou *hash*.

3.2. GERENCIAMENTO DE MEMÓRIA

3.2.1. Instanciar explicitamente todas as variáveis e dados persistentes durante a declaração, ou antes da primeira utilização;
3.2.2. Ao usar funções que aceitem determinado número de bytes para realizar cópias (ex.: strncpy()), verificar se o tamanho do buffer de destino é igual ao tamanho do buffer de origem. Neste caso, ele não pode encerrar a sequência de caracteres com valor nulo (*null*);
3.2.3. Verificar os limites do buffer caso as chamadas à função sejam realizadas em ciclos (*loop*) e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado;
3.2.4. Truncar todas as *strings* de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação;
3.2.5. Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo, dentre outros, não contar exclusivamente com o "*garbage collector*" e realizar a tarefa de liberação de memória explicitamente;
3.2.6. Atentar para as discrepâncias de tamanho de byte, precisão, distinções de sinal (*signed/unsigned*), truncamento, conversão de variáveis (*type casting*), cálculos que devolvam erros do tipo *not-a-number* e representação interna de números muito grandes ou pequenos;
3.2.7. Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos os pontos de saída.

3.3. CONTROLE DE ACESSOS

3.3.1. Utilizar um único componente para realizar o processo de verificação de autorização de acesso. Isto inclui bibliotecas que invocam os serviços externos de autorização. Caso a aplicação não seja possível às configurações de segurança, negar todos os acessos;
3.3.2. Garantir o controle de autorização em todas as requisições, inclusive em scripts do lado servidor, "*includes*" e requisições do lado cliente, tais como: AJAX, Flash, etc;
3.3.3. Isolar do código da aplicação os trechos de código que contêm lógica privilegiada, isto é, com permissões exclusivas;
3.3.4. Quando a aplicação tiver que ser executada com privilégios elevados, realizar esta atividade o mais tarde possível e revogá-los logo que seja possível;
3.3.5. Proteger variáveis compartilhadas e os recursos contra acessos concorrentes

inapropriados;

3.3.6. Restringir o acesso somente aos usuários autorizados de URLs, funções protegidas, serviços e dados da aplicação (atributos e campos), referências diretas e configurações de segurança, incluindo definições do servidor, arquivos de configuração e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação;

3.3.7. Não incluir credenciais diretamente no código-fonte. Adicionalmente, utilizar ofuscação de código para a proteção de dados sensíveis, tais como consultas SQL (PROTEÇÃO CONTRA ENGENHARIA REVERSA)

3.3.8. As regras de controle de acesso representadas pela camada de apresentação devem coincidir com as regras presentes no lado servidor;

3.3.9. Caso seja necessário armazenar o estado dos dados no lado cliente, utilizar mecanismos de criptografia e verificação para detectar possíveis alterações;

3.3.10. Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo;

3.3.11. Não utilizar os campos de cabeçalho (por exemplo: *referer*, *user-agent*,cookie, etc) individualmente como forma de validação de autorização. Estes devem ser utilizados sempre em conjunto com outros recursos;

3.3.12. Se for permitida a existência de sessões autenticadas por longos períodos de tempo, fazer a revalidação periódica da autorização do usuário para garantir que os privilégios não foram modificados e, caso tenham sido, realizar o registro em log do usuário e exigir nova autenticação.

3.4. GERENCIAMENTO DE SESSÕES E COMUNICAÇÕES

3.4.1. Utilizar controles de gerenciamento de sessão baseados no servidor ou em framework confiável. A aplicação deve reconhecer apenas esses identificadores de sessão como válidos;

3.4.2. O controle de gestão de sessão deve usar algoritmos conhecidos, padronizados e bem testados que garantam a aleatoriedade dos identificadores de sessão;

3.4.3. Definir o domínio e o caminho para os *cookies* que contenham identificadores de sessão autenticados, para um valor devidamente restrito ao site;

3.4.4. A funcionalidade de saída (*logout*) necessita estar disponível em todas as páginas que requerem autenticação e deve encerrar completamente a sessão ou conexão associada. Adicionalmente, não permitir *logins* persistentes (sem prazo de expiração);

3.4.5. Estabelecer um tempo de expiração baseado nos riscos e requisitos funcionais do negócio;

3.4.6. Se uma sessão estava estabelecida antes do *login*, ela deve ser encerrada (gerando um novo identificador de sessão) para que uma nova seja estabelecida;

3.4.7. Não permitir conexões simultâneas com o mesmo identificador de usuário;

3.4.8. Não expor os identificadores de sessão em URLs, mensagens de erro ou logs. Os identificadores de sessão devem apenas ser encontrados no cabeçalho do cookie HTTP. Por exemplo, não trafegar os identificadores de sessão sob a

forma de parâmetros GET;

3.4.9. Gerar um novo identificador de sessão caso a segurança da conexão mude de HTTP para HTTPS, como pode ocorrer durante a autenticação;

3.4.10. Utilizar mecanismos complementares ao mecanismo padrão de gerenciamento de sessões para operações sensíveis do lado servidor, como por exemplo o controle de *tokens* aleatórios ou outros parâmetros adicionais de autenticação;

3.4.11. Quando possível, configurar o atributo "*secure*" para cookies enviados de conexões SSL/TLS;

3.4.12. Configurar os cookies com o atributo HttpOnly, a menos que seja explicitamente necessário ler ou definir os valores dos mesmos através de scripts do lado cliente da aplicação;

3.4.13. Somente trafegar senhas através de uma conexão protegida (SSL/TLS) ou conexões cifradas. Senhas temporárias devem ser avaliadas junto a equipe de segurança;

3.4.14. Filtrar os parâmetros que contenham informações sensíveis, provenientes do "*HTTP referer*", nos links para sites externos;

3.4.15. Não transferir, diretamente, dados fornecidos pelo usuário para qualquer função de execução dinâmica sem realizar o tratamento dos dados de modo adequado;

3.4.16. As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos devem possuir o menor privilégio possível.

3.5. AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAS

3.5.1. Assegurar que os usuários sejam autenticados em todas as páginas e recursos do sistema, exceto para dados públicos;

3.5.2. Os controles de autenticação devem ser executados em um sistema confiável, centralizado e possível com bibliotecas exclusivas para esse tipo de atividade;

3.5.3. Mediante situações excepcionais nos controles de autenticação, negar quaisquer solicitações;

3.5.4. Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial;

3.5.5. As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como "nome de usuário incorreto" ou "senha incorreta", utilize apenas "usuário e/ou senha inválidos";

3.5.6. As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em local protegido, por exemplo, no servidor da aplicação;

3.5.7. Em aplicações web, utilizar apenas requisições com o método POST para transmitir credenciais de acesso;

3.5.8. A entrada da senha deve permanecer ofuscada. Em HTML, utilizar o campo do tipo "*password*";

3.5.9. Os processos de redefinição de senhas e operações de mudanças devem exigir os mesmos níveis de controle previstos para a criação de contas e

autenticação;

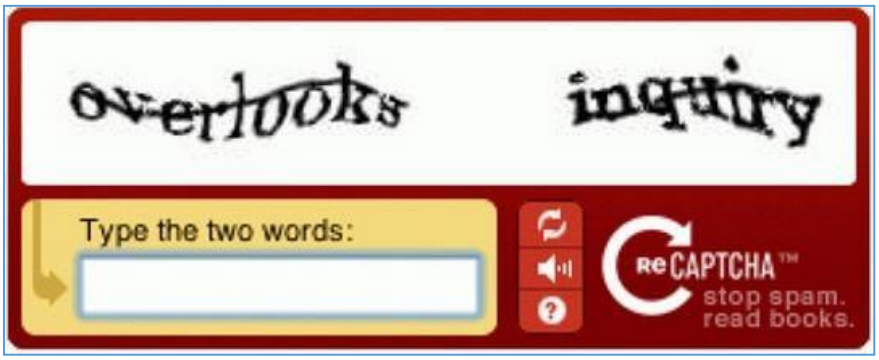
3.5.10. Se optar por usar redefinição de senha baseada em e-mail, enviar a mensagem somente para o endereços pré-definidos, com senha de acesso temporária ou link (esta opção deve considerar uma validade para o método de troca não superior a 60 minutos);

3.5.11. Exigir a mudança de senhas temporárias quando na realização do primeiro *logon*;

3.5.12. Informar ao usuário autenticado data/hora e o endereço IP da sua última utilização do sistema;

3.5.13. Se a aplicação gerenciar um repositório de credenciais, o sistema deverá garantir que as senhas sejam armazenadas na base de dados somente sob a forma de *hash*, conforme padronização contida no item 3.9“Padrões de Criptografia e Funções de *Hash*” ;

3.5.14. Para evitar ataques de *brute force* ou mesmo a utilização inadvertida de rôbos, adotar mecanismos de CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), para a diferenciação entre máquinas e humanos. Por se tratar de um desafio cognitivo, considera-se que aquele que incorpora uma solução correta é presumidamente humano. Exemplos:



3.6. VALIDAÇÃO DOS DADOS DE ENTRADA / SAÍDA

3.6.1. Efetuar toda a validação dos dados em um sistema confiável, centralizado no

servidor/aplicação;

3.6.2. Especificar o conjunto de caracteres apropriado (ex: UTF-8) e determinar se o sistema suporta essa codificação, validando se os dados recebidos estão realmente neste formato;

3.6.3. Quando ocorrer falha na validação dos dados, a aplicação deve rejeitar as informações e impedir o prosseguimento das atividades;

3.6.4. Validar todos os dados provenientes de redirecionamento ou inseridos por clientes antes do processamento, incluindo parâmetros, campos de formulário, conteúdo e cabeçalhos. Certificar-se ainda de incluir mecanismos automáticos de *postback* nos blocos de código JavaScript, Flash ou qualquer outra estrutura embutida;

3.6.5. Quando na integração com outros sistemas, utilizar preferencialmente API's que executem tarefas específicas para função desejada. Deve-se evitar que a aplicação execute comandos diretamente no sistema operacional, especialmente através da utilização de *shells*;

3.6.6. Validar, sempre que possível, todos os dados de entrada através de um método baseado em "listas brancas" que utilizem uma lista de caracteres ou expressões regulares com os caracteres permitidos. Em geral: a-z (inclusive acentuados), A-Z (inclusive acentuados), 0-9;

3.6.7. Se qualquer caractere potencialmente perigoso precisa ser permitido na entrada de dados da aplicação – como campos de senha, por exemplo – certificar-se de que foram implementados controles adicionais como a codificação dos dados de saída. Como exemplo de caracteres potencialmente "perigosos", temos: ' " < > ./ \ - | ( ) ;

3.6.8. Incluir a verificação das seguintes entradas para a validação dos dados: bytes nulos (%00), caracteres de nova linha (%0d, %0a, \r, \n) e caracteres "ponto-ponto barra" (../ ou ..\);

3.6.9. A "canonicalização" deve ser utilizada para resolver problemas de codificação dupla (*double encoding*) ou ataques por ofuscação;

3.6.10. Um computador é capaz de interpretar diversas formas de representação para um mesmo caractere, tais como: DECIMAL, HEXADECIMAL, OCTAL, HTML/UNICODE e BINÁRIO. Por esse motivo, considerar filtros e proteções em variadas formatações. Para mais informações, vide ANEXO I – REPRESENTAÇÃO DE CARACTERES ESPECIAIS.

3.6.11. Dentro do modelo MVC (Model View Controler) utilizar a validação através do serviço de controle ao invés de deixar a regra na camada de Visão ou Interface.

3.7. SEGURANÇA EM BANCO DE DADOS

3.7.1. 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;

3.7.2. Utilizar sempre que possível APIs para abstrair o acesso aos dados, quando não for possível, usar procedimentos armazenados (*stored procedures*) e permitir a remoção de permissões das tabelas no banco de dados;

3.7.3. Usar variáveis e consultas parametrizadas fortemente “tipadas”;

3.7.4. 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;

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

3.7.6. Utilizar cofre de senha (cyberark) para integração com banco de dados.

3.8. TESTES

3.8.1. Discutir a ampla utilização de testes de segurança, manuais e automatizados, de diferentes tipos, em ambiente separado de homologação e produção.

3.8.2. Discutir testes de aceitação independentes, com uso de scanners de vulnerabilidade em testes regulares e proteção dos dados utilizados para testes.

3.8.3. Discutir tratamento de casos de “abuso de segurança” em baterias de testes automatizados ou manuais.

3.8.4. Discutir a prevenção de ataques de phishing

3.8.5. Discutir a prevenção de ataques utilizando páginas falsas.

3.8.6. Discutir a prevenção de ataques utilizando cookies de terceiros.

3.8.7. Detalhar principais ataques em sistemas.

3.9. CRIPTOGRAFIA E HASHES

3.9.1. Criptografia e Hash Diretrizes para a configuração e utilização de algoritmos de criptografia e hash visando prover confidencialidade a dados.

3.9.2. Observação. Dados sigilosos e sensíveis devem ser criptografados sempre que possível. O método de criptografia empregado deve obedecer às particularidades dos dados e de sua utilização, seguindo os parâmetros aqui listados.

3.9.3. Observação. Deve-se utilizar hashes criptográficos sempre que possível, sobretudo nos seguintes casos: verificação da integridade de dados; armazenamento e verificação de senhas; provimento de identificador “único” para objetos em um sistema e geração de números pseudo-aleatórios.

3.9.4. Mínimo - Deve-se utilizar um método criptográfico que siga o princípio de

Kerckhoffs ; o 12 método de encriptação e seus parâmetros devem ser públicos e estar documentados, somente a chave criptográfica deve ser mantida em sigilo.

3.9.5. Não se deve utilizar um cifrador que admita um método conhecido para quebra da chave criptográfica melhor do que a força bruta, baseada em tentativa e erro.

3.9.6. Não se deve utilizar o modo de cifrador de bloco electronic codebook

3.9.7. (ECB) ou modos menos seguros.

3.9.8. Não se deve utilizar um tamanho da chave menor que 128 bits (cifrador simétrico) ou 1024 bits (cifrador assimétrico).

3.9.9. Não se deve utilizar função de hash sem algum tipo de salt

3.9.10. Padrão - Não se deve utilizar algoritmos considerados obsoletos para criptografia e hash criptográfico. Exemplos: MD5, SHA1, DES/3DES, RC2, RC4, MD4.

3.9.11. - Não se deve utilizar um tamanho da chave menor que 192 bits (cifrador simétrico) ou 2048 bits (cifrador assimétrico).

3.9.12. - Não se deve distribuir chaves criptográficas sem a utilização de uma infraestrutura de chave pública e, portanto, sem a utilização de um cifrador assimétrico

3.9.13. Forte - Não se deve utilizar um tamanho da chave menor que 256 bits (cifrador simétrico) ou 4096 bits (cifrador assimétrico).

3.10. AUDITORIA, RASTREAMENTO E LOGS

3.10.1. Eventos a serem registrados:

3.10.2. operações de login e logout;

3.10.3. acessos a determinadas telas ou seções do sistema;

3.10.4. acesso a informações com alguma restrição (eg documentos sigilosos, processos em segredo de justiça, dados pessoais ou bancários)

3.10.5. documentos sigilosos, processos em segredo de justiça, dados pessoais ou ba operações de consulta, inclusão, alteração ou exclusão de registros no banco de dados;

3.10.6. alteração de perfil de acesso ou status de usuários (para sistemas que possuem acesso com diferentes perfis)

3.10.7. execução de jobs e tarefas automatizadas

3.10.8. Exemplos de informações que podem ser armazenadas, relativas a cada evento:

3.10.9. data e hora

3.10.10. usuário que efetuou a operação

3.10.11. endereço IP + porta lógica

3.10.12. hostname

3.10.13. identificador da sessão do usuário (quando aplicável, eg, cookie)

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

3.10.15. identificador da instância (para sistemas clusterizados)

3.10.16. mac address

3.10.17. geolocalização

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

3.10.19. parâmetros informados pelo usuário (eg, parâmetros GET ou POST), tomando cuidado de não armazenar dados sensíveis, como senhas.

3.10.20. tempo de resposta do sistema

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

Obs.: Para aplicações que utilizam PostgreSQL, há uma proposta de rotina de auditoria de DML em https://wiki.postgresql.org/wiki/Audit_trigger_91plus. Para aplicações que utilizam Hibernate, é possível utilizar "Envers" https://docs.jboss.org/envers/docs/ ou outro event listener.

3.11. DEVSECOPS/CONTAINERS

Adoção de containers dá suporte a prática que une desenvolvimento com operações. Cada microsserviço implementa um recurso de negócios, executa seus próprios processos e comunica-se por meio de interfaces de programação de aplicações (API) ou aplicações de mensageria. Sendo possível gerenciar essas comunicações por meio de camada de malha de serviço.

Esse tipo de framework precisa ter implantada a segurança para que nesse tipo de serviço a segurança seja uma responsabilidade compartilhada e integrada do início ao fim. Dessa forma DevSecOps significa pensar na segurança da aplicação e infraestrutura desde o início, assim como automatizar algumas barreiras de segurança para evitar que o fluxo desse tipo de trabalho fique lento. Sendo que o Sec no meio do DevOps viabiliza ter uma Segurança contínua com desenho seguro do início ao fim, tendo idealmente a abordagem de segurança integrada, não apenas uma camada de proteção em torno de aplicações e dados.

3.11.1. Diretrizes de segurança específicas para containers.

3. Cada serviço deve ter o mínimo possível de privilégios para reduzir as conexões e os acessos não autorizados

4. Ter um controle rígido do acesso e usar mecanismos de autenticação

centralizados são fatores essenciais para a segurança dos microsserviços, já que a autenticação é iniciada em vários pontos com centralização dos recursos de controle de acesso e identidade de usuários.

5. Isole containers que executam microsserviços um dos outros e da rede. Isso inclui dados em trânsito e em repouso, já que ambos os tipos podem ser alvos de ataques.
6. Orquestração de containers com recursos de segurança integrados ajuda a minimizar a chance de ocorrerem acessos não autorizados com dados criptografados trocados entre aplicativos e serviços.
7. Introduza gateways de API seguros,APIs seguras com visibilidade de autorização e roteamento, para reduzir as superfícies.

3.11.2. Segurança do processo de CI/CD

8. Integrar verificadores de segurança para containers: parte do processo de container no registro.
9. Automatizar os testes de segurança no processo de integração contínua para executar ferramentas de análise estática de segurança como parte das compilações, bem como verificar quaisquer imagens de containers criadas anteriormente para encontrar vulnerabilidades de segurança conhecidas conforme elas são inseridas no pipeline da criação.
10. Adicionar testes automatizados para os recursos de segurança no processo de teste de aceitação para automatizar os testes de validação de entradas, bem como os recursos de autorização e autenticação da verificação.
11. Automatizar as atualizações de segurança, patches conforme está no MNP DE SEGURANÇA DA INFORMAÇÃO, CAPÍTULO XV - NORMAS PARA GESTÃO DE VULNERABILIDADES DE TECNOLOGIA DA INFORMAÇÃO.

Automatizar os recursos de gerenciamento das configurações de serviços e sistemas em conformidade com as políticas de segurança da informação e segurança cibernética assim como os MNPs de Segurança da Informação e Segurança para Sistemas Corporativos.

4. GUIA REFERÊNCIA RÁPIDA

Tópico	Descrição	Diretriz Mínimo	Diretriz Padrão	Diretriz Forte
Armazenamento de Dados	Armazenamento para Dados Abertos	Acesso de escrita restringido por senha		
Armazenamento de Dados	Armazenamento para Dados Fechados	Acesso de leitura/escrita restrito por senha	Deve-se usar criptografia de 192/2048 bits para armazenar dados	Deve-se usar criptografia de 256/4096 bits para armazenar dados

Armazenamento de Dados	Permissões de Acesso a Dados em Banco	Aplicação não deve utilizar usuário root.	Aplicação não deve ter permissões DDL, somente permissões estritamente necessárias com correspondência 1-1 entre usuário de sistema e de banco.	
Armazenamento de Dados	Gerenciamento e Distribuição de Senhas para Acesso a Dados	Senhas devem seguir padrão de força mínima que deve ser segura; não devem ser armazenadas em código fonte.	Senhas devem seguir padrão deste documento; Não utilizar mesma senha para desenvolvimento, homologação e produção; Salvar de forma segura dados de usuários e sistemas que utilizam a senha.	
Controle de Usuários: Acessos e Permissões	Identidade do Usuário e Nível de Acesso	Usuário e senha nominais.	Dar ciência das permissões e níveis de acesso. Utilizar grupos do AD.	Utilizar certificado digital/segundo fator de autenticação.
Controle de Usuários: Acessos e Permissões	Autenticação de Usuários	Não armazenar senhas em texto plano sem utilizar um algoritmo de hash seguro e salt.	Deve-se utilizar autenticação via AD (LDAPs) e/ou o framework OAuth2 para autenticar usuários internos	Deve-se utilizar autenticação via AD (LDAPs) e o framework OAuth2 além de multifator de autenticação
Controle de Usuários: Acessos e Permissões	Autenticação em Sistemas Web		HTTPS em todo o sistema e verificações adicionais.	
Comunicação Segura	Comunicação entre sistemas e/ou módulos	controle de duplicação e integridade da informação	controle de autenticação e confidencialidade	controle para não-repúdio e registro de entrega
Ataques à Sistemas e suas Defesas	Prevenção de ataques	Prevenir SQL Injection, HTML Injection e	Prevenir ataques XSS, de quebra de autenticação e	Submeter sistema a ferramentas de

		Javascript Injection	gerenciamento de sessão	testes de invasão
Auditoria, Rastreamento e Logs	Rastreamento das operações realizadas pelos usuários nos sistemas	Documento de requisitos do software deverá definir as informações a serem armazenadas e o local de armazenamento.	Documento de requisitos do software deverá definir políticas de retenção e revisão dos logs.	
Prevenção, Reação e Mitigação de Falhas de Segurança	Diretivas de backup	Incluir no plano de projeto as necessidades e responsabilidade s de backup de dados e código-fonte	Definir procedimento e capacitar responsáveis pela restauração de backups	Criar baselines de versões e realizar simulações de restauração de dados continuamente
Prevenção, Reação e Mitigação de Falhas de Segurança	Políticas de testes	Realizar testes manuais antes de liberações de versão de software	Elaborar testes automatizados, cenários de testes e outras políticas que garantam segurança, sigilo e não vulnerabilidade do software	Propor constantes desafios com intuito de identificar falhas de segurança nos softwares
Prevenção, Reação e Mitigação de Falhas de Segurança	Ocorrências de falhas de segurança	Definir política para imediata indisponibilizaçã o do sistema e correção da falha	Política de acompanhament o pós-ocorrência	Revisão contínua da política de testes com base em lições aprendidas
Criptografia e Hash	Tamanho de chave para cifradores simétricos/assi m étricos.	128/1024 bits	192/2048 bits	256/4096 bits
Criptografia e Hash	Modo de cifrador de bloco.	Mais seguro que ECB		
Criptografia e Hash	Requisitos cifradores.	Somente chave sigilosa, melhor ataque força-bruta.	Não usar cifradores/modo s obsoletos. E.g ., DES, RC4, etc.	
Criptografia e Hash	Requisitos função de hash criptográfico.	Usar salt sempre que possível	Não usar cifradores/modo s obsoletos. E.g .MD5, SHA1, etc	

Senhas	Tamanho de senhas.	8 caracteres mín. (parametrizado)	12 caracteres mín. (parametrizado)	20 caracteres mín. (parametrizado)
Senhas	Variação de tipos de caracteres: letras maiúsculas, letras minúsculas, dígitos, símbolos	2 dos 4 tipos ao menos	Letras maiúsculas e minúsculas mais um 1 dos 2 tipos restantes ao menos.	Mistura de todos os tipos de caracteres.
Senhas	Geração.	Não utilizar senhas comuns. E.g. , 12345, datas de aniversário.	Usar software gerador de senhas.	Usar software validador de senhas diferente do gerador
Senhas	Periodicidade de troca	Não superior a 1 ano.	Não superior a 6 meses.	
Senhas	Armazenamento	Senhas devem ser armazenadas criptografadas e com hash.	Criptografia usada para o armazenamento com a descrita no nível padrão.	Criptografia usada para o armazenamento com a descrita no nível forte.
Senhas	Número permitido de tentativas de validação parametrizado	Não superior a n tentativas por minuto parametrizado.	Senha bloqueada em caso de n erros de validação consecutivos parametrizado.	Exigir prova de de origem da requisição (e.g. , captcha , assinatura digital) após a primeira falha.
Ciclo de Vida de Software	Projeto e desenvolvimento	Deve haver etapa de modelagem de riscos de segurança, com verificações periódicas no cronograma.		
Ciclo de Vida de Software	Documentação e codificação.	Documentar medidas de segurança, inclusive no código da aplicação.		
Comunicação inter-sistemas	Comunicação segura entre sistemas e módulos	HTTPS	HTTPS, certificado digital, banco de dados, VPN	WS-ReliableMessaging
Ambiente de desenvolvimento	Armazenamento do código fonte	Sistema de controle de versão	Sistema de controle de	

			versão distribuído	
Ambiente de desenvolvimento	Acesso ao código fonte	Servidor SVN	Definir com chefia caso-a-caso.	
Ambiente de desenvolvimento	Segregação dos ambientes (DEV,PRD,HOM	Banco de dados e servidor de aplicação individualizados		Acesso restrito ao ambiente de produção
Ambiente de desenvolvimento	E-mails dos sistemas	E-mail criado especificamente para o sistema		

5. CHECKLIST DE DESENVOLVIMENTO

☐	Implementar rotinas para tratamento de erros, evitando que mensagens de falha ou debug sejam exibidas para o usuário. Além disso, assegurar que as mensagens de erro para falhas de autenticação não especifiquem o ponto de falha.	**Ataque/Vulnerabilidade** 2.12) Tratamento inadequado de erros e exceções (ERROR HANDLING) 2.12) Ataques de enumeração (ENUMERATION) **Referências** 3.4) Gerenciamento de sessões e comunicações 3.5) Autenticação e gerenciamento de credencias
☐	Implementar rotinas que verificam se os dados de entrada podem ser alterados em sua formatação para modificar o resultado de saída.	**Ataque/Vulnerabilidade** 2.12) Ataque de formação de strings (FORMAT STRINGS ATTACKS) **Referências** 3.6) Validação dos dados de Entrada / Saída
☐	Implementar rotinas de verificação que impeçam a alocação, por usuários ou funções internas, de quantidade de dados acima do que o tipo da variável suporta.	**Ataque/Vulnerabilidade** 2.12) Estouro de Memória (BUFFER OVERFLOW) 2.12) Estouro de Inteiros (INTEGER OVERFLOW) **Referências** 3.2) Gerenciamento de Memória
☐	Implementar rotinas para impedir que arquivos da aplicação e/ou sistema operacional fora contexto do sistema sejam acessados,	**Ataque/Vulnerabilidade** 2.12) Caminho Reverso (PATH TRAVERSAL) 6.6) Execução com privilégios desnecessários

	baixados ou exibidos para o usuário.	**Referências** 3.1) Gerenciamento de Arquivos 3.3) Controle de Acessos
□	Definir restrições para que o usuário não receba informações adicionais referentes a: ID's de outros usuário, produtos, funções, rotinas, cadastros, documento, etc.	**Ataque/Vulnerabilidade** 2.12) Caminho Reverso (PATH TRAVERSAL) 2.12) Ataques de enumeração (ENUMERATION) 2.12) Força Bruta e uso de robôs automatizados **Referências** 3.3) Controle de Acessos 3.4) Gerenciamento de sessões e comunicações
□	Estabelecer controles para evitar que a aplicação receba caracteres especiais como dados de entrada que podem resultar em comandos arbitrários do sistema operacional, banco de dados ou própria linguagem de programação. Observação: considerar as diversas formas de representação de um mesmo caractere.	**Ataque/Vulnerabilidade** 2.12) Injeção de Comandos (COMMAND INJECTION) 2.12) Injeção de códigos SQL (SQL INJECTION) 2.12) Cross-Site Scripting (XSS) **Referências** 3.6) Validação dos dados de Entrada / Saída 3.7) Segurança em Banco de Dados
□	Construir mecanismos para que o upload de arquivos ocorra somente por usuários autenticados e a aplicação receba o input de somente formatos ou extensões esperadas.	**Ataque/Vulnerabilidade** 2.12) Upload de arquivos potencialmente perigosos **Referências** 3.1) Gerenciamento de Arquivos 3.3) Controle de Acessos
□	Assegurar que dados sensíveis, credenciais de acesso e *strings* de conexão não sejam fixadas no código fonte.	**Ataque/Vulnerabilidade** 2.12) Senhas incluídas no código fonte do sistema (USE OF HARD-CODED PASSWORD) **Referências** 3.3) Controle de Acessos 3.5) Autenticação e gerenciamento de credencias

☐	Realizar a ofuscação em executáveis ou bibliotecas no intuito de dificultar que informações contidas no código fonte sejam visualizadas através do processo de engenharia reversa.	**Ataque/Vulnerabilidade** 2.12) Senhas incluídas no código fonte do sistema (USE OF HARD-CODED PASSWORD)
		Referências 3.3) Controle de Acessos 3.5) Autenticação e gerenciamento de credencias
☐	Assegurar que as diretrizes de senha definidas para a Plataforma Empresa XPTO estejam devidamente aplicadas para o sistema. Implementar também recursos para a distribuição de credenciais temporárias e/ou imposição do processo de alteração de senha após o primeiro *logon*.	**Ataque/Vulnerabilidade** 2.12) Força Bruta e uso de robôs automatizados
		Referências 3.5) Autenticação e gerenciamento de credencias Critérios e Restrições para o uso de senhas: NORMA DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS. Critérios e Restrições para contas de usuários: NORMA DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS.
☐	Assegurar que todos os dados trafegados não estejam em texto claro, isto é, todo fluxo de informações devem estar criptografadas.	**Ataque/Vulnerabilidade** 2.12) Interceptação do fluxo de comunicação
		Referências 3.4) Gerenciamento de sessões e comunicações 9) Padrões de Criptografia e Funções Hash
☐	Definir critérios e especificações de segurança para que dados trafegados por webservices sejam devidamente cifrados em nível de mensagem e/ou protegidos por autenticação.	**Ataque/Vulnerabilidade** 2.12) Interceptação do fluxo de comunicação
		Referências 3.4) Gerenciamento de sessões e comunicações 10.2) Segurança em nível de aplicação/mensagem

☐	Assegurar o armazenamento adequado das credencias de acesso no banco de dados. Implementar funções de hash+salt para os casos onde não seja utilizado SSO (*single-sign-on*).	**Ataque/Vulnerabilidade** 2.12) Força Bruta e uso de robôs automatizados **Referências** 9) Padrões de Criptografia e Funções Hash
☐	Assegurar que os processos de liberação de memória estejam sendo realizados com eficiência e sem ação exclusiva do *garbage collector*.	**Ataque/Vulnerabilidade** 2.12) Estouro de Memória (BUFFER OVERFLOW) 2.12) Estouro de Inteiros (INTEGER OVERFLOW) **Referências** 3.2) Gerenciamento de Memória
☐	Verificar se a aplicação está sendo executada com o menor nível de privilégio possível.	**Ataque/Vulnerabilidade** 2.12) Execução com privilégios desnecessários **Referências** 3.3) Controle de Acessos
☐	Assegurar que chamadas a aplicativos externos são realizadas somente a partir de caminhos absolutos.	**Ataque/Vulnerabilidade** Não relacionado neste documento. Link externo: CWE-114, CWE-427 **Referências** 3.1) Gerenciamento de Arquivos
☐	Estabelecer mecanismos para manter a aleatoriedade dos identificadores de sessão e revalidar periodicamente os *logins* em utilização. Além disso, implementar rotinas para que o sistema não permita *logins* simultâneos de um mesmo usuário.	**Ataque/Vulnerabilidade** Não relacionado neste documento. Link externo: CWE-330 **Referências** 3.3) Controle de Acessos 3.4) Gerenciamento de sessões e comunicações

☐	Implementar recursos de CAPTCHA para evitar, quando não autorizado, a utilização do sistema por robôs ou rotinas automatizadas.	**Ataque/Vulnerabilidade** Não relacionado neste documento. Link externo: CWE-804 **Referências** 3.5) Autenticação e gerenciamento de credencias
☐	Assegurar que as *strings* de conexão da aplicação com as bases de dados utilizem usuários específicos e estejam em arquivos devidamente criptografados.	**Ataque/Vulnerabilidade** Não relacionado neste documento. Link externo: CWE-311, CWE-319 **Referências** 3.7) Segurança em Banco de Dados
☐	Implementar registros históricos e trilhas de auditorias (logs) para o processo de autenticação e funções críticas do sistema.	**Ataque/Vulnerabilidade** Não relacionado neste documento. Link externo: CWE-778 **Referências** 3.3) Controle de Acessos 3.5) Autenticação e gerenciamento de credencias

ANEXO VI - DIRETRIZES PARA UTILIZAÇÃO DE NUVEM

1. OBJETIVO

Apresentar as diretrizes para utilização de nuvem de forma segura, por meio dos recursos corporativos fornecidos pelo Banco do Estado do Pará.

2. DEFINIÇÕES

- DATACENTER – Uma estrutura disposta em uma ou mais localidade e/ou país. Projetado para abrigar hardware, software e outros componentes como sistemas de armazenamento de dados, ou seja, onde o ambiente de nuvem está fisicamente localizado.

- EULA – *End User license Agreement* – acordo de licença de usuário final – é o contrato entre o licenciante e o comprador, que estabelece o direito ao comprador de utilizar o software.

- Gestor da Informação – Representante da área de negócio do Banpara.

- IAAS – Infraestrutura como serviço – *Infraestructure as a service* – é o provisionamento pelo fornecedor de processamento, armazenamento, comunicação de redes e outros recursos fundamentais de computação, nos quais o cliente pode instalar e executar software em geral, incluindo sistemas operacionais e aplicativos. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem, mas tem controle sobre o espaço de armazenamento e aplicativos instalados.

- PAAS – Plataforma como serviço – *Platform as a service* – os recursos fornecidos são linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, para que o cliente possa implantar, na infraestrutura de nuvem, aplicativos criados ou adquiridos por ele. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem que são fornecidos coo IAAS (Rede, servidores e armazenamento) mas tem controle sobre as aplicações implantadas e possivelmente sobre as configurações do ambiente que as hospeda.

- SAAS – Software como serviço – *Software is a service* – trata-se de um modelo de nuvem cuja aplicação é fornecida como serviço, eliminando-se a necessidade de adquirir ou manter infraestrutura de TI. O cliente gerencia apenas as configurações dos aplicativos específicas do usuário.

- *On premise* – instalado em ambiente e local próprio do Banpara.

- Informações corporativas classificadas – são documentos ou dados cuja perda, mal uso ou acesso não autorizado afetam negativamente a privacidade dos empregados, os negócios ou operações financeiras do Banpara, conforme descrito no manual de classificação e tratamento da Informação.

- Nuvem Hibrida – é a junção de duas ou mais infraestruturas de nuvem (pública e privada), interconectadas. É uma forma de valer-se dos benefícios das infraestruturas de nuvem pública e privada, bem com atuar na mitigação de riscos e custos associados a cada tipo.

- Nuvem Privada – a infraestrutura de nuvem privada está alocada para uso exclusivo de um único cliente. Sua utilização, gerenciamento e operação podem ser feitos pelo cliente, em suas dependências ou nas do provedor, além disso, a nuvem privada tem sua flexibilidade reduzida.

- Nuvem Pública – É uma infraestrutura de serviços e/ou recursos tecnológicos que está disponível para acesso por meio da internet e que reside nas instalações do fornecedor.

- Provisionamento – criação, manutenção e desativação de acessos do usuário em um ou mais serviços, diretórios ou aplicações, em resposta a processos de negócios automatizados ou interativos.

- Recursos corporativos – recursos exclusivos da organização, tais como e-mail, servidores, sistema ou serviços de TI.

- Unidade / Unidade Gestora – é o componente organizacional que possui gestor, equipe, atividades e responsabilidades.

- Usuário Banpara – Empregado do Banpara, prestador de serviços, usuário da fábrica, estagiário, menor aprendiz ou usuário externo autorizado a ter acesso a informações, dados, materiais ou documentos do Banpara para desempenho de suas atribuições.

3. NORMAS

3.1 DISPOSIÇÕES GERAIS

3.1.1 A contratação de serviços em nuvem é precedida por avaliação dos requisitos da solução e de segurança feito pelas áreas de arquitetura de software, Segurança da informação e continuidade de negócios, respectivamente, as quais avaliam de acordo com suas alçadas.

3.1.2 A utilização de serviço de nuvem também é precedida pela avaliação da área de infraestrutura quanto a capacidade interna ou quanto a existência de um contrato ativo de serviço de nuvem.

3.1.3 Toda a informação a ser utilizada em serviço em nuvem, deve ser classificada de acordo com os critérios estabelecidos no manual de classificação e tratamento da informação.

3.1.4 As informações classificadas como #confidencial, #restrita #interna poderão ser hospedadas em nuvem desde que observadas os parâmetros contratuais presentes neste normativo.

3.1.5 As informações não podem ser compartilhadas sem autorização expressa do gestor da informação, respeitando-se o disposto no manual de classificação e tratamento da informação.

3.1.6 O uso, desenvolvimento, testes, atualização, implantação e manutenção dos serviços armazenados em nuvem deve ser realizado somente por meio dos recursos computacionais do Banpara (Rede de Computadores Corporativa), devendo respeitar a jornada de trabalho para utilização exclusiva das necessidades relacionadas às atividades desenvolvidas pelo empregado no exercício do seu cargo.

3.1.7 O Banpara pode controlar, monitorar e suspender o uso de recursos em nuvem conforme normas vigentes.

3.1.8 O Banpara é detentor da propriedade de qualquer dado enviado para os serviços em nuvem por meios dos recursos corporativos.

3.1.9 O Banpara tem o direto de acessar qualquer informação submetida por meio dos recursos corporativos a qualquer momento.

3.1.10 Não é permitido o uso de nuvem pública gratuita que não tenha a possibilidade de realização de contrato corporativo, exceto para informações classificadas com #publica, sujeito a avaliação da área de segurança da informação.

3.2 PARÂMETROS CONTRATUAIS

3.2.1 Devem ser observados os seguintes itens na contratação dos serviços de nuvem:

3.2.1.1 O contrato entre o Banco e o prestador do serviço deve respeitar a regulamentação do Banco Central do Brasil, CMN resolução nº 4.658, de 26 de abril de 2018.

3.2.1.2 O Prestador do serviço deve apresentar expressamente concordância sobre a prevalência da legislação brasileira sobre qualquer outra.

3.2.1.3 O contrato entre o Banpara e o prestador de serviço deve estabelecer direitos claros e exclusivos de propriedade de acesso aos dados, inclusive logs.

3.2.1.4 Devem ser definidas cláusulas contratuais estabelecendo responsabilidade do provedor em garantir o isolamento de recursos de dados contra acesso indevido por outros clientes.

3.2.1.5 O Banco deve assegurar contratualmente que as informações sob custodia do provedor serão tratadas como informações sigilosas, não podendo ser usadas pelo fornecedor e nem fornecidos a terceiros sob nenhuma hipótese sem autorização formal do Banpara.

3.2.1.6 O prestador do serviço deve apresentar o convênio para a troca de informações com o Banco Central do Brasil.

3.2.1.7 O fornecedor de serviço deverá privilegiar datacenter localizados em território nacional.

3.2.1.8 Poderão ser utilizados serviços em nuvem, cujo o armazenamento de dados se materialize fora do território nacional desde que aderente a CMN resolução nº 4.658, de 26 de abril de 2018, onde exista um convênio para a troca de informações do Banco Central do Brasil com as autoridades supervisoras de onde o serviço será prestado baseado no comunicado BACEN n° 31.999 de 10/5/2018.

3.2.1.9 O provedor deve informar no ato da contratação a localização física do datacenter utilizado para fornecimento dos serviços, incluindo o datacenter de contingência. (País, Cidade).

3.2.1.10 O Provedor deve assegurar que os dados estejam sujeitos a limites geográficose que não sejam migrados para além das fronteiras definidas em contrato, inclusiveem situações de backup, contingencia ou recuperação de desastres.

3.2.1.11 A política para a gestão de mudança deve ser acordada entre o provedor e o Banpara que deve ser comunicado com antecedência mínima de 72 horas sobre mudanças.

3.2.1.12 Deve ser previsto em contrato que o fornecedor possua uma política deexclusão segura dos dados e que esta precisa ser apreciada pelo Banpara ou seguir o modelo de destruição de documentos em formato digital baseado na norma DoD 5220.22-M (ECE) ou o método descrito por Peter Gutmman no artigo “Secure Deletion of Data From Magnetic and Solid-State Memory” ou através da utilização de desmagnetizadores (degausser).

3.2.1.13 Deve ser previsto em contrato as condições, o processo operacional com os limites e os custos para a saída do fornecedor com a realização do backup e transferência dos dados em casos de não renovação contratual que necessite de repasse dos dados para outro fornecedor.

3.2.1.14 A EULA deve prever que os direitos de propriedade sobre os dados enviados pelo Banpara para a nuvem permaneçam de propriedade exclusiva do Banco nãosendo transferido para o custodiante.

3.2.1.15 O Banco Central do Brasil poderá a qualquer momento realizar inspeções no ambiente contratado.

3.2.1.16 O contrato deve prever continuidade do sistema fornecendo o código fonte do sistema ao Banpará em caso de falência do contratado ou caso de descontinuidade do serviço pelo contratado, dessa forma o banco pode dar continuidade a manutenção do serviço.

3.2.1.17 O contratado deve aplicar teste de intrusão no seu sistema de forma anual e enviar relatório de vulnerabilidades ao banpará.

3.2.1.18 O contrato deve informar a área de continuidade de negócio do Banpará seus planos de continuidade e recuperação de desastre para aprovação assim como calendário de testes de continuidade de negócio.

3.3 REQUISITOS DE ARQUITETURA

3.3.1 Deve-se privilegiar soluções de nuvem hibrida considerando sempre a melhor alocação de informações de acordo com sua classificação.

3.3.2 Não se deve adotar solução de nuvem que compartilhe a camada de dados entre os clientes.

3.3.3 O fornecedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado facilitando sua migração.

3.3.4 A gestão das chaves criptográficas, incluindo as chaves privadas, são de responsabilidade do Banpara e estas não podem ser armazenadas em nuvem.

3.3.5 Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo fornecedor para gerenciamento de vulnerabilidades conhecidas com atualização de softwares garantindo que aplicações, sistemas e dispositivos de rede sejam avaliados e que as atualizações de segurança sejam aplicadas em tempo hábil priorizando os paths com maior criticidade.

3.3.6 O processo de gestão de vulnerabilidade do provedor deve ser transparente para o Banpara e deve ser emitido relatórios mensais com as demonstrações das ações pertinentes ao processo de atualização e aplicação dos paths necessários a correções de segurança do ambiente.

3.3.7 O provedor deve prover mecanismo para acesso aos logs gerados pela infraestrutura utilizada pelo Banpara.

3.3.8 O provedor deve manter um plano de continuidade de negócio para seu datacenter utilizado para fornecimento do serviço em nuvem.

3.3.9 O datacenter de contingência deve atender as mesmas características do datacenter principal.

3.3.10 O provedor deve manter disponibilidade mínima de 99,741% dos datacenters conforme TIA 942 TIER II.

3.3.11 O provedor deve utilizar conexão segura para acesso as páginas de serviços de nuvem (HTTPS).

3.3.12 O provedor deve possuir controle que possa restringir o acesso ao serviço de nuvem por range de IP.

3.3.13 O provedor deve possuir controle de acesso físico e lógico que assegurem a confidencialidade dos dados armazenados na nuvem.

3.3.14 Provedor dispobilizar um CASB para posicionar entre o Banpará e a nuvem que está disponibilizando para impor políticas de segurança, conformidade e governança para aplicativos em nuvem, sendo que a gerência desse CASB será da SUROP/GESEI.

3.3.15 O fornecedor deve possuir log de auditoria que evidencie as ações realizados no mínimo (quem, o que, quando e onde) conforme normativos de Segurança da Informação do Banpará.

3.3.16 O serviço deve possuir proteção contra ataques de negação de serviço distribuído (anti-DDoS).

3.3.17 O provedor deve possuir capacidade de proteção dos dados em repouso.

3.3.18 Proteção

3.3.19 O provedor deve possuir certificação ISO 27001.

ADENDO VII - RECOMENDAÇÕES E PADRÕES DE SEGURANÇA TECNOLÓGICA MÍNIMA

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

1. ROTEADORES:

a) Utilização de filtros nos roteadores de borda.

2. FIREWALL:

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

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

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

f) Relativo à configuração dos firewall deverá ser observado:

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

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

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

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

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

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

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

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

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

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

3. IDS – Sistemas de Detecção de Intrusão:

a) Soluções de IDS – Sistema de Detecção de Intrusão em todas as regiões de fronteira das redes de comunicação TCP/IP relacionadas às aplicações onde sejam implementados pontos de conexão externa da CONTRATADA.
Nestes pontos são executadas interfaces de comunicação, transmissão e transferência de dados;

b) Devem ter funcionalidades que permitam a criação automática de regras de defesa, quando sob ataque, no dispositivo responsável pela autorização de tráfego;

c) Integração automática com a solução de firewall em níveis de bloqueio, proteção, alertas e geração de log;

d) Demonstrar a disponibilidade de funcionamento à taxa de 99,99% mensurada mensalmente.

e) A solução deve contemplar sensores de rede e de servidores, para os servidores envolvidos na infra-estrutura da CONTRATADA.

f) Um gráfico descrevendo a topologia dos pontos de aplicação dos sensores deve ser especificado e entregue ao BANPARÁ num período máximo de 30 (trinta) dias a contar da assinatura do contrato.

g) Entenda-se como topologia um desenho ou imagem descritiva, na qual estejam representadas as disposições das redes e seus respectivos ativos envolvidos, bem como os sensores de IDS.

h) O BANPARÁ deve ter acesso on line à configuração destes equipamentos através de sua console a qualquer momento.

i) Este acesso deverá ser seguro (autenticidade, integridade e confidencialidade dos dados) e restrito à operação de leitura.

j) A solução de IDS deve prover, no mínimo:

a. Detecção de ataques ou comportamentos anômalos baseado em "assinaturas" e/ou comportamental;

b. Permitir reset de conexão para ataques selecionados;

c. Envio de alarmes para console de gerenciamento própria com níveis de severidade de acordo com o tipo do ataque;

d. Permitir análise de segmentos de rede no modo "promíscuo";

e. Alarme por presença de strings e/ou assinaturas customizadas;

f. Criptografia dos dados entre a console administrativa e o dispositivo coletor de dados.

k) Garantia de disponibilidade de funcionamento à taxa de 99,9% medida e relatada mensalmente.

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

4. ANTIVÍRUS:

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

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

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

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

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

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

5. POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÕES

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

6. SEGURANÇA FÍSICA E LÓGICA

O acesso físico e lógico ao ambiente controlado da BANPARÁ somente será disponibilizado aos funcionários da CONTRATADA mediante o cumprimento das condições de segurança estabelecidas neste Termo de Referência e no Contrato.
Como padrão de segurança será adotada criptografia para as senhas pessoais dos usuários e para o tráfego de dados em rede, para Extranet ou Internet.
O Gestor do CONTRATO irá especificar quais dados serão armazenados no Banco de Dados e nos backups de forma criptografada.

Os dados que trafegarem pela Extranet ou Internet deverão ser criptografados podendo utilizar em sua última versão e com chave de 128 bits, um dos padrões a seguir:

a) S.S.L. - *Secure Sockets Layer*;
b) T.L.S - *Transport Layer Security.*

A CONTRATADA deverá possuir, em suas instalações, padrões mínimos necessários de segurança, objetivando garantir a segurança contra ataques externos e tentativas de invasão.

Os empregados da CONTRATADA podem ter acesso ao ambiente do BANPARÁ, exceto partições de homologação/produção e de suporte técnico, respeitados os padrões de Controle de Acesso Lógico a Sistemas Computacionais.

O acesso às bases de dados internas dos clientes do BANPARÁ, e/ou eventual armazenamento destes dados por parte da CONTRATADA dar-se-á conforme os padrões do BANPARÁ.

A CONTRATADA e seus empregados bem como a eventual subcontratada e seus empregados devem manter, sob as penas da lei, o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais dos materiais do BANPARÁ, de que venham a tomar conhecimento ou ter acesso, ou que venham a ser ele confiados, sejam relacionados ou não com o fornecimento objeto do contrato.

7. POLÍTICA DE ACESSO LÓGICO

Os documentos que constituem a política de acesso lógico a ser utilizada em todas as instâncias da infra-estrutura de rede e dos sistemas computacionais da CONTRATADA, correlatos ao processo a ser contratado, devem ser entregues ao BANPARÁ dentro de um prazo máximo de 30 (trinta) dias a contar da assinatura do contrato.

Essa política deve estar em conformidade com a norma NBR ISO/IEC 27002:2007, itens 11.1, 11.2, 11.3 e 11.4.

Caso exista alguma discordância por parte do corpo técnico do BANPARÁ as adequações deverão estar corrigidas nos documentos e implementadas num prazo inferior a 10 (dez) dias.

8. ARQUITETURA DA SISTEMA - PLATAFORMA

Deverá utilizar o conceito das três camadas no desenvolvimento da Solução: aplicação, dados e apresentação.

Deverá possuir mecanismos automáticos e manuais de manutenção das bases de dados (exemplo: reorganização de base, reindexação de tabelas), sendo todas as ações registradas em *log*.

Deverá seguir o padrão J2EE, MVC2 e W3C para a camada de apresentação *web*_.

Deverá ser desenvolvida como sendo uma coleção de módulos funcionais, onde cada módulo deverá corresponder a uma unidade de execução de uma seqüência de tarefas que compreende um determinado serviço bem delineado como, por exemplo, autorização, fraude, cobrança, fatura.

9. SEGURANÇA - ADMINISTRAÇÃO E OPERAÇÃO

Deverá suportar a segregação das funções de administração de sistemas e a administração de segurança para propiciar separação de responsabilidades no sistema.

Deverá realizar validação de entrada de dados na camada *Web* a fim de evitar ataques como SQL *Injection, Cross Site Scripting* e *Cookie Poisoing.*

10. SEGURANÇA - GERENCIAMENTO DE SESSÃO

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

11. ATENDIMENTO A RESOLUÇÃO 4658/2018 DO BANCO CENTRAL

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

11.1. Segundo art. 12 assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da CONTRATANTE aos dados e às informações a serem processados ou armazenados pelo prestador de serviço (CONTRATADA);

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço (CONTRATADA);

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) o acesso da CONTRATANTE aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço (CONTRATADA), relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) O Banpará assim como seu órgão regulador pode auditar e/ou verificar os controles da CONTRATANTE quanto a segurança mínima da mesma.

g) A CONTRATADA deve fornecer o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

h) a identificação e a segregação dos dados dos clientes da CONTRATANTE por meio de controles físicos ou lógicos; e

i) 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 VIII

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

1. – OBJETIVO

1.1. 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.

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

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

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

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

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:

1.4.1. Realiza movimentação financeira em contas de clientes (PF/PJ/Governo/Prefeitura);

1.4.2. Realiza movimentação financeira em contas da instituição financeira (Banpará);

1.4.3. Realiza movimentação de dados de clientes (PF/PJ/Governo/Prefeitura);

1.4.4. Sistemas com acesso externo ou integrado a um sistema externo;

1.4.5. Possui integração com órgãos/entidades regulamentadoras;

1.4.6. Possui integração com órgãos/entidades de apoio ao sistema financeiro nacional;

1.4.7. Possui integração com sistema que realize movimentação financeira, seja da instituição ou cliente independente da sua natureza;

1.4.8. Possui integração com parceiros de negócio;

1.4.9. Gera arquivos de natureza legal;

1.4.10. 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.

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:

1.4.11. 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.

1.4.12. 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.

1.4.13. 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.

1.4.14. Consideram-se novos sistemas como sistemas sob a responsabilidade da SUPRO/SUSIS, 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.

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.

1.4.15. 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 (Anexos: **Erro! Fonte de referência não encontrada.**, **Erro! Fonte de referência não encontrada.**, **Erro! Fonte de referência não encontrada.**, **Erro! Fonte de referência não encontrada.**) e para sistemas não críticos (Anexo VII) é imprescindível possuir gestão de: usuário, senha, perfis, perfil temporário, log transacional e de segurança; e não permitir multisessão.

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.

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.

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

É necessário que seja gravado histórico das funcionalidades do sistema

Criptografia de senha armazenada, com capacidade de ser alterada sem ônus por SUROP/GESEI. O padrão de criptografia será revisado anualmente pela SUROP/GESEI.

Para autenticação integrar via LDAPs ao Active Directory.

ESPECIFICAÇÕES DE INTEROPERABILIDADE PARA CONTROLE DE ACESSO

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.

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.

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:

1.4.16. Dos acessos dos sistemas que serão gerenciados e suas transações;

1.4.17. Dos perfis dos usuários;

1.4.18. Das contas dos usuários com um dos status abaixo:

1.4.18.1. Ativo: o usuário está habilitado a utilizar o sistema;

1.4.18.2. 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.

1.4.18.3. 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.

1.4.19. Da definição e consulta de logs dos sistemas.

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

1.4.20. 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.

1.4.21. 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.

1.4.22. 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.

1.4.23. 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.

1.4.24. 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.

1.4.25. 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.

1.4.26. 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.

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

1.4.27. 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).

1.4.28. 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.

1.4.29. 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.

1.4.30. 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.

1.4.31. 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.

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

1.4.32. 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.

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

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

1.4.34. 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.

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

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

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

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.

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.

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

ESPECIFICAÇÕES DE INTEROPERABILIDADE PARA TRILHAS DE AUDITORIA

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

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.

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

1.4.36. São consideradas duas categorias de Log: Log de Segurança de Acesso e Log de Transações.

1.4.36.1. 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.

1.4.36.2. 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.

1.4.37. 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:

1.4.37.1. Usuário de rede;

1.4.37.2. Login do Usuário;

1.4.37.3. Grupo (perfil) do usuário;

1.4.37.4. Operação;

1.4.37.5. Contexto ();

1.4.37.6. Endereço IP e porta lógica que realizou as transações;

1.4.37.7. Nome de máquina (Hostname);

1.4.37.8. A data e hora de evento do usuário, sendo (recomendável o uso do relógio do sistema e não o do host);

1.4.37.9. MAC Address;

1.4.37.10. Geolocalização;

1.4.37.11. Os registros das informações deverão ser mantidos em base de dados em ambiente de produção por período definido pela SUROP.

1.4.38. 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:

1.4.38.1. Login do usuário;

1.4.38.2. Endereço IP com porta lógica do acesso e Hostname da máquina que realizou as transações;

1.4.38.3. A data e hora de evento do usuário sendo (recomendável o uso do relógio do sistema e não o do host) com geolocalização;

1.4.38.4. Usuário de rede;

1.4.38.5. Perfil do usuário;

1.4.38.6. Eventos do usuário, a exemplo, gravação de arquivo, inclusão, alteração e exclusão de dados, deverão ser formatos em tabela. Em casos em que o evento for alterado, deverá ser incluso o dado anterior e posterior á ação salva;

1.4.38.7. Módulo Acessado;

1.4.38.8. Relatório do Log com permissão para salvar e imprimir, de acordo com a necessidade do usuário que está consultando o log.

1.4.39. 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:

1.4.39.1. Login do usuário;

1.4.39.2. Endereço IP com porta lógica do acesso e Hostname da máquina que realizou as transações;

1.4.39.3. A data e hora de evento do usuário sendo (recomendável o uso do relógio do sistema e não o do host) com geolocalização;

1.4.39.4. Usuário de rede;

1.4.39.5. Eventos do usuário, a exemplo, gravação de arquivo, inclusão, alteração e exclusão de dados, deverão ser formatos em tabela. Em casos em que o evento for alterado, deverá ser incluso o dado anterior e posterior á ação salva;

1.4.39.6. Módulo Acessado;

1.4.39.7. Relatório do Log com permissão para salvar e imprimir, de acordo com a necessidade do usuário que está consultando o log.

1.4.40. Eventos a serem registrados:

1.4.40.1. operações de login e logout;

1.4.40.2. acessos a todas as telas ou seções do sistema;

1.4.40.3. acesso a informações com alguma restrição (eg documentos sigilosos, processos em segredo de justiça, dados pessoais ou bancários)

1.4.40.4. documentos sigilosos, processos em segredo de justiça, dados pessoais ou ba operações de consulta, inclusão, alteração ou exclusão de registros no banco de dados;

1.4.40.5. alteração de perfil de acesso ou status de usuários (para sistemas que possuem acesso com diferentes perfis)

1.4.40.6. execução de jobs e tarefas automatizadas

1.4.41. 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.

1.4.41.1. 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.

1.4.41.2. 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.

1.4.42. 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 acesso.

1.4.43. 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.

1.4.44. Sistema deve permitir a consulta de logs de auditoria dos sistemas integrados a ele.

1.4.45. 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.

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

1.4.47. 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.

1.4.48. 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.

1.4.49. O sistema deve permitir relatórios dos logs de auditoria conforme a seguir:

1.4.49.1. Relatório Auditoria

1.4.49.1.1. Sistema:

1.4.49.1.2. Módulo:

1.4.49.1.3. Documento:

1.4.49.1.4. Função:

1.4.49.1.5. Usuário de sistema:

1.4.49.1.6. Usuário de banco de dados:

1.4.49.1.7. Usuário de rede:

1.4.49.1.8. IP:

1.4.49.1.9. Data Inicial:

1.4.49.1.10. Data Final:

1.4.49.1.11. Empresa:

1.4.49.1.12. Unidade:

1.4.49.1.13. Data:

1.4.49.1.14. Operação:

1.4.49.1.15. Banco:

1.4.49.1.16. Tabela:

1.4.49.1.17. Comando Sql:

1.4.49.1.18. Mudança:

1.4.49.1.19. Nº de Linhas Incluída(s):

1.4.49.1.20. Registros Incluído(s): Nº Linha, Coluna, Descrição Coluna, Valor

1.4.49.2. Relatório Auditoria Gestor:

1.4.49.2.1. Sistema:

1.4.49.2.2. Módulo:

1.4.49.2.3. Documento:

1.4.49.2.4. Função:

1.4.49.2.5. Usuário de sistema:

1.4.49.2.6. Usuário de rede:

1.4.49.2.7. IP:

1.4.49.2.8. Data Inicial:

1.4.49.2.9. Data Final:

1.4.49.2.10. Empresa:

1.4.49.2.11. Unidade:

1.4.49.2.12. Data:

1.4.49.2.13. Operação:

1.4.49.2.14. Banco:

1.4.49.2.15. Tabela:

1.4.49.2.16. Nº de Linhas Incluída(s):

1.4.49.2.17. Registros Incluído(s): Nº Linha, Coluna, Descrição Coluna, Valor

RELATÓRIOS

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.

Deverá ser fornecido a consulta e relatório contendo as informações do sistema/módulo, usuários, quantidade de acesso, data e hora do último acesso

Disponibilizar a exportação dos relatórios para arquivos do tipo documento (.rtf), planilhas (.xls) e formato de documento portátil (.pdf)

Disponibilizar relatório com mapeamento de perfil x funcionalidade por sistema na seguinte estrutura:

1.4.50. Imprimir em paisagem

1.4.51. Sistema Integrado

1.4.51.1. 1ª coluna: funcionalidades

1.4.51.2. Seguir a estrutura a seguir:

1.4.51.2.1. Sistema

1.4.51.2.2. Módulo>>Menu >> Transação >> Função

1.4.51.2.3. Módulo>>Menu >> Transação >> Função [Botão] Editar

1.4.51.2.4. A partir da segunda coluna incluir um perfil por coluna até terminar todos os perfis que possuem acesso ao sistema.

1.4.51.2.5. As colunas dos perfis devem ser preenchidas com: S: Possui permissão ou N: Não possui permissão.

1.4.51.2.6. A última coluna após terminar os perfis que possuem acesso deve ser incluída a Legenda do mapeamento:

1.4.51.2.7. Permissão:

1.4.51.2.7.1. S: Possui permissão

1.4.51.2.7.2. N: Não possui permissão.

1.4.51.2.8. Legenda perfis de acesso:

1.4.51.2.9. 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.

1.4.51.2.10. Responsável pelas definições: área gestora do sistema.

1.4.51.2.11. Responsável pela Estruturação: quem parametrizou no sistema de gestão de acessos do SPA as permissões dos perfis para o sistema integrado

Disponibilizar relatório com mapeamento com todas as permissões do usuário por sistema que possui acesso, sendo cada sistema na estrutura do item 4.

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.

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.

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.

1.5 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.

ADENDO IX

DECLARAÇÃO DE VISTORIA

A empresa declara, para os devidos fins, que no dia _____/_____/_____, realizou vistoria nas instalações da SUPRO, local onde obteve acesso às informações sobre a infraestrutura de rede de dados e voz do BANPARÁ, bem como obteve todas as informações necessárias para elaboração da proposta que atenda o solicitado no Termo de Referência Edital SUPRO **025**/2022, não encontrando nenhum óbice à execução do objeto.

LOCAL E DATA

Nome:
N.º de identidade:
Órgão Exp.:
Carimbo com razão social e CNPJ:

_____
Assinatura do Representante Legal da Empresa

TERMO DE COMPROVAÇÃO DE VISTORIA

Ref.: **Pregão Eletrônico nº 025/2022 – BANPARÁ**

De acordo com o estabelecido no item 6.7 do Termo de Referência da licitação em referência, declaramos que a empresa_____, representada pelo(s) Sr(s)._____, compareceu à vistoria de que trata o referido item. Nesta oportunidade, o(s) representante(s) exibiu(ram) documento comprobatório de estar(em) credenciado(s) pela empresa interessada.

LOCAL E DATA

_____

(carimbo e assinatura do servidor do BANPARÁ)

ADENDO X

DECLARAÇÃO DE ATENDIMENTO ÀS EXIGÊNCIAS MÍNIMAS

A empresa declara, para os devidos fins, que abre mão da realização de visita técnica pois obteve todas as informações necessárias para elaboração da proposta que atenda o solicitado no Termo de Referência Edital SUPRO **025**/2022, não encontrando nenhum óbice à execução do objeto.

LOCAL E DATA

Nome:
N.º de identidade:
Órgão Exp.:
Carimbo com razão social e CNPJ:

_____
Assinatura do Representante Legal da Empresa

ADENDO XI
DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE SUSTENTABILIDADE

[Nome da Empresa], CNPJ nº_____sediada [Endereço completo], declara sobas penas da lei, que:

I. Não permite 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 fimde que esses também se comprometam no mesmo sentido.

II. 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.

III. 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 implementar esforços nesse sentido junto aos seus respectivos fornecedores.

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

V. Protege e preserva 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.

VI. Desenvolve suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados proteção dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para odisposto 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.

VII. Atende à Política Nacional de Resíduos Sólidos (Lei 12.305/2010), observando quanto ao descarte adequado e ecologicamente correto.

VIII. Apresenta conformidade com a legislação e regulamentos que disciplinam sobre a prevenção e combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo, bem como com a legislação anticorrupção vigente.

IX. Não sofreu sanções que implicam na restrição de participar de licitações ou de celebrar contratos com a Administração Pública, não constar registro da empresa e/ou sócios e representantes no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP) e Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) atendendo às diretrizes anticorrupção.

X. Adota práticas e métodos voltados para a preservação da confidencialidade e integridade, atentando à Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018.

O Banpará poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia

defesa, caso se comprove que a contratada, subcontratados ou fornecedores utilizam-se de trabalhoem desconformidade com as condições referidas nas cláusulas supracitadas.

_____

Local e Data

_____

Nome e Identidade do declarante

ANEXO II - MODELO DE DECLARAÇÃO – CONFORMIDADE AO ART.38 DA LEI Nº 13.303/2016

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

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

Prezados senhores,

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

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

Aplica-se a vedação também:

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

b) empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

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

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

.....
(Local e Data)

.....
(representante legal)

ANEXO 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, n.º 251, Bairro Comércio, CEP. 66.010-000, Belém-PA, inscrito no Ministério da Fazenda sob o CNPJ n.º 04.913.711/0001-08, neste ato representada legalmente pordois de seus Diretores infra-assinados, doravante denominado BANPARÁ e, de outrolado, ..., estabelecida à ....., inscrita no CNPJ sob o nº ....., por seus representantes, infra-assinados, doravante designada simplesmente CONTRATADA, celebram o presente contrato mediante as cláusulas seguintes:

1. CLÁUSULA PRIMEIRA – OBJETO

O presente contrato tem como objeto **Contratação de soluções tecnológicas especializadas de serviços em telecomunicações, contemplando fornecimento de Redes MPLS concomitante ao uso de tecnologia SD-WAN com implantação, configuração, gerenciamento e manutenção da rede de enlaces dedicados para transmissão de dados nos sites remotos, possibilitando conexão de dados através de diferentes tecnologias, incluindo 3G ou superior, visando fornecer conectividade e disponibilidade para as unidades do Banpará espalhadas pelo Estado do Pará e os datacenters localizados em Belém, assim como enlaces de conectividade à rede Internet com solução anti-DDoS nos sites centrais,** conforme especificações, exigências e condições estabelecidas no Edital e seus anexos.

1.1. O presente contrato decorre do processo nº **1321/2021**, realizado pelo edital da licitação do PE nº 025/2022.

2. CLÁUSULA SEGUNDA – ADENDOS

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

Adendo 1 – Edital / Anexos / Termo de Referência

Adendo 2 – Proposta de Preços.

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

Adendo 4 – Termo de Política Anticorrupção.

Adendo 5- Segurança da informação.

Adendo 6- Termo de responsabilidade com as recomendações do código de ética e de conduta do Banpará.

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

3. CLÁUSULA TERCEIRA – PRAZOS

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

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

4 CLÁUSULA QUARTA – VALOR DO CONTRATO E RECURSOS ORÇAMENTÁRIOS

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

LOTE	ITEM	OBJETO	MEIO DE TRANSMISSÃO	BANDA	QTDE	VLR MENSAL	VLR ANUAL
I	01	Enlace de Internet com Anti-DDoS	Fibra óptica	500mbps	2		
	02	Concentrador	Fibra óptica	300mbps	2		
	03	Enlace MPLS/SD-WAN	Fibra óptica	4mbps/ 10mbps	32		

LOTE	ITEM	OBJETO	MEIO DE TRANSMISSÃO	BANDA	QTDE	VLR MENSAL	VLR ANUAL
II	04	Concentrador	Fibra óptica	300mbps	2		
	05	Enlace MPLS/SD-WAN	Satélite Banda Ku	4mbps uplink 1mbps downlink	50		

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

5 CLÁUSULA QUINTA – GARANTIA

5.1 Para garantia do fiel e perfeito cumprimento de todas as obrigações ora ajustadas, a CONTRATADA deve, dentro de 10 (dez) dias úteis, contados a partir da assinatura do contrato, apresentar garantia ao BANPARÁ, no valor equivalente a 5% (cinco por cento) do valor total desta contratação, que deve cobrir o período de execução do contrato e estender-se até 3 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação contratual e complementada em casos de aditivos e apostilas para reajustes.

5.1.1 A CONTRATADA deve prestar garantia numa das seguintes modalidades:

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

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

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

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

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

b) Caução em dinheiro, valor **depositado** pela CONTRATADA, no Banco ....., Agência ....., Conta Corrente n. ....., em nome do BANPARÁ. A cópia do recibo será entregue ao gestor do contrato.

c) Seguro Garantia feito junto à **entidade** com situação regular no mercado de seguros do Brasil para análise e aceitação por parte do BANPARÁ.

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

a) Prejuízos advindos do não cumprimento ou do cumprimento irregular do objeto do presente contrato;

b) Prejuízos diretos causados ao BANPARÁ decorrentes de culpa ou dolo durante a execução do contrato;

c) Multas moratórias e compensatórias aplicadas pelo BANPARÁ à CONTRATADA; e

d) Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

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

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

a) Promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações; ou

b) Reter o valor da garantia dos pagamentos eventualmente devidos à CONTRATADA até que a garantia seja apresentada.

5.3 A garantia deve ser considerada extinta:

a) Com a devolução da apólice, carta-fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do BANPARÁ, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato; ou

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

6 CLÁUSULA SEXTA – EXECUÇÃO DO CONTRATO

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

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

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

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

6.4 A gestão do presente contrato deve ser realizada pela área técnica do BANPARÁ. A gestão do contrato abrange o encaminhamento de providências, devidamente instruídas e motivadas, identificadas em razão da fiscalização da execução do contrato, suas alterações, aplicação de sanções, rescisão contratual e outras medidas que importem disposição sobre o contrato.

6.5 A fiscalização da execução do presente contrato será realizada por agentes de fiscalização, que devem ser designados pelo gestor do contrato, permitindo-se

designar mais de um empregado e atribuir-lhes funções distintas, como a fiscalização administrativa e técnica, consistindo na verificação do cumprimento das obrigações contratuais por parte da CONTRATADA, com a alocação dos recursos, pessoal qualificado, técnicas e materiais necessários.

6.6 O gestor do contrato pode suspender a sua execução em casos excepcionais e motivados tecnicamente pelo fiscal técnico do contrato, devendo comunicá-la ao preposto da CONTRATADA, indicando:

a) O prazo da suspensão, que pode ser prorrogado, se as razões que a motivaram não estão sujeitas ao controle ou à vontade do gestor do contrato;

b) Se deve ou não haver desmobilização, total ou parcial, e quais as atividades devem ser mantidas pela CONTRATADA;

c) O montante que deve ser pago à CONTRATADA a título de indenização em relação a eventuais danos já identificados e o procedimento e metodologia para apurar valor de indenização de novos danos que podem ser gerados à CONTRATADA.

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

6.7.1 Verificada eventual situação de descumprimento das condições de habilitação, o CONTRATANTE pode conceder prazo para que a CONTRATADA regularize suas obrigações ou sua condição de habilitação, conforme disposto no Art. 95, itens 5 e 6 do Regulamento, quando não identificar má fé ou incapacidade da CONTRATADA corrigir tal situação.

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

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

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

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

evitar ou impedir. Essa exoneração de responsabilidade deve produzir efeitos nos termos do parágrafo único do artigo 393 do Código Civil Brasileiro.

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

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

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

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

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

E-mail BANPARÁ - .....

E-mail CONTRATADA - .....

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

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

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

7 CLÁUSULA SÉTIMA – RECEBIMENTO

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

8 CLÁUSULA OITAVA – CONDIÇÕES DE FATURAMENTO E PAGAMENTO

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

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

8.3 As faturas que apresentarem erros ou cuja documentação suporte esteja em desacordo com o contratualmente exigido devem ser devolvidas à CONTRATADA pela unidade de gestão de contrato do BANPARÁ para a correção ou substituição. O BANPARÁ, por meio da unidade de gestão de contrato, deve efetuar a devida comunicação à CONTRATADA dentro do prazo fixado para o pagamento. Depois de apresentada a Nota Fiscal/Fatura, com as devidas correções, o prazo previsto no subitem acima deve começar a correr novamente do seu início, sem que nenhuma atualização ou encargo possa ser imputada ao BANPARÁ.

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

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

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

8.7 Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo BANPARÁ, incidirá sobre os valores em atraso juros de mora no percentual de 1% (um por cento) ao mês, *pro rata die*, calculados de forma simples

sobre o valor em atraso e devidos a partir do dia seguinte ao do vencimento até a data da efetiva liquidação do débito.

9 CLÁUSULA NONA – DA INEXISTÊNCIA DE VÍNCULO EMPREGATÍCIO

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

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

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

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

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

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

10 CLÁUSULA DEZ – ALTERAÇÕES INCIDENTES SOBRE O OBJETO DO CONTRATO

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

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

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

b) Deve ser mantida a diferença, em percentual, entre o valor global do contrato e o valor orçado pelo BANPARÁ, salvo se o fiscal técnico do contrato

apontar justificativa técnica ou econômica, que deve ser ratificada pelo gestor do contrato;

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

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

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

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

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

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

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

10.2 As alterações incidentes sobre o objeto devem ser:

a) Instruídas com memória de cálculo e justificativas de competência do fiscal técnico e do fiscal administrativo do BANPARÁ, que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites;

b) As justificativas devem ser ratificadas pelo gestor do contrato do BANPARÁ; e

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

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

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

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

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

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

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

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

11 CLÁUSULA ONZE – EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO

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

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

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

11.2 Os valores contratados serão reajustados anualmente, a contar da data de assinatura deste contrato, no prazo da lei, segundo o IPCA (Índice Nacional de Preços ao Consumidor Amplo), ou outro, na falta deste, que estiver estabelecido na legislação à época de cada reajuste.

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

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

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

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

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

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

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

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

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

12 CLÁUSULA DOZE – RESCISÃO

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

12.2 A parte que pretende a rescisão deve avaliar e responder motivadamente a manifestação referida no subitem precedente no prazo de 5 (cinco) dias úteis, comunicando a outra parte, na forma prevista neste contrato, considerando-se o contrato rescindido com a referida comunicação.

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

a) Impactos econômicos e financeiros decorrentes do atraso na fruição dos benefícios do empreendimento;

b) Riscos sociais, ambientais e à segurança da população local decorrentes do atraso na fruição dos benefícios do empreendimento;

c) Motivação social e ambiental do empreendimento;

d) Custo da deterioração ou da perda das parcelas executadas;

e) Despesa necessária à preservação das instalações e dos serviços já

executados;

f) Despesa inerente à desmobilização e ao posterior retorno às atividades;

g) Possibilidade de saneamento dos descumprimentos contratuais;

h) Custo total e estágio de execução física e financeira do contrato;

i) Empregos diretos e indiretos perdidos em razão da paralisação do contrato;

j) Custo para realização de nova licitação ou celebração de novo contrato;

k) Custo de oportunidade do capital durante o período de paralisação.

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

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

13 CLÁUSULA TREZE – SANÇÕES ADMINISTRATIVAS

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

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

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

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

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

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

e) Praticar ato fraudulento na execução do contrato;

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

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

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

b) Caracterizada a má-fé ou intenção desonesta, a pena base deve ser de 1 (um)

ano e a pena mínima deve ser de 6 (seis) meses, mesmo aplicando as atenuantes previstas.

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

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

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

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

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

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

c) em 1/4 (um quarto), se a CONTRATADA tiver reconhecido a falta e se dispuser a tomar medidas para corrigi-la; e

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

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

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

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

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

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

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

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

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

14 CLÁUSULA CATORZE – RESPONSABILIZAÇÃO ADMINISTRATIVA POR ATOS LESIVOS AO BANPARÁ

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

a) Fraudar o presente contrato;

b) Criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o contrato;

c) Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações deste contrato, sem autorização em lei, no ato convocatório da licitação pública ou neste instrumento contratual;

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

e) Realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei n. 12.846/2013, Decreto n. 8.420/2015, Lei n. 8.666/1993, ou de quaisquer outras leis ou regulamentos aplicáveis, ainda que não relacionadas no presente contrato.

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

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

b) Publicação extraordinária da decisão condenatória.

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

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

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

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

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

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

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

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

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

14.3.2 Caso os atos lesivos apurados envolvam infrações administrativas à Lei n. 8.666/1993, ou a outras normas de licitações e contratos da administração pública, e tenha ocorrido a apuração conjunta, o licitante também estará sujeito a sanções administrativas que tenham como efeito restrição ao direito de participar em licitações ou de celebrar contratos com a administração pública, a serem aplicadas no PAR.

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

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

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

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

14.5 As disposições deste subitem se aplicam quando o licitante se enquadrar na definição legal do parágrafo único do artigo 1º da Lei n. 12.846/2013.

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

15 CLÁUSULA QUINZE – PUBLICIDADE E CONFIDENCIALIDADE

15.1 Quaisquer informações relativas ao presente contrato, somente podem ser dadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, após autorização, por escrito, do BANPARÁ. Para os efeitos desta Cláusula, deve ser formulada a solicitação, por escrito, ao BANPARÁ, informando todos os pormenores da intenção da CONTRATADA, reservando-se, ao BANPARÁ, o direito de aceitar ou não o pedido, no todo ou em parte.

16 CLÁUSULA DEZESSEIS – DAS PRÁTICAS ANTICORRUPÇÃO E DE PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO

16.1 As PARTES se obrigam, sob as penas previstas no CONTRATO e na legislação aplicável, a analisar e cumprir rigorosamente todas as leis cabíveis, abrangendo, mas não se limitando à legislação brasileira anticorrupção e a legislação brasileira de prevenção à lavagem de dinheiro e financiamento do terrorismo.

16.2 As PARTES afirmam e garantem que não estão envolvidas ou irão se envolver, direta ou indiretamente, por meio de seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, partes relacionadas, durante o cumprimento das obrigações previstas no Contrato, em qualquer atividade ou prática que constitua uma infração aos termos das leis anticorrupção e de prevenção a lavagem de dinheiro e financiamento do terrorismo.

16.3 As PARTES afirmam e garantem que não se encontram, assim como seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, direta ou indiretamente (i) sob investigação em virtude de denúncias de suborno e/ou corrupção; (ii) no curso de um processo judicial e/ou administrativo ou foi condenada ou indiciada sob a acusação de corrupção ou suborno; (iii) suspeita de práticas de terrorismo e/ou lavagem de dinheiro por qualquer entidade governamental; e (iv) sujeita às restrições ou sanções econômicas e de negócios por qualquer entidade governamental.

16.4 A CONTRATADA afirma que, direta ou indiretamente, não ofereceu, prometeu, pagou ou autorizou o pagamento em dinheiro, deu ou concordou em dar presentes ou qualquer objeto de valor e, durante a vigência do Contrato, não irá ofertar, prometer, pagar ou autorizar o pagamento em dinheiro, dar ou concordar em dar presentes ou qualquer objeto de valor a qualquer pessoa ou

entidade, pública ou privada, com o objetivo de beneficiar ilicitamente a CONTRATANTE e/ou seus negócios.

16.5 A CONTRATADA afirma que, direta ou indiretamente, não irá receber, transferir, manter, usar ou esconder recursos que decorram de qualquer atividade ilícita, bem como não irá contratar como empregado ou de alguma forma manter relacionamento profissional com pessoas físicas ou jurídicas envolvidas em atividades criminosas, em especial pessoas investigadas pelos delitos previstos nas leis anticorrupção, de lavagem de dinheiro, tráfico de drogas e terrorismo.

16.6 A CONTRATADA se obriga a notificar prontamente, por escrito, à CONTRATANTE a respeito de qualquer suspeita ou violação do disposto nas leis anticorrupção e ainda de participação em práticas de suborno ou corrupção, assim como o descumprimento de qualquer declaração prevista nestas Cláusulas.

16.7 A CONTRATADA afirma e garante que (i) os atuais representantes da CONTRATADA não são funcionários públicos ou empregados do governo; e que (ii) informará por escrito, no prazo de 3 (três) dias úteis, qualquer nomeação de seus representantes como funcionários públicos ou empregados do governo. A CONTRATANTE poderá, a seu exclusivo critério, rescindir o CONTRATO, caso a CONTRATADA realize referida nomeação nos termos do item "ii" acima, sendo que, neste caso, não serão aplicáveis quaisquer multas ou penalidades à CONTRATANTE pela rescisão do CONTRATO, devendo a CONTRATADA responder por eventuais perdas e danos.

16.8 A CONTRATADA se obriga a cumprir e respeitar o código de ética e a política institucional de prevenção a lavagem de dinheiro e financiamento do terrorismo da CONTRATANTE ("Código de Ética" e "Política de PLD_FT), o qual declara conhecer. O Código de Ética deve ser solicitado pela CONTRATADA à CONTRATANTE.

16.9 Qualquer descumprimento das disposições de Anticorrupção, em qualquer um dos seus aspectos, ensejará a rescisão motivada do presente instrumento, independentemente de qualquer notificação, observadas as penalidades previstas neste Contrato, bem como facultará à parte faltosa o ressarcimento, perante a parte inocente, de todo e qualquer dano suportado em função do referido descumprimento

17 CLÁUSULA DEZESSETE – DO TRATAMENTO DE DADOS

17.1. Definições: Para fins de cláusulas, serão utilizadas as definições conforme disposto na Lei Geral de Proteção de Dados, Lei Nº 13.709/2018, no artigo 5º e seus incisos:

a) Dados pessoais é toda informação relacionada a pessoa natural identificada ou identificável;

b) Dados pessoais sensíveis é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

c) Titular de dados é toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

d) Controlador é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

e) Operador é toda pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

f) Encarregado é pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

g) Tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

17.2 Em complemento às definições supra, as Partes reconhecem que os dados pessoais a que este instrumento se refere tratam-se dos dados de produção da CONTRATANTE, inseridos em seus sistemas.

17.3 **Escopo/Objeto:** Este Contrato de processamento de dados se aplica exclusivamente ao processamento de dados pessoais que está sujeito à Lei Geral de Proteção de Dados (LGPD) entre as partes, durante a vigência do contrato para a prestação dos seguintes serviços: Fornecimento de soluções tecnológicas especializadas de serviços em telecomunicações, contemplando fornecimento de Redes MPLS concomitante ao uso de tecnologia SD-WAN com implantação, configuração, gerenciamento e manutenção da rede de enlaces dedicados para transmissão de dados nos sites remotos, possibilitando conexão de dados através de diferentes tecnologias, incluindo 3G ou superior, visando fornecer conectividade e disponibilidade para as unidades do Banpará espalhadas pelo Estado do Pará e os datacenters localizados em Belém, assim como enlaces de conectividade à rede Internet com solução anti-DDoS nos sites centrais.

17.4. **Das Responsabilidades e Obrigações da Contratante:** A CONTRATANTE obriga-se a não transmitir ou compartilhar com a CONTRATADA qualquer dado pessoal que não tenha sido previamente anonimizado ou pseudoanonimizado, ficando a cargo da CONTRATANTE a escolha da técnica de descaracterização a ser empregada em cada caso, desde que a sua aplicação prática impossibilite à CONTRATADA identificar ou reidentificar os seus respectivos titulares.

17.4.1. A CONTRATADA não tratará os dados pessoais provenientes da CONTRATANTE sem que estes estejam devidamente descaracterizados, não podendo ser imputadas à CONTRATADA, em casos tais, as consequências do descumprimento do SLA contratado ou, ainda, de outros indicadores de inadimplemento das obrigações pactuadas, quando o atraso na prestação dos serviços originar-se na inobservância, pela CONTRATADA, da referida regra de segurança.

17.4.2. Caso sejam enviados dados não descaracterizados à CONTRATADA, esta os excluirá de seus sistemas e arquivos, informando o fato à CONTRATANTE para que seja providenciada a anonimização ou a pseudoanonimização dos mesmos antes de encaminhá-los novamente à CONTRATADA.

17.4.3. A CONTRATADA não é responsável pela descaracterização dos dados da CONTRATANTE em seu próprio ambiente, tampouco pelo fornecimento de scripts ou de ferramentas de anonimização ou criptografia à CONTRATANTE, serviço este cuja prestação, se desejada, dependerá de negociação e precificação apartadas, salvo acordo em contrário celebrado entre as Partes.

17.5. Caso o acesso a dados pessoais não anonimizados seja indispensável para a prestação dos serviços, a CONTRATADA dará ciência deste fato à CONTRATANTE para que as providências necessárias à segurança da operação sejam previamente adotadas por ambas as Partes, incluindo a assinatura de termos específicos de confidencialidade, caso necessário.

17.5.1. Somente serão compartilhados com a CONTRATADA os dados pessoais mínimos e imprescindíveis para a prestação satisfatória do serviço contratado, os quais serão determinados pela CONTRATADA e indicados à CONTRATANTE, por escrito, acompanhado da devida justificativa, quando solicitado.

17.5.2. A transmissão de dados pessoais entre as Partes deverá ocorrer de forma encriptada, sempre que possível, e por meios seguros que sejam capazes de assegurar níveis adequados de proteção aos dados em trânsito, a exemplo dos protocolos HTTPS, SFTP, FTP, FTPS ou outros assemelhados.

17.5.3. Com o objetivo de conferir proteção adequada aos dados pessoais, as Partes comprometem-se a utilizar, para toda e qualquer comunicação, a ferramenta de chamados por ela disponibilizada para a realização de atendimentos, sem prejuízo do emprego de outros meios comprovadamente mais seguros, mediante mútuo acordo.

17.5.4. A utilização de e-mails para transitar dados pessoais e demais informações sigilosas entre as Partes é vedada no âmbito do Contrato, salvo em hipóteses excepcionais ou emergenciais, devidamente justificadas, e desde que sejam empregadas ferramentas adicionais de criptografia de dados em e-mail.

17.5.5. Fica proibido, no âmbito do Contrato, o uso de aplicativos de mensagens instantâneas para transitar dados pessoais, estejam eles instalados em equipamentos pessoais ou corporativos.

17.5.6. A CONTRATANTE deverá orientar e fiscalizar os seus colaboradores para que estes cumpram com os deveres de segurança relativos a dados pessoais, tanto aqueles previstos neste Acordo quanto em seus

normativos internos, evitando a transmissão de dados desnecessários e em excesso à CONTRATADA, bem como a utilização de formas de transmissão dessas informações que não ofereçam a segurança adequada ao trânsito e à recepção das mesmas.

17.5.7. Caso a CONTRATANTE transmita à CONTRATADA dados em excesso, além daqueles indicados como sendo suficientes à execução do serviço, ou, ainda, promova o trânsito de dados pessoais por meios inseguros e/ou expressamente proibidos por este instrumento, incorrerá exclusivamente em todos os riscos advindos de tais operações.

17.6. A CONTRATANTE não permitirá o acesso da CONTRATADA aos seus ambientes sem a devida descaracterização dos dados neles localizados. A CONTRATADA não deverá ter acesso ao ambiente de produção da CONTRATANTE, ficando limitada a sua atuação somente ao ambiente de homologação.

17.6.1. Quando for imprescindível à execução do Contrato, esta poderá ter acesso ao ambiente de produção da CONTRATANTE, mediante autorização prévia. Nessa hipótese, tanto a supervisão das atividades quanto a assinatura dos termos de responsabilidade e confidencialidade serão obrigatórias e condicionarão a prestação dos serviços.

17.6.2. O acesso da CONTRATADA aos ambientes da CONTRATANTE deverá ocorrer sempre de forma assistida, mediante a concessão de credenciais (login e senha) individuais, tantos quantos forem os colaboradores da CONTRATADA envolvidos na prestação do serviço.

17.7. Com relação aos dados pessoais tratados no âmbito do Contrato, a CONTRATANTE obriga-se a:

a) Garantir que as operações de tratamento de dados delegadas à CONTRATADA pela via contratual sejam lícitas do ponto de vista da autorização legal para o processamento, assegurando, assim, a subsunção a uma das hipóteses legais de tratamento elencadas no artigo 7º ou 11 da Lei Geral de Proteção de Dados, a depender do caráter sensível ou não das informações;

b) Observar e respeitar, em sua relação com a CONTRATADA, os princípios da finalidade, da adequação e da minimização dos dados pessoais, disponibilizando à CONTRATADA as informações que sejam estritamente necessárias à execução do Contrato;

c) Sempre que a base legal eleita para legitimar o tratamento de dados pessoais for o consentimento do titular dos dados (artigo 7º, I, LGPD), a CONTRATANTE será a única e exclusiva responsável pela coleta das autorizações, bem como por sua posterior gestão e garantia de sua validade, especialmente quando se tratar de dados pessoais sensíveis, nos termos da Lei;

d) Em havendo tratamento de dados de crianças e adolescentes, a CONTRATANTE será a única e exclusiva responsável por assegurar que o processamento se dará no melhor interesse do menor, bem como por obter o

consentimento específico e em destaque dado por um dos pais ou pelo responsável legal, empreendendo esforços razoáveis para verificar que essa autorização foi dada pelo efetivo responsável pela criança;

e) Observar e respeitar os princípios da informação e da transparência, provendo os titulares dos dados de conhecimento suficiente e apto a possibilitar a identificação dos agentes de tratamento, as atividades realizadas com os dados e a plena compreensão da extensão dos seus direitos e das maneiras de exercê-los.

17.8. A CONTRATANTE, ainda que pela via regressiva, responsabilizar-se-á pelas sanções administrativas e pelos danos originados em tratamentos de dados por ela realizados em desconformidade com a legislação de proteção de dados, especialmente no que concerne à satisfação dos requisitos legais e regulatórios para o processamento lícito dessas informações.

17.9. A CONTRATANTE é a única responsável pelo atendimento das solicitações e requisições feitas pelos titulares de dados pessoais, relativamente aos dados tratados pelas Partes por força do Contrato, as quais representem o exercício de direitos elencados na LGPD, não podendo exigir da CONTRATADA, em nenhuma hipótese, que o faça em seu lugar ou que se responsabilize pelo descumprimento dessa obrigação legal.

17.10. **Das Responsabilidades e Obrigações da Contratada:** A CONTRATADA, quando necessário à execução do Contrato, realizará o tratamento dos dados pessoais compartilhados pela CONTRATANTE em observância ao disposto na Lei nº 13.709/2018 e em outras leis de privacidade e proteção de dados aplicáveis, seguindo, ainda, as instruções lícitas fornecidas pela CONTRATANTE para a condução das atividades de processamento.

17.10.1. A CONTRATADA processará os dados pessoais somente sob as instruções expressas da CONTRATANTE, de maneira que – e na medida em que – seja apropriado para a prestação dos serviços, exceto quando necessário para cumprir uma obrigação legal. Nesse caso, a CONTRATADA deverá informar à CONTRATANTE dessa obrigação legal, preferencialmente antes de realizar o processamento, a menos que essa obrigação legal proíba o fornecimento de tais informações à CONTRATADA.

17.10.2. A CONTRATADA nunca deverá processar os dados pessoais de maneira inconsistente com as instruções expressas da CONTRATANTE.

17.10.3. A CONTRATANTE obriga-se a não transmitir à CONTRATADA orientações que inviabilizem o tratamento de dados pessoais, consideradas, em especial, as limitações de ordem técnica existentes à época do processamento e ao estado da arte então vigente.

17.10.4. Caso a CONTRATADA considere qualquer das instruções passadas pela CONTRATANTE como sendo contrárias à Lei Geral de Proteção de Dados Pessoais ou a outros diplomas normativos afetos ao tema, inclusive de abrangência setorial, deverá notificar imediatamente o fato à CONTRATANTE, para que esta preste os esclarecimentos necessários e tome

as providências que julgar cabíveis, dando novas orientações à CONTRATADA ou reforçando aquelas anteriormente veiculadas, de forma fundamentada.

17.10.5. A CONTRATADA não será obrigada a executar diretrizes manifestamente ilícitas, o que deverá ser informado por escrito à CONTRATANTE. Caso seja exigido o cumprimento da ordem, será facultado à CONTRATADA rescindir o Contrato de imediato, sem quaisquer ônus ou penalidades.

17.10.6. A CONTRATANTE é a única responsável pela licitude dos comandos transmitidos à CONTRATADA para o tratamento de dados pessoais e responderá pelas sanções cíveis e administrativas decorrentes de desconformidades relacionadas direta ou reflexamente às ordens impostas à CONTRATADA, arcando, ainda, com a reparação dos danos causados à CONTRATADA ou a terceiros.

17.11. As orientações transmitidas pela CONTRATANTE versarão sobre os aspectos essenciais do tratamento de dados, a exemplo da seleção das operações a serem realizadas com os dados pessoais compartilhados, em qual tempo e/ou periodicidade e em que condições. A escolha dos meios e ferramentas técnicas para fazê-lo ficará a cargo da CONTRATADA, a qual detém expertise em tecnologia e segurança da informação.

17.11.1. Em qualquer caso, os deveres da CONTRATADA enquanto Operadora de dados estarão condicionados às limitações técnicas existentes à época do processamento e ao estado da arte então vigente. A evolução da tecnologia e as suas consequências sobre os padrões de segurança e confidencialidade do mercado não tornarão desconforme o tratamento realizado pela CONTRATADA até então e não autorizarão a sua penalização a qualquer título.

17.11.2. Para os fins deste Acordo, as Partes reconhecem que, quando o esforço operacional e/ou financeiro inerente ao emprego de determinadas técnicas ou ferramentas tecnológicas for excessivamente oneroso para a CONTRATADA, considerados fatores como investimento, tempo e risco da operação, tal óbice será considerado como análogo a uma limitação técnica. Em casos tais, meios alternativos deverão ser empregados para assegurar o tratamento lícito de dados pessoais, sem prejuízo de revisões futuras acerca da utilização de novas tecnologias disponíveis no mercado.

17.12. A CONTRATADA deverá fornecer à CONTRATANTE documentação relevante, necessária e suficiente para a verificação da observância de diretrizes relativas à proteção de dados, como, por exemplo, a sua política de privacidade, política de gerenciamento de registros, código de conduta aprovado, política de segurança da informação, plano de continuidade de negócio, documentação com regras para tratamento de dados sensíveis, tanto para transporte como repouso, além do relatório de incidentes envolvendo a CONTRATANTE. A entrega de tais documentos ficará condicionada à sua efetiva disponibilidade, bem como às normas internas da CONTRATADA sobre sigilo e confidencialidade documental, respeitados, em qualquer caso, os seus segredos comerciais e de negócios. Toda a documentação

deverá ser disponibilizada anualmente, no mínimo, e deverá ser entregue em até 15 (quinze) dias contados da solicitação formal feita à CONTRATADA.

17.13. O tratamento dos dados pessoais recebidos ou acessados pela CONTRATADA em função do Contrato destinar-se-á a possibilitar a execução do seu objeto, tendo como finalidade viabilizar o desempenho das atividades inerentes à boa performance contratual.

17.14. Caso a CONTRATADA venha a executar tratamento diferente daquele definido pela CONTRATANTE, desviando-se das instruções por ela transmitidas para o tratamento de dados e utilizando-os em proveito próprio, aquela será alçada à condição de Controladora e terá as mesmas responsabilidades.

17.15. Sem prejuízo de quaisquer acordos contratuais existentes entre as Partes, a CONTRATADA tratará todos os dados pessoais como estritamente confidenciais e informará todos os seus funcionários, agentes e/ou suboperadores aprovados [se permitido] envolvidos no processamento de dados pessoais de natureza confidencial de tais informações.

17.16. A CONTRATADA deverá garantir que todas essas pessoas ou partes tenham assinado um instrumento de confidencialidade apropriado e estejam vinculadas a um dever de confidencialidade ou estejam sob uma obrigação estatutária apropriada de confidencialidade. A qualquer momento a CONTRATANTE poderá solicitar a prestação de contas sobre tal ato.

17.17. A CONTRATADA deverá garantir que as informações confidenciais deverão ser utilizadas apenas para os propósitos do Contrato nº 119/2017, e que serão divulgadas apenas para seus Diretores, Sócios, Administradores, Empregados, Prestadores de Serviço, Preposto ou quaisquer representantes, respeitando o princípio do privilégio mínimo, com a devida classificação de informação, conforme disposto na ISO/IEC 27002:2005 (ABNT NBR).

17.18. A CONTRATADA não poderá divulgar, publicar ou de qualquer forma revelar qualquer informação CONFIDENCIAL, RESTRITA, SENSÍVEL ou INTERNA recebida da CONTRATANTE para qualquer pessoa física ou jurídica, de direito público ou privado, sem a prévia autorização escrita da CONTRATANTE.

17.19. Quaisquer informações relativas ao presente acordo de **TRATAMENTO DE DADOS** somente poderão ser levadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, mediante requisição por escrito a ser encaminhada para avaliação da CONTRATANTE, informando todas as minúcias da intenção da CONTRATADA, reservando-se àquela o direito de deferir ou não o pedido, no todo ou em parte.

17.20. A CONTRATANTE poderá solicitar à CONTRATADA, a qualquer momento, o retorno de todas as **INFORMAÇÕES SIGILOSAS** recebidas pelo **OPERADOR** de forma escrita ou tangível, incluindo cópias, reproduções ou outra mídia contendo tais informações, dentro de um período máximo de 10 (dez) dias a contar da formalização do pedido.

17.21. A CONTRATADA deverá dar ciência das referidas cláusula a todos os seus sócios, empregados, prestadores de serviço, prepostos ou quaisquer representantes que participarão do tratamento de dados descritos no contrato e que venham a ter acesso a quaisquer dados e informações **CONFIDENCIAIS, RESTRITAS, SENSÍVEIS** ou **INTERNA** do **CONTROLADOR** para que cumpram as obrigações constantes neste documento.

17.22. Levando em consideração o estado da arte, os custos de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como o risco de probabilidades e severidade variáveis dos direitos e liberdades das pessoas físicas, sem prejuízo de outras normas de segurança agredido pelas Partes, CONTRATANTE e CONTRATDA deverão implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança no processamento de dados pessoais apropriado ao risco. Essas medidas devem procurar garantir que:

a) Os dados podem ser acessados, alterados, divulgados ou excluídos apenas com autorização da CONTRATANTE;

b) Os dados permaneçam precisos e completos em relação à finalidade pela qual estão sendo tratados;

c) Os dados permaneçam acessíveis e utilizáveis, ou seja, se os dados pessoais forem acidentalmente perdidos, alterados ou destruídos, deverá ser garantida a recuperação dos mesmos, evitando qualquer dano às partes envolvidas.

17.23. A CONTRATADA informará imediatamente a CONTRATANTE se houver a necessidade de transferência internacional de dados pessoais para a execução do contrato. A remessa dos dados pessoais para fora do território nacional somente poderá ocorrer mediante autorização da CONTRATANTE.

17.24. Quando a CONTRATADA tomar conhecimento de um incidente que afeta o processamento dos dados pessoais que está sujeito ao Contrato de Serviços, deverá notificar prontamente a CONTRATANTE sobre o mesmo, sem demora injustificada, devendo sempre cooperar com a CONTRATANTE e seguir as suas instruções em relação a esses incidentes, a fim de permitir que a CONTRATANTE realize uma investigação completa sobre o incidente, formule uma resposta correta e tome as medidas adequadas a respeito do incidente.

17.25. Ao relatar uma violação, o **OPERADOR** deverá fornecer ao **CONTROLADOR**:

a) Uma descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares de dados em causa;

b) O nome e os detalhes de contato do responsável pela proteção de dados ou outro ponto de contato onde mais informações possam ser obtidas;

c) Uma descrição das prováveis consequências da violação de dados pessoais;

d) Uma descrição das medidas adotadas, ou propostas a serem adotadas, para lidar com a violação de dados pessoais, incluindo, se for o caso, as medidas adotadas para mitigar possíveis efeitos adversos.

17.26. O **OPERADOR** não deverá subcontratar para nenhuma de suas atividades relacionadas ao serviço que consistam, mesmo que parcialmente, no processamento de dados pessoais ou na exigência de que os dados pessoais sejam processados por terceiros sem a autorização prévia e por escrito do **CONTROLADOR**.

17.27. Após a rescisão deste Contrato de Tratamento de Dados, mediante solicitação por escrito da CONTRATANTE ou após o cumprimento de todos os propósitos acordados no contexto dos Serviços, nos quais nenhum processamento adicional é necessário, a CONTRATADA deverá, a critério da CONTRATANTE, excluir, destruir ou devolver todos os dados pessoais a esta, bem como destruir ou devolver quaisquer cópias existentes, a menos que exista alguma obrigação legal que exija que os dados pessoais permaneçam armazenados.

17.27.1. Os dados deverão ser restituídos e excluídos em até 30 (trinta) dias ou em outro prazo acordado entre as Partes.

17.27.2. Não sendo possível a exclusão dos dados, a CONTRATADA procederá à anonimização dos mesmos, o que será informado com antecedência à CONTRATANTE.

17.27.3. A CONTRATADA deverá emitir documento ratificando que todos os dados pessoais foram devolvidos ou descartados. Todas as atividades de devolução ou descarte de dados não devem gerar ônus à CONTRATANTE, observada a razoabilidade das medidas.

17.27.4. Todos os dados compartilhados por força do Contrato são de propriedade da CONTRATANTE.

17.28. A CONTRATADA deverá auxiliar a CONTRATANTE, por medidas técnicas e organizacionais apropriadas, naquilo que lhe couber e na medida do possível, sempre à luz do escopo e objeto do contrato, para o cumprimento das suas obrigações enquanto Controladora de responder à solicitação de exercício dos direitos dos titulares de dados sobre a Lei Geral de Proteção de Dados, como solicitações de acesso, solicitações de retificação ou descarte de dados pessoais e objeções ao tratamento.

17.28.1. Em nenhuma hipótese a CONTRATADA assumirá a condição de destinatária dos deveres correlatos aos direitos dos titulares de dados, ficando afastadas quaisquer penalidades oriundas de sua violação.

17.28.2. Na eventualidade de a CONTRATADA ser acionada diretamente pelo titular de dados, esta orientará o solicitante a realizar o pleito junto à Controladora, dando-se ciência ao titular das informações de contato do responsável pelo tratamento da LGPD na estrutura da CONTRATANTE, quando a disponibilização dessas informações à CONTRATADA tenha ocorrido previamente.

17.29. A CONTRATADA deverá auxiliar a CONTRATANTE, naquilo que lhe couber e for possível, sempre à luz do escopo e objeto do contrato, a garantir o cumprimento das obrigações previstas nas cláusulas de segurança e nas consultas realizadas pela Autoridade Nacional de Proteção de Dados, levando em consideração a natureza do processamento e as informações disponíveis para a CONTRATANTE.

17.29.1. Em nenhuma hipótese a CONTRATADA ficará responsável pela elaboração de quaisquer documentos que sejam exigidos do Controlador, tampouco pela adoção de medidas de remediação a eles relacionadas, incluindo, mas não se limitando a apresentação do Relatório de Impacto à Proteção de Dados Pessoais à Agência Nacional de Proteção de Dados (ANPD) ou a outro órgão público, a prestação de esclarecimentos ou informações a essas mesmas autoridades e o envio da Notificação de Incidente de Dados à ANPD ou aos titulares de dados.

17.30. O **OPERADOR** deverá cumprir com as suas obrigações de manter os dados pessoais seguros, notificar violações de dados pessoais ao **CONTROLADOR** e realizar avaliações de impacto na proteção de dados pessoais sobre as suas atividades de processamento, quando a Lei assim exigir.

17.31. Cada Parte, ainda que pela via regressiva, responsabilizar-se-á pelas sanções administrativas e pelos danos diretos originados em tratamentos de dados por ela realizados em desconformidade com este Acordo e/ou com as leis de proteção de dados, especialmente no que concerne à satisfação dos requisitos legais e regulatórios para o processamento lícito dessas informações.

17.31.1. O dever de indenização de uma Parte em relação à outra, em razão de demandas judiciais ou administrativas, abrangerá os valores que tiverem sido incorridos pela Parte Prejudicada com a demanda, o que abrange todas as custas processuais em que comprovadamente tenha incorrido e os valores desembolsados a título de indenização, limitado ao valor global do Contrato, entendido este como sendo o somatório das 12 (doze) últimas parcelas pagas ao prestador de serviços.

17.31.2. A responsabilidade da Parte e a reparação ou ressarcimento por ela devido será proporcional à sua efetiva participação no evento ilícito ou lesivo e ficará adstrita à comprovação da irregularidade e/ou do dano, decorrentes de condutas que lhe sejam atribuíveis a título de dolo ou culpa, por sentença judicial transitada em julgado.

17.31.3. Fica assegurado às Partes, nos termos da Lei, o direito de regresso.

17.32. A CONTRATADA deverá fornecer à CONTRATANTE todas as informações necessárias para demonstrar o cumprimento das medidas técnicas de proteção de dados pessoais.

17.33. A CONTRATADA deverá permitir e contribuir para auditorias e diligências realizadas pela CONTRATANTE ou por um auditor nomeado por este, mediante notificação prévia encaminhada com antecedência mínima de 05 (cinco) dias úteis. Os métodos usados para monitorar a conformidade e a frequência do monitoramento dependerão das circunstâncias do processamento e serão definidas pela CONTRATADA, desde que razoáveis.

17.33.1. Qualquer diligência realizada no âmbito da auditoria deverá necessariamente guardar pertinência com a verificação do adimplemento das disposições deste Acordo, sob pena de ser indeferida pela CONTRATADA. Em nenhuma hipótese a CONTRATANTE ou quem a represente poderá ter acesso a informações relativas a outros clientes da CONTRATADA, devendo ser respeitados, ainda, os seus segredos comerciais e/ou de negócios.

17.33.2. A realização da auditora será condicionada à assinatura de Termos de Confidencialidade específicos pelos colaboradores, contratados ou representantes da CONTRATANTE.

17.33.3. As informações coletadas durante a diligência deverão ser utilizadas exclusivamente para fins de inspeção ou auditoria, devendo a CONTRATANTE mantê-las sob sigilo enquanto estiverem em seu poder e excluí-las em definitivo, após o encerramento dos trabalhos, encaminhando à CONTRATADA as evidências apropriadas de que o fez.

17.34. O presente Contrato não transfere a propriedade dos dados da CONTRATANTE ou dos clientes desta para a CONTRATADA. Os dados gerados, obtidos ou coletados a partir da prestação dos serviços ora contratados são de propriedade do **CONTROLADOR**.

17.35. A CONTRATANTE é a exclusiva titular dos direitos de propriedade intelectual sobre qualquer novo elemento de dados, produto ou subproduto que seja criado a partir do tratamento de dados estabelecido por este Contrato, quando houver.

17.36. A CONTRATANTE não autoriza a CONTRATADA a usar, compartilhar ou comercializar quaisquer eventuais elementos de dados, produtos ou subprodutos que se originem ou sejam criados a partir do tratamento de dados estabelecido por este Contrato.

17.37. A rescisão ou expiração deste Contrato de Tratamento de Dados não exonera o **OPERADOR** de suas obrigações de confidencialidade, de acordo com as cláusulas de Confidencialidade.

17.38. O **OPERADOR** deverá processar os dados pessoais até a data de rescisão do contrato, a menos que instruído de outra forma pelo **CONTROLADOR**, ou até que esses dados sejam retornados ou destruídos por instrução do **CONTROLADOR**.
No caso de qualquer tipo de inconsistência entre as disposições deste Contrato de Tratamento de Dados e as disposições do Contrato de Serviço, as disposições deste Contrato de Tratamento de Dados prevalecerão.

18 CLÁUSULA 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 .....
Diretor Presidente

Pela CONTRATADA:

.....

Nome

:CPF.:

Cargo:

Testemunhas:

1ª..... 2ª.....
.....
Nome Nome
:CPF: :CPF:

ADENDO 4 AO CONTRATO

TERMO DE COMPROMISSO DE POLÍTICA ANTICORRUPÇÃO

Por este instrumento particular, a CONTRATADA compromete-se a cumprir integralmente as disposições da Políticas de Controles Internos e de Compliance do BANPARÁ, da qual tomou conhecimento neste ato por meio da leitura da cópia que lhe foi disponibilizada.

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

a) qualquer empregado, oficial de governo ou representante de, ou qualquer pessoa agindo oficialmente para ou em nome de uma entidade de governo, uma de suas subdivisões políticas ou uma de suas jurisdições locais, um órgão, conselho, comissão, tribunal ou agência, seja civil ou militar, de qualquer dos indicados no item anterior, independente de sua constituição, uma associação, organização, empresa ou empreendimento controlado ou de propriedade de um governo, ou um partido político (os itens A a D doravante denominados conjuntamente autoridade governamental);
b) oficial legislativo, administrativo ou judicial, independentemente de se tratar de cargo eletivo ou comissionado;
c) oficial de, ou indivíduo que ocupe um cargo em, um partido político;
d) candidato ou candidata a cargo político;
e) um indivíduo que ocupe qualquer outro cargo oficial, cerimonial, comissionado ou herdado em um governo ou qualquer um de seus órgãos; ou

f) um oficial ou empregado(a) de uma organização supranacional (por exemplo, Banco Mundial, Nações Unidas, Fundo Monetário Internacional, OCDE) (doravante denominado oficial de governo);
g) ou a qualquer pessoa enquanto se saiba, ou se tenha motivos para crer que qualquer porção de tal troca é feita com o propósito de:
    i. influenciar qualquer ato ou decisão de tal oficial de governo em seu ofício, incluindo deixar de realizar ato oficial, com o propósito de assistir o BANPARÁ ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro;
    ii. assegurar vantagem imprópria;
    iii. induzir tal oficial de governo a usar de sua influência para afetar ou influenciar qualquer ato ou decisão de uma autoridade governamental com o propósito de assistir o BANPARÁ ou qualquer outra pessoa a obter ou reter negócios, ou direcionar negócios a qualquer terceiro; ou
    iv. fornecer um ganho ou benefício pessoal ilícito, seja financeiro ou de outro valor, a tal oficial de governo.

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

a) permanecer em inteira conformidade com as Leis Anticorrupção, e qualquer legislação antissuborno, anticorrupção e de conflito de interesses aplicável, ou qualquer outra legislação, regra ou regulamento de propósito e efeito similares, abstendo-se de qualquer conduta que possa ser proibida a pessoas sujeitas às Leis Anticorrupção;
b) tomar todas as precauções necessárias visando prevenir ou impedir qualquer incompatibilidade ou conflito com outros serviços ou com interesses do BANPARÁ, o que inclui o dever de comunicar as relações de parentesco existentes entre os colaboradores da CONTRATADA e do BANPARÁ; e
c) observar, no que for aplicável, o Código de Ética e de Condutas Institucionais do BANPARÁ, sobre o qual declara ter pleno conhecimento.

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

Caso a CONTRATADA ou qualquer de seus colaboradores venha a tomar conhecimento de atitudes ilícitas ou suspeitas, especialmente se referentes à violação das Leis Anticorrupção, deve informar prontamente ao BANPARÁ, por meio do Canal de Denúncias .....

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

Por fim, a CONTRATANTE declara estar ciente de que a fiel observância deste instrumento é fundamental para a condução das atividades inerentes ao contrato

maneira ética e responsável constituindo falta grave, passível de imposição de penalidade, qualquer infração, no disposto deste instrumento.

.....

(Local e Data)

.....

(Representante legal)

ADENDO 5 AO CONTRATO

SEGURANÇA DA INFORMAÇÃO

Com relação às disposições constantes do Anexo I (Segurança da Informação), as Partes concordam que a sua aplicabilidade ficará condicionada, em qualquer caso, à compatibilidade e à aderência das mesmas em relação aos serviços contratados, e que a exigência, pela CONTRATANTE, das obrigações nele dispostas, estará sujeita à eventual precificação por parte da CONTRATADA, mediante análise do escopo contratual somente para os itens que não estão aderentes ou compatíveis ao Anexo I

a. Para versão web deve protocolo https e usar SSL (TSL 1.2) no servidor e também rodar o certificado SSL para comunicação
b. Não permitir que senha copiada ou que esteja na área de transferência seja colada no campo senha para fazer login.
c. 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.
d. 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.
e. Permitir que somente usuários credenciados configurem seu funcionamento da melhor maneira que convier ao Banpará.

Garantir que atende as melhores práticas de desenvolvimento seguro conforme elencado a seguir assim como MNP de Desenvolvimento Seguro:

1.1. Validação dos dados de Entrada / Saída

1.1.1. Efetuar toda a validação dos dados em um sistema confiável, centralizado no servidor/aplicação;

1.1.2. Identificar todas as fontes de dados e classificá-las como sendo confiáveis ou não. Em seguida, validar os dados provenientes de fontes nas quais não se possa confiar (ex: base de dados, stream de arquivos etc.)

1.1.3. Especificar o conjunto de caracteres apropriado (ex: UTF-8) e determinar se o sistema suporta essa codificação, validando se os dados recebidos estão realmente neste formato;

1.1.4. Quando ocorrer falha na validação dos dados, a aplicação deve rejeitar as informações e impedir o prosseguimento das atividades;

1.1.5. Validar todos os dados provenientes de redirecionamento ou inseridos por clientes antes do processamento, incluindo parâmetros, campos de formulário, conteúdo e cabeçalhos. Certificar-se ainda de incluir mecanismos automáticos de postback nos blocos de código JavaScript, Flash ou qualquer outra estrutura embutida;

1.1.6. Verificar se os valores de cabeçalho, tanto das requisições, como das respostas, contêm apenas caracteres ASCII

1.1.7. Quando na integração com outros sistemas, utilizar preferencialmente API's que executem tarefas específicas para função desejada. Deve-se evitar que a aplicação execute comandos diretamente no sistema operacional, especialmente através da utilização de shells;

1.1.8. Validar, sempre que possível, todos os dados de entrada através de um método baseado em "listas brancas" que utilizem uma lista de caracteres ou expressões regulares com os caracteres permitidos. Em geral: a-z (inclusive acentuados), A-Z (inclusive acentuados), 0-9;

1.1.9. Se qualquer caractere potencialmente perigoso precisa ser permitido na entrada de dados da aplicação – como campos de senha, por exemplo – certificar-se de que foram implementados controles adicionais como a codificação dos dados de saída. Como exemplo de caracteres potencialmente "perigosos", temos: ' " < > ./ \ - | ( ) ;

1.1.10. Incluir a verificação das seguintes entradas para a validação dos dados: bytes nulos (%00), caracteres de nova linha (%0d, %0a, \r, \n) e caracteres "ponto-ponto barra" (../ ou ..\);

1.1.11. A "canonicalização" deve ser utilizada para resolver problemas de codificação dupla (double encoding) ou ataques por ofuscação;

1.1.12. Um computador é capaz de interpretar diversas formas de representação para um mesmo caractere, tais como: DECIMAL, HEXADECIMAL, OCTAL, HTML/UNICODE e BINÁRIO. Por esse motivo, considerar filtros e proteções em variadas formatações. Para mais informações, vide ANEXO I – REPRESENTAÇÃO DE CARACTERES ESPECIAIS.

1.1.13. Dentro do modelo MVC (Model View Controler) utilizar a validação através do serviço de controle ao invés de deixar a regra na camada de Visão ou Interface.

1.2. Gerenciamento de Arquivos

1.2.1. Solicitar autenticação antes de permitir que seja feito o upload de arquivos;

1.2.2. Limitar os tipos de arquivos que podem ser enviados para aceitar somente os tipos necessários ao propósito do negócio (trabalhar com o modelo de white list). Validar os arquivos através da verificação dos cabeçalhos, uma vez que extensões de arquivos são facilmente modificadas;

1.2.3. Não salvar arquivos no mesmo diretório de contexto da aplicação, principalmente se esta for web. Preferencialmente, utilizar servidores de conteúdo ou bases de dados específicas;

1.2.4. Nos diretórios onde serão recebidos arquivos de upload, desativar privilégios de execução de binários, scripts ou arquivos de linguagens específicas, tais como: ASP, PHP, Perl, etc.

1.2.5. Não enviar caminhos de diretórios ou de arquivos em requisições. Utilizar mecanismos de mapeamento desses recursos para índices definidos em uma lista pré-definida de caminhos;

1.2.6. Nunca devolver o caminho absoluto do arquivo para o cliente da aplicação ou usuário final;

1.2.7. Quando necessário referenciar outros aplicativos, não utilizar nome relativos e sim o caminho absoluto do sistema. Por exemplo, ao invés de regedit.exe, utilizar %systemroot%\regedit.exe;

1.2.8. Ao realizar chamadas de outros aplicativos, utilizar mecanismos de verificação de integridade por checksum ou hash.

1.3. Gerenciamento de Memória

1.3.1. Instanciar explicitamente todas as variáveis e dados persistentes durante a declaração, ou antes da primeira utilização;

1.3.2. Ao usar funções que aceitem determinado número de bytes para realizar cópias (ex.: strncpy()), verificar se o tamanho do buffer de destino é igual ao tamanho do buffer de origem. Neste caso, ele não pode encerrar a sequência de caracteres com valor nulo (null);

1.3.3. Verificar os limites do buffer caso as chamadas à função sejam realizadas em ciclos (loop) e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado;

1.3.4. Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação;

1.3.5. Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo, dentre outros, não contar exclusivamente com o “garbage collector” e realizar a tarefa de liberação de memória explicitamente;

1.3.6. Atentar para as discrepâncias de tamanho de byte, precisão, distinções de sinal (signed/unsigned), truncamento, conversão de variáveis (type casting), cálculos que devolvam erros do tipo not-a-number e representação interna de números muito grandes ou pequenos;

1.3.7. Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos os pontos de saída.

1.4. Controle de Acessos

1.4.1. Utilizar um único componente para realizar o processo de verificação de autorização de acesso. Isto inclui bibliotecas que invocam os serviços externos de

autorização. Caso a aplicação não seja possível às configurações de segurança, negar todos os acessos;

1.4.2. Garantir o controle de autorização em todas as requisições, inclusive em scripts do lado servidor, "includes" e requisições do lado cliente, tais como: AJAX, Flash, etc; dessa forma se requer autenticação para todas as páginas e recursos.

1.4.3. Isolar do código da aplicação os trechos de código que contêm lógica privilegiada, isto é, com permissões exclusivas;

1.4.4. Quando a aplicação tiver que ser executada com privilégios elevados, realizar esta atividade o mais tarde possível e revogá-los logo que seja possível;

1.4.5. Proteger variáveis compartilhadas e os recursos contra acessos concorrentes inapropriados;

1.4.6. Restringir o acesso somente aos usuários autorizados de URLs, funções protegidas, serviços e dados da aplicação (atributos e campos), referências diretas e configurações de segurança, incluindo definições do servidor, arquivos de configuração e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação;

1.4.7. Não incluir credenciais diretamente no código-fonte. Adicionalmente, utilizar ofuscação de código para a proteção de dados sensíveis, tais como consultas SQL (PROTEÇÃO CONTRA ENGENHARIA REVERSA)

1.4.8. As regras de controle de acesso representadas pela camada de apresentação devem coincidir com as regras presentes no lado servidor;

1.4.9. Caso seja necessário armazenar o estado dos dados no lado cliente, utilizar mecanismos de criptografia e verificação para detectar possíveis alterações;

1.4.10. Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo;

1.4.11. Não utilizar os campos de cabeçalho (por exemplo: referer, user-agent, cookie, etc) individualmente como forma de validação de autorização. Estes devem ser utilizados sempre em conjunto com outros recursos;

1.4.12. Isolar do código da aplicação os trechos de código que contêm lógica privilegiada

1.4.13. Restringir o acesso aos arquivos e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação, somente aos usuários autorizados

1.4.14. Restringir o acesso às URLs protegidas somente aos usuários autorizados

1.4.15. Restringir o acesso às funções protegidas somente aos usuários autorizados

1.4.16. Restringir o acesso às referências diretas aos objetos somente aos usuários autorizados

1.4.17. Restringir o acesso aos serviços somente aos usuários autorizados

1.4.18. Restringir o acesso aos dados da aplicação somente aos usuários autorizados

1.4.19. Restringir o acesso aos atributos e dados dos usuários, bem como informações das políticas usadas pelos mecanismos de controle de acesso

1.4.20. Restringir o acesso às configurações de segurança relevantes apenas aos usuários autorizados

1.4.21. Se for permitida a existência de sessões autenticadas por longos períodos de tempo, fazer a revalidação periódica da autorização do usuário para garantir que os privilégios não foram modificados e, caso tenham sido, realizar o registro em log do usuário e exigir nova autenticação.

1.4.22. Separar a lógica de autenticação do recurso que está a ser requisitado e usar redirecionadores dos controladores de autenticação centralizados

1.4.23. Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial

1.4.24. As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como “Nome de usuário incorreto” ou “Senha incorreta”, utilize apenas mensagens como: “Usuário e/ou senha inválidos”, para ambos os casos de erro. As respostas de erro devem ser idênticas nos dois casos.

1.4.25. Utilizar autenticação para conexão a sistemas externos que envolvam tráfego de informação sensível ou acesso a funções

1.4.26. As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em um local protegido de um sistema confiável, por exemplo, no servidor da aplicação.

Obs.: o código-fonte não é considerado um local seguro

1.4.27. Utilizar apenas requisições POST para transmitir credenciais de autenticação

1.4.28. Somente trafegar senhas (não temporárias) através de uma conexão protegida (SSL/TLS) ou no formato de dado cifrado, como no caso de envio de e-mail cifrado. Senhas temporárias enviadas por e-mail podem ser um caso de exceção aceitável

1.4.29. A entrada da senha deve ser ocultada na tela do usuário. Em HTML, utilizar o campo do tipo "password"

1.4.30. Notificar o usuário quando a senha for reiniciada (reset)

1.4.31. Desativar a funcionalidade de lembrar a senha nos campos de senha do navegador

1.4.32. A data/hora da última utilização (bem ou mal sucedida) de uma conta de usuário deve ser comunicada no próximo acesso ao sistema

1.4.33. Realizar monitoramento para identificar ataques contra várias contas de usuários, utilizando a mesma senha. Esse padrão de ataque é utilizado para explorar o uso de senhas padrão

1.4.34. Utilizar autenticação de múltiplos fatores (utilizando simultaneamente token, senha, biometria etc.5) via multifatorial

1.4.35. Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo (parametrizável).

1.4.36. Utilizar o campo “referer” do cabeçalho somente como forma de verificação suplementar. O mesmo não deve ser usado sozinho como forma de validação de autorização porque ele pode ter o valor adulterado

1.4.37. Implementar a auditoria das contas de usuário e assegurar a desativação de contas não utilizadas. A aplicação deve dar suporte à desativação de contas e ao encerramento das sessões quando terminar a autorização do usuário.

1.4.38. . As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos não podem efetuar autenticação no sistema.

1.5. Gerenciamento de sessões e comunicações

1.5.1. Utilizar controles de gerenciamento de sessão baseados no servidor ou em framework confiável. A aplicação deve reconhecer apenas esses identificadores de sessão como válidos;

1.5.2. O controle de gestão de sessão deve usar algoritmos conhecidos, padronizados e bem testados que garantam a aleatoriedade dos identificadores de sessão.

1.5.3. Definir o domínio e o caminho para os cookies que contenham identificadores de sessão autenticados, para um valor devidamente restrito ao site;

1.5.4. A funcionalidade de saída (logout) necessita estar disponível em todas as páginas que requerem autenticação e deve encerrar completamente a sessão ou conexão associada. Adicionalmente, não permitir logins persistentes (sem prazo de expiração);

1.5.5. Estabelecer um tempo de expiração baseado nos riscos e requisitos funcionais do negócio;

1.5.6. Não permitir logins persistentes (sem prazo de expiração) e realizar o encerramento da sessão periodicamente, mesmo quando ela estiver ativa. Isso deve ser feito, especialmente, em aplicações que suportam várias conexões de rede ou que se conectam a sistemas críticos. O tempo de encerramento deve estar de acordo com os requisitos do negócio e o usuário deve receber notificações suficientes para atenuar os impactos negativos dessa medida

1.5.7. Se uma sessão estava estabelecida antes do login, ela deve ser encerrada (gerando um novo identificador de sessão) para que uma nova seja estabelecida;

1.5.8. Não permitir conexões simultâneas com o mesmo identificador de usuário;

1.5.9. Não expor os identificadores de sessão em URLs, mensagens de erro ou logs. Os identificadores de sessão devem apenas ser encontrados no cabeçalho do cookie HTTP. Por exemplo, não trafegar os identificadores de sessão sob a forma de parâmetros GET;

1.5.10. Gerar um novo identificador de sessão caso a segurança da conexão mude de HTTP para HTTPS. Uilizar HTTPS de forma constante em vez de alternar entre HTTP e HTTPS

1.5.11. Configurar o atributo “secure” para cookies enviados de conexões SSL/TLS;

1.5.12. Configurar os cookies com o atributo HttpOnly, a menos que seja explicitamente necessário ler ou definir os valores dos mesmos através de scripts do lado cliente da aplicação;

1.5.13. Somente trafegar senhas através de uma conexão protegida (SSL/TLS) ou conexões cifradas. Senhas temporárias devem ser avaliadas junto a equipe de segurança;

1.5.14. Filtrar os parâmetros que contenham informações sensíveis, provenientes do “HTTP referer”, nos links para sites externos;

1.5.15. Não transferir, diretamente, dados fornecidos pelo usuário para qualquer função de execução dinâmica sem realizar o tratamento dos dados de modo adequado;

1.5.16. As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos devem possuir o menor privilégio possível

1.5.17. Utilizar mecanismos complementares ao mecanismo padrão de gerenciamento de sessões para operações sensíveis do lado servidor – como no caso de operações de gerenciamento de contas, transações financeiras ou informações que se enquadrem como CONFIDENCIAL conforme MNP de Classificação e Tratamento da Informação –. através da utilização de tokens aleatórios ou parâmetros em cada requisição em vez de basear-se apenas na sessão. Esse método usado para prevenir ataques do tipo Cross Site Request Forgery (CSRF)

1.6. Autenticação e gerenciamento de credencias

1.6.1. Assegurar que os usuários sejam autenticados em todas as páginas e recursos do sistema, exceto para dados públicos;

1.6.2. Os controles de autenticação devem ser executados em um sistema confiável, centralizado e possível com bibliotecas exclusivas para esse tipo de atividade;

1.6.3. Mediante situações excepcionais nos controles de autenticação, negar quaisquer solicitações;

1.6.4. Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial;

1.6.5. As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como “nome de usuário incorreto” ou “senha incorreta”, utilize apenas “usuário e/ou senha inválidos”;

1.6.6. As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em local protegido, por exemplo, no servidor da aplicação;

1.6.7. Em aplicações web, utilizar apenas requisições com o método POST para transmitir credenciais de acesso;

1.6.8. A entrada da senha deve permanecer ofuscada. Em HTML, utilizar o campo do tipo "password";

1.6.9. Os processos de redefinição de senhas e operações de mudanças devem exigir os mesmos níveis de controle previstos para a criação de contas e autenticação;

1.6.10. Se optar por usar redefinição de senha baseada em e-mail, enviar a mensagem conforme definido em integração com Multifatorial

1.6.11. Exigir a mudança de senhas temporárias quando na realização do primeiro logon, a não ser que esteja integrado ao AD e assim quem gerencia a conformidade de senha/validade/força/integração com RH é o AD. Entretanto deve utilizar integração via LDAPs.

1.6.12. Informar ao usuário autenticado data/hora e o endereço IP da sua última utilização do sistema;

1.6.13. Se a aplicação gerenciar um repositório de credenciais, o sistema deverá garantir que as senhas sejam armazenadas na base de dados somente sob a forma de hash, conforme padronização contida no capítulo “Padrões de Criptografia e Funções de Hash”;

1.6.14. Para evitar ataques de brute force ou mesmo a utilização inadvertida de rôbos, adotar mecanismos de CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), para a diferenciação entre máquinas e humanos. Por se tratar de um desafio cognitivo, considera-se que aquele que incorpora uma solução correta é presumidamente humano.

1.7. Práticas de Criptografia:

1.7.1. Todas as funções de criptografia utilizadas para proteger dados sensíveis dos usuários da aplicação, devem ser implantadas em um sistema confiável (neste caso o servidor)

1.7.2. A senha mestre deve ser protegida contra acessos não autorizados

1.7.3. Quando ocorrer alguma falha nos módulos de criptografia, permitir que as mesmas ocorram de modo seguro

1.7.4. Todos os números, nomes de arquivos, GUIDs e strings aleatórias devem ser gerados usando um módulo criptográfico com gerador de números aleatórios, somente se os valores aleatórios gerados forem impossíveis de serem deduzidos

1.7.5. Os módulos de criptografia usados pela aplicação devem ser compatíveis com a FIPS 140-2 ou com um padrão equivalente (http://csrc.nist.gov/groups/STM/cmvp/validation.html)

1.7.6. Estabelecer e utilizar uma política e processo que defina como é realizado o gerenciamento das chaves criptográficas.

1.8. Tratamento de Erros e Log:

1.8.1. Não expor informações sensíveis nas repostas de erros, inclusive detalhes de sistema, identificadores de sessão ou informação da conta do usuário

1.8.2. Usar mecanismos de tratamento de erros que não mostrem informações de depuração (debug) ou informações da pilha de exceção

1.8.3. Usar mensagens de erro genéricas e páginas de erro personalizadas

1.8.4. A aplicação deve tratar os erros sem se basear nas configurações do servidor

1.8.5. A memória alocada deve ser liberada de modo apropriado quando ocorrerem condições de erro

1.8.6. O tratamento de erros lógicos associados com os controles de segurança devem, por padrão, negar o acesso

1.8.7. Todos os controles de log devem ser implementados em um sistema confiável, por exemplo, centralizar todo o processo no servidor

1.8.8. Os controles de log devem dar suporte tanto para os casos de sucesso como os de falha relacionados com os eventos de segurança

1.8.9. Garantir que os logs armazenam eventos importantes

1.8.10. Garantir que as entradas de log que incluam dados nos quais não se confia não sejam executadas como código-fonte na interface de visualização de logs

1.8.11. Restringir o acesso aos logs apenas para pessoal autorizado

1.8.12. Utilizar uma rotina centralizada para realizar todas as operações de log

1.8.13. Não armazenar informações sensíveis nos registros de logs, como detalhes desnecessários do sistema, identificadores de sessão e senhas

1.8.14. Garantir o uso de algum mecanismo que conduza (ou facilite) o processo de análise de logs

1.8.15. Registrar em log todas as falhas de validação de entrada de dados

1.8.16. Registrar em log todas as tentativas de autenticação, especialmente as que falharam por algum motivo

1.8.17. Registrar em log todas as falhas de controle de acesso

1.8.18. Registrar em log todos os eventos suspeitos de adulteração, inclusive alterações inesperadas no estado dos dados

1.8.19. Registrar em log as tentativas de conexão com tokens de sessão inválidos ou expirados

1.8.20. Registrar em log todas as exceções lançadas pelo sistema

1.8.21. Registrar em log todas as funções administrativas, inclusive as mudanças realizadas nas configurações de segurança

1.8.22. Registrar em log todas as falhas de conexão TLS com o backend

1.8.23. Registrar em log todas as falhas que ocorreram nos módulos de criptografia

1.8.24. Utilizar uma função de hash criptográfica para validar a integridade dos registros de log

1.9. Segurança nas comunicações:

1.9.1. Utilizar criptografia na transmissão de todas as informações sensíveis. Isto deve incluir TLS para proteger a conexão e deve ser complementado com criptografiade arquivos que contém dados sensíveis ou conexões que não usam o protocolo HTTP

1.9.2. Os certificados TLS devem ser válidos, possuírem o nome de domínio correto, não estarem expirados e serem instalados com certificados intermediários, quando necessário

1.9.3. Quando ocorrer alguma falha nas conexões TLS, o sistema não deve fornecer uma conexão insegura

1.9.4. Utilizar conexões TLS para todo o conteúdo que requerer acesso autenticado ou que contenha informação sensível

1.9.5. Utilizar TLS para conexões com sistemas externos que envolvam funções ou informações sensíveis

1.9.6. Utilizar um padrão único de implementação TLS configurado de modo apropriado

1.9.7. Especificar a codificação dos caracteres para todas as conexões

1.9.8. Filtrar os parâmetros que contenham informações sensíveis, provenientes do "HTTP referer", nos links para sites externos.

1.10. Gerenciamento de Memória:

1.10.1. Utilizar controle de entrada/saída para os dados que não sejam confiáveis

1.10.2. Verificar se o buffer é tão grande quanto o especificado

1.10.3. Ao usar funções que aceitem determinado número de bytes para realizar cópias, como strncpy(), esteja ciente de que se o tamanho do buffer de destino for igual ao tamanho do buffer de origem, ele não pode encerrar a sequência decaracteres com valor nulo (null)

1.10.4. Verificar os limites do buffer caso as chamadas à função sejam realizadas em ciclos e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado

1.10.5. Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação

1.10.6. Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo etc., não contar com o "garbage collector" e realizar a tarefa explicitamente

1.10.7. Usar pilhas não executáveis, quando disponíveis

1.10.8. Evitar o uso de funções reconhecidamente vulneráveis como printf(), strcat(), strcpy() etc.

1.10.9. Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos pontos de saída.

ADENDO 6 AO CONTRATO – TERMO DE RESPONSABILIDADE COM AS RECOMENDAÇÕES DO CÓDIGO DE ÉTICA E DE CONDUTA DO BANPARÁ

Eu, , representante da empresa _____, inscrita no CNPJ sob o nº _____ , sediada na _____, Bairro _____, CEP _____, Cidade – Estado declaro:

Declaro:

a) Que recebi, li e compreendi, tendo, assim, conhecimento do inteiro teor do mencionado Código de Ética e de Conduta Institucional do Banpará e concordo com os princípios e orientações nele contidos;

b) Que a empresa Contratada atuará conforme os padrões e princípios deste Código, ciente de que o desrespeito às suas disposições pode acarretar a rescisão do contrato, sem prejuízo das penalidades contratuais cabíveis;

c) Que estou ciente de que o documento se encontra disponível no seguinte endereço: https://www.banpara.b.br/banpara/regulamentos/.

(Cidade), _____ de _____ de _____.

_____

TESTEMUNHAS:

1ª..... 2ª.....

Nome: Nome:

CPF: CPF: