**TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇO DE ESCRITURAÇÃO ELETRÔNICA DE AÇÕES, REFERENTE À CARTEIRA DE ACIONISTAS DO BANCO DO ESTADO DO PARÁ (BANPARÁ), QUE ENTRE SI FAZEM O BANCO DO ESTADO DO PARÁ S.A. E A EMPRESA BANCO DO BRADESCO S.A.**

Por este instrumento particular, de um lado, o BANCO DO ESTADO DO PARÁ S.A., instituição financeira, com sede em Belém do Pará, na Avenida Presidente Vargas, n.º 251, Bairro Comércio, CEP. 66.010-000, Belém-PA, inscrito no Ministério da Fazenda sob o CNPJ n.º 04.913.711/0001-08, neste ato representada legalmente por dois de seus Diretores infra-assinados, doravante denominado BANPARÁ e, de outro lado, BANCO DO BRADESCO S.A**.**, estabelecida no Núcleo Cidade de Deus, s/n°, Vila Yara, Osasco/SP, CEP 06.029-900, inscrita no CNPJ sob o nº 60.746.948/0001-12, 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 a **Contratação de serviço de "Escrituração eletrônica de ações", referente à carteira de acionistas do Banco do Estado do Pará (BANPARÁ)**, **na forma da Resolução CVM nº 33, de 19/05/2021 e suas alterações posteriores, bem como da Lei nº 6.404/76 e suas alterações posteriores e demais instruções editadas pela CVM – Comissão de Valores Mobiliários e pelos demais órgão normatizadores/fiscalizadores,** conforme especificações, exigências e condições estabelecidas no edital e seus Anexos.

**1.1.** O presente contrato decorre do processo nº **0522/2023**, realizado pelo edital da licitação do **PE nº 029/2023.**

## 2. CLÁUSULA SEGUNDA – ADENDOS

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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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** - Termo de Responsabilidade com as Recomendações do Código de Ética e de Conduta do Banpará
**Adendo 6** – Diretrizes para Utilização de Desenvolvimento Seguro
**Adendo 7** – Matriz de Risco

**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** A vigência do Contrato será de 12 (doze) meses, contados da data de sua assinatura do respectivo termo, podendo ser prorrogado na forma da lei.

**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 estimado de **R$164.308,72 (cento e sessenta e quatro mil, trezentos e oito reais e setenta e dois centavos)**, conforme o valor da tabela abaixo e nas condições estabelecidas no **Termo de Referência** (**ANEXO I** do Edital e Adendo 1 deste contrato):

| **A – CUSTOS INICIAIS:** | | | **VALOR ÚNICO** |
|---|---|---|---|
| Implantação do serviço de escrituração de ações | | | R$0,00 |
| **TOTAL CUSTO A** | | | **R$0,00** |
| **B - CUSTOS FIXOS:** | **VALOR UNITÁRIO** | **VALOR MENSAL** | **VALOR FIXO PARA O PERÍODO DE 12 MESES (VALOR MENSAL X 12)** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | |
|---|---|---|---|
| Custo mensal | | R$10.538,06 | R$126.456,72 |
| Custo adicional por acionista X 1.500 acionistas | R$1,09 | R$1.635,00 | R$19.620,00 |
| **TOTAL DO CUSTO B** | | | **R$146.076,72** |
| **C – CUSTOS DE REMUNERAÇÃO AOS ACIONISTAS:** | **VALOR UNITÁRIO POR EVENTO** | **VALOR TOTAL POR EVENTO (VALOR UNITÁRIO X 1.500 ACIONISTAS)** | **VALOR ANUAL (04 EVENTOS POR ANO)** |
| Pagamento de distribuição de dividendos / JCP realizado com correntista do Banco contratado | R$0,00 | R$0,00 | R$0,00 |
| Pagamento de distribuição de dividendos / JCP realizado com correntista de outros Bancos | R$0,00 | R$0,00 | R$0,00 |
| Pagamento por Caixa | R$0,00 | R$0,00 | R$0,00 |
| **TOTAL CUSTO C** | | | **R$0,00** |
| **D - CUSTOS VARIÁVEIS COM ASSEMBLEIAS GERAIS:** | | **VALOR UNITÁRIO POR EVENTO** | **VALOR ANUAL (03 EVENTOS POR ANO)** |
| Evento de voto a distância | | R$4.767,76 | R$14.303,28 |
| **TOTAL CUSTO D** | | **R$4.767,76** | **R$14.303,28** |
| **E - CUSTOS VARIÁVEIS POR ACIONISTA** | | **VALOR UNITÁRIO POR EVENTO** | **VALOR TOTAL POR EVENTO (VALOR UNITÁRIO X 1.500 ACIONISTAS)** |
| Alteração cadastral/Implantação/Movimentação/Gravames | | R$0,00 | R$0,00 |
| Emissão de Documentos | | R$0,00 | R$0,00 |
| **TOTAL CUSTO E** | | **R$0,00** | **R$0,00** |
| **F – DEMAIS CUSTOS VARIÁVEIS** | | | **VALOR ÚNICO** |
| Cálculo por evento deliberado | | | R$3.928,72 |
| Postagem de Documentos - Taxa ECT | | | Taxa ECT |
| Livro RAN | | | R$0,00 |
| Eventos Societários Simples (Grupamentos, Desdobramentos, Bonificações, Subscrições, Resgate, Dissidência, etc.) | | | R$0,00 |
| Tarifa DOC/TED – Taxa BACEN | | | Taxa BACEN |
| **TOTAL CUSTO F** | | | **R$3.928,72** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | |
|---|---|
| **VALOR GLOBAL ANUAL DA PROPOSTA (A + B + C+ D + E + F)** | **R$164.308,72** |

**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, deslocamentos 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.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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 0,07% (sete centésimos por cento) sobre o valor total do contrato, por dia de atraso, limitada a 2% (dois 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

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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.

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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.

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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 – NURIN@banparanet.com.br

E-mail CONTRATADA – dac.escrituracao@bradesco.com.br

**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,

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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;

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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:

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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 apresentação da proposta, no prazo da lei, segundo a variação acumulada do INPC do Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro, na falta deste, que estiver estabelecido na legislação à época de cada reajuste.

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

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

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

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

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

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

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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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.

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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

## 13 CLÁUSULA 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:

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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 – POLÍTICA DE RELACIONAMENTO E ANTICORRUPÇÃO

**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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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 declara que tem conhecimento de que a CONTRATANTE possui políticas e procedimentos internos que têm como objetivo garantir o cumprimento dos compromissos legais e éticos assumidos, dentre os quais está incluído o Código de Conduta Ética e Conduta, disponível em https://www.banpara.b.br/banpara/regulamentos/.

**16.9** A CONTRATADA, em consonância com cláusula anterior, declara que 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.

**16.10** 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 CLÁSULA DEZESSETE – DA DOTAÇÃO ORÇAMENTÁRIA

17.1 As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento do Banpará, para o exercício de 2023 na classificação abaixo:

Gestão/Unidade: NURIN

Conta Contábil: 8.1.7.54.00.001.011 – ESCRITURAÇÃO DE AÇÕES

## 18 CLÁUSULA DEZOITO – DO TRATAMENTO DE DADOS PESSOAIS

**18.1. DEFINIÇÕES**: O **CONTRATATE** E O **CONTRATADO**, ora denominado **CONTROLADORES INDEPENDENTES**, concordam que, para fins de tratamento de dados pessoais, serão utilizadas as definições conforme disposto na Lei Geral de Proteção de Dados, Lei nº 13.709/2018, no artigo 5º e seus incisos.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

18.2. A **CONTROLADORIA INDEPENTENTE** ocorre quando o tratamento dos dados pessoais é feito em conjunto por dois controladores, com finalidades distintas, onde ambos possuem autonomia para determinar as finalidades próprias e atinentes à sua atividade, para o tratamento de dados pessoais.

**18.3. ESCOPO DO TRATAMENTO DE DADOS PESSOAIS:** Esta cláusula se aplica exclusivamente ao tratamento de dados pessoais pelas partes que está sujeito à Lei Geral de Proteção de Dados (LGPD), durante a vigência deste contrato.

18.4. Cada **CONTROLADOR DE DADOS** será responsável pelo tratamento de dados pessoais que realizar, sendo vedado tratamento para finalidades distintas das previstas neste CONTRATO, exceto quando necessário para cumprimento de obrigação legal ou regulatória.

18.5. Em razão do objeto do Contrato, poderão ser tratados os seguintes dados pessoais: login e email

**18.6. RESPONSABILIDADES:** Cada **CONTROLADOR DE DADOS** irá determinar o escopo, o propósito e a maneira pela qual os dados pessoais serão tratados no âmbito de sua atividade, sempre vinculados às finalidades previstas neste **CONTRATO**.

18.7. Cada **CONTROLADOR DE DADOS** será responsável por suas próprias violações das leis de proteção de dados e das obrigações oriundas este Contrato, **não havendo responsabilidade solidária entre as partes.**

**18.8. AS PARTES** deverão informar imediatamente a outra se verificar ou houver suspeita infração à Lei Geral de Proteção de Dados ou outras disposições de proteção de dados do país ou regulamentos/tratados internacionais.

18.9. Cada **CONTROLADOR DE DADOS** será responsável por garantir os direitos dos titulares de dados em virtude do tratamento de dados que realizar, tais como solicitações de acesso, solicitações de retificação ou descarte de dados pessoais e objeções ao tratamento.

**18.10. CONFIDENCIALIDADE**: Sem prejuízo de quaisquer acordos contratuais existentes, **AS PARTES** tratarão todos os dados pessoais como estritamente confidenciais e informarão todos os seus funcionários, agentes envolvidos no processamento de dados pessoais de natureza confidencial, bem como garantirão que todos os envolvidos estejam sob égide de acordo de confidencialidade apropriado.

18.11. Quaisquer informações relativas ao presente CONTRATO somente poderão ser dadas ao conhecimento de terceiros, inclusive através dos meios de publicidade disponíveis, mediante acordo por escrito entre **AS PARTES.**

**18.12. COMPARTILHAMENTO E TRANSFERÊNCIA**: **OS CONTROLADORES** se comprometem a informar a ocorrência de compartilhamento com terceiros dos dados pessoais advindos deste CONTRATO e de quaisquer transferências permanentes ou temporárias (planejadas) dos dados pessoais para um país fora do Brasil, sendo

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

vedado qualquer compartilhamento ou transferência internacional para finalidades diversas das previstas neste CONTRATO, salvo se necessários para cumprimento de obrigação legal ou regulatória.

**18.13. SUBCONTRATAÇÕES**: Caso **OS CONTROLADORES** decidam realizar subcontratações para cumprimento das obrigações oriundas deste CONTRATO, estas deverão sem comunicadas à outra PARTE, com a garantia de que os subcontratantes estejam sujeitos às mesmas obrigações de proteção de dados estipuladas neste Contrato.

**18.14. OBRIGAÇÕES EM CASO DE INCIDENTE**: **OS CONTROLADORES** se comprometem a comunicar formalmente a outra a ocorrência de qualquer incidente de segurança com os dados pessoais oriundos deste **CONTRATO** no âmbito de sua atuação, se comprometendo a adotar todas as medidas para mitigação dos danos, bem como a comunicar a Autoridade e os titulares afetados em caso de incidentes que possam gerar riscos ou danos relevantes aos titulares, com auxílio mútuo para a melhor resolução do incidente e proteção dos direitos dos titulares.

**18.15. COMUNICAÇÃO: OS CONTROLADORES** estipulam os seguintes canais para comunicações necessárias sobre o tratamento de dados pessoais que ocorrerão na execução deste CONTRATO:

**I - CONTRATADA:**
**Encarregado Pela Proteção de Dados Pessoais: nomeado e identificado conforme informação constante no seguinte link https://www.bradescoseguranca.com.br/html/seguranca_corporativa/pf/lei-geral/index.shtm**
**E-mail: proteção.dados@bradescoseguros.com.br**

**II - CONTRATANTE: BANCO DO ESTADO DO PARÁ S.A**
**Encarregado Pela Proteção de Dados Pessoais: nomeado e identificado conforme informação constante no seguinte link https://www.banpara.b.br/banpara/seguranca/politica-de-privacidade/**
**E-mail:** dpo@banparanet.com.br

**18.16. DO TÉRMINO DE TRATAMENTO DE DADOS PESSOAIS:** Ao término da relação entre **OS CONTROLADORES**, estes se comprometem a eliminar, corrigir, anonimizar, armazenar e/ou bloquear o acesso às informações, em caráter definitivo ou não, que tiverem sido tratadas em decorrência deste CONTRATO, salvo permissão legal para a manutenção desse tratamento, estendendo-se essa obrigação a eventuais cópias desses Dados Pessoais. Mesmo após a rescisão deste instrumento ou de outros acordos celebrados entre as Partes, as obrigações destas perdurarão enquanto ela tiver acesso, estiver em posse ou conseguir realizar qualquer operação de tratamento com os Dados Pessoais envolvendo informações fornecidas pela outra Parte.

18.17. No caso de qualquer tipo de inconsistência entre as disposições desta Cláusula de Tratamento de Dados e as disposições do Contrato, as disposições desta Cláusula de Tratamento de Dados prevalecerão.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

## 19 CLÁUSULA DEZENOVE – MATRIZ DE RISCOS

**19.1.** Na hipótese de ocorrência de um dos eventos listados no item 17 do Termo de Referência (Adendo IV – Matriz de Riscos), o CONTRATADO deverá, no prazo de 01 (um) dia útil, informar ao CONTRATANTE sobre o ocorrido, contendo as seguintes informações mínimas

**a)** Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada;
**b)** As medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;
**c)** As medidas que irá tomar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;
**d)** As obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e,
**e)** Outras informações relevantes.

19.2. Após a notificação, o CONTRATANTE decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais ao CONTRATADO. Em sua decisão o CONTRATANTE poderá isentar temporariamente o CONTRATADO do cumprimento das obrigações contratuais afetadas pelo Evento.

19.3. A concessão de isenção não exclui a possibilidade de aplicação das sanções previstas neste Contrato.

19.4. O reconhecimento pelo CONTRATANTE dos eventos descritos no item 17 do TR, que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente ao CONTRATADO, não dará ensejo a recomposição do equilíbrio econômico financeiro do contrato, devendo o risco ser suportado exclusivamente pelo CONTRATADO.

19.5. As obrigações contratuais afetadas por caso fortuito, fato do príncipe ou força maior deverão ser comunicadas pelas partes em até 01 (um) dia útil, contados da data da ocorrência do evento.

19.6. As partes deverão acordar a forma e o prazo para resolução do ocorrido.

**19.7.** As partes não serão consideradas inadimplentes em razão do descumprimento contratual decorrente de caso fortuito, fato do príncipe ou força maior.
19.8. Avaliada a gravidade do evento, as partes, mediante acordo, decidirão quanto à recomposição do equilíbrio econômico financeiro do contrato, salvo se as consequências do evento sejam cobertas por Seguro.

19.9. O contrato poderá ser rescindido mediante as hipóteses previstas no Regulamento de Licitações e Contratos do CONTRATANTE.

19.10. As partes se comprometem a empregar todas as medidas e ações necessárias a fim de minimizar os efeitos advindos dos eventos de caso fortuito, fato do príncipe ou força maior.

**19.11.** Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos na Matriz de Riscos,

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico financeiro do contrato.

## 20 CLÁUSULA VINTE – DA ASSINATURA DIGITAL

20.1. As PARTES expressamente anuem, autorizam, aceitam e reconhecem que todos os documentos pertinentes ao Contrato, inclusive o próprio instrumento contratual e seus aditivos, todas as páginas de assinatura e eventuais anexos, podem ser assinados digitalmente com as respectivas assinaturas mediante certificados eletrônicos, com autenticidade reconhecida pelo certificado digital ICP-Brasil, e enviados entre as partes por meio eletrônico nos termos do art. 10, º2º da MP nº 2.220-

## 21 CLÁUSULA VINTE E UM – DO FORO

**21.1** 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:

RUTH PIMENTEL MELLO:18168442253 Assinado de forma digital por RUTH PIMENTEL MELLO:18168442253

.....

Diretor Presidente

IGOR BARBOSA GONCALVES:94329656272 Assinado de forma digital por IGOR BARBOSA GONCALVES:94329656272 Dados: 2024.01.18 17:33:21 -03'00'

.....

Diretor .....

Pela CONTRATADA:

.....

Nome : JOSE ARY DE CAMARGO SALLES NETO:15106300827 Assinado de forma digital por JOSE ARY DE CAMARGO SALLES NETO:15106300827 DN: c=BR, o=ICP-Brasil, ou=AC SOLUTI Multipla v5, ou=09461647000195, ou=Presencial, ou=Certificado PF A3, cn=JOSE ARY DE CAMARGO SALLES NETO:15106300827 Dados: 2024.01.29 14:19:42 -03'00'

CPF.: 7

Cargo:

ROSELI MARIA LOUZANO:15262846858 Assinado de forma digital por ROSELI MARIA LOUZANO:15262846858 DN: c=BR, o=ICP-Brasil, ou=AC SOLUTI Multipla v5, ou=09461647000195, ou=Videoconferencia, ou=Certificado PF A3, cn=ROSELI MARIA LOUZANO:15262846858 Dados: 2024.01.29 14:54:06 -03'00'

Testemunhas:

1ª.....

Nome:

CPF:

2ª.....

Nome:

CPF:

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

## 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;

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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)

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**ADENDO 5 AO CONTRATO**
**TERMO DE RESPONSABILIDADE COM AS RECOMENDAÇÕES DO CÓDIGO DE ÉTICA E DE CONDUTA DO BANPARÁ**

**Eu,** (nome do representante da empresa), representante da empresa BANCO DO BRADESCO S.A., inscrita no CNPJ sob o nº nº 60.746.948/0001-12, 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/.

....., ..... de .....de .....

.....
(Representante legal)

**TESTEMUNHAS:**

| | |
|---|---|
| 1ª..... | 2ª..... |
| Nome: | Nome: |
| CPF: | CPF: |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**ADENDO 6 AO CONTRATO**
**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 ADEND - 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);

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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)

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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;

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

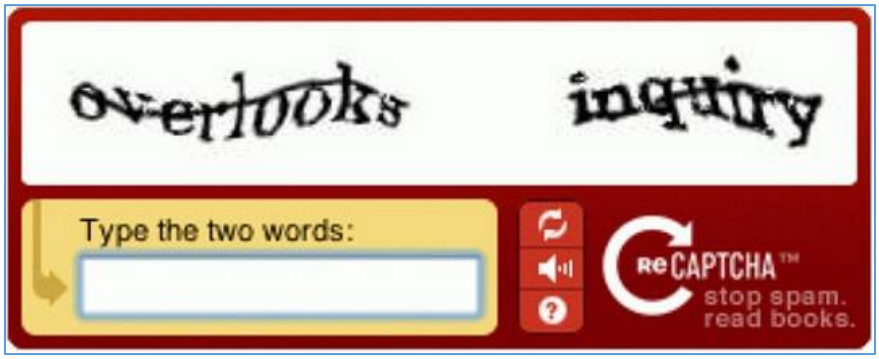
3.4.13. Somente trafegar senhas através de uma conexão protegida (SSL/TLS) ou conexões cifradas. Senhas temporárias devem ser avaliadas junto a equipe de segurança;
3.4.14. Filtrar os parâmetros que contenham informações sensíveis, provenientes do "*HTTP referer*", nos links para sites externos;
3.4.15. 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*

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

*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;

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

## 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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

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. | |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | | |
|---|---|---|---|---|
| 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 Javascript Injection | Prevenir ataques XSS, de quebra de autenticação e gerenciamento de sessão | Submeter sistema a ferramentas de testes de invasão |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | | |
|---|---|---|---|---|
| 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 responsabilidades 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 indisponibilização do sistema e correção da falha | Política de acompanhamento pós-ocorrência | Revisão contínua da política de testes com base em lições aprendidas |
| Criptografia e Hash | Tamanho de chave para cifradores simétricos/assim 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/modos obsoletos. E.g | |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | | |
|---|---|---|---|---|
| | | | ., DES, RC4, etc. | |
| Criptografia e Hash | Requisitos função de hash criptográfico. | Usar salt sempre que possível | Não usar cifradores/modos 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 | | |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | | |
|---|---|---|---|---|
| | | 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 | | |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| ☐ | Implementar rotinas para tratamento de erros, evitando que mensagens de falha ou debug sejam exibidas para o usuário.<br><br>Além disso, assegurar que as mensagens de erro para falhas de autenticação não especifiquem o ponto de falha. | **Ataque/Vulnerabilidade**<br>2.12) Tratamento inadequado de erros e exceções (ERROR HANDLING)<br>2.12) Ataques de enumeração (ENUMERATION) |
| | | **Referências**<br>3.4) Gerenciamento de sessões e comunicações<br>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**<br>2.12**) Ataque de formação de strings (FORMAT STRINGS ATTACKS)** |
| | | **Referências**<br>**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**<br>**2.12) Estouro de Memória (BUFFER OVERFLOW)**<br>**2.12) Estouro de Inteiros (INTEGER OVERFLOW)** |
| | | **Referências**<br>3.2) Gerenciamento de Memória |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| ☐ | Implementar rotinas para impedir que arquivos da aplicação e/ou sistema operacional fora contexto do sistema sejam acessados, baixados ou exibidos para o usuário. | **Ataque/Vulnerabilidade**<br>**2.12) Caminho Reverso (PATH TRAVERSAL)**<br>**6.6) Execução com privilégios desnecessários**<br><br>**Referências**<br>**3.1) Gerenciamento de Arquivos**<br>**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**<br>**2.12) Caminho Reverso (PATH TRAVERSAL)**<br>**2.12) Ataques de enumeração (ENUMERATION)**<br>**2.12) Força Bruta e uso de robôs automatizados**<br><br>**Referências**<br>**3.3) Controle de Acessos**<br>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.**<br><br>**Observação: considerar as diversas formas de representação de um** | **Ataque/Vulnerabilidade**<br>**2.12) Injeção de Comandos (COMMAND INJECTION)**<br>**2.12) Injeção de códigos SQL (SQL INJECTION)**<br>**2.12) Cross-Site Scripting (XSS)**<br><br>**Referências**<br>**3.6) Validação dos dados de Entrada / Saída**<br>**3.7) Segurança em Banco de Dados** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| | **mesmo caractere.** | |
| ☐ | 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**<br>2.12) Upload de arquivos potencialmente perigosos |
| | | **Referências**<br>**3.1) Gerenciamento de Arquivos**<br>**3.3) Controle de Acessos** |
| ☐ | Assegurar que dados sensíveis, credenciais de acesso e *strings* de conexão não sejam fixadas no código fonte. | **Ataque/Vulnerabilidade**<br>**2.12) Senhas incluídas no código fonte do sistema (USE OF HARD-CODED PASSWORD)** |
| | | **Referências**<br>**3.3) Controle de Acessos**<br>**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**<br>**2.12) Senhas incluídas no código fonte do sistema (USE OF HARD-CODED PASSWORD)** |
| | | **Referências**<br>**3.3) Controle de Acessos**<br>**3.5) Autenticação e gerenciamento de credencias** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| ☐ | 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**<br>**2.12) Força Bruta e uso de robôs automatizados**<br><br>**Referências**<br>**3.5) Autenticação e gerenciamento de credencias**<br>**Critérios e Restrições para o uso de senhas: NORMA DE REQUISITOS DE SEGURANÇA PARA CONTROLE DE ACESSO E AUDITORIA NOS SISTEMAS CORPORATIVOS.**<br>**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**<br>**2.12) Interceptação do fluxo de comunicação**<br><br>**Referências**<br>3.4) Gerenciamento de sessões e comunicações<br>**9) Padrões de Criptografia e Funções Hash** |
| ☐ | Definir critérios e especificações de segurança para que dados trafegados por webservices sejam devidamente | **Ataque/Vulnerabilidade**<br>**2.12) Interceptação do fluxo de comunicação** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| | cifrados em nível de mensagem e/ou protegidos por autenticação. | **Referências**<br>3.4) Gerenciamento de sessões e comunicações<br>**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**<br>**2.12) Força Bruta e uso de robôs automatizados**<br><br>**Referências**<br>**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**<br>**2.12) Estouro de Memória (BUFFER OVERFLOW)**<br>**2.12) Estouro de Inteiros (INTEGER OVERFLOW)**<br><br>**Referências**<br>**3.2) Gerenciamento de Memória** |
| ☐ | Verificar se a aplicação está sendo executada com o menor nível de privilégio possível. | **Ataque/Vulnerabilidade**<br>**2.12) Execução com privilégios desnecessários** |

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| | | **Referências**<br>**3.3) Controle de Acessos** |
| ☐ | Assegurar que chamadas a aplicativos externos são realizadas somente a partir de caminhos absolutos. | **Ataque/Vulnerabilidade**<br>**Não relacionado neste documento.**<br>**Link externo:** CWE-114, CWE-427 |
| | | **Referências**<br>**3.1) Gerenciamento de Arquivos** |
| ☐ | Estabelecer mecanismos para manter a aleatoriedade dos identificadores de sessão e revalidar periodicamente os *logins* em utilização.<br><br>Além disso, implementar rotinas para que o sistema não permita *logins* simultâneos de um mesmo usuário. | **Ataque/Vulnerabilidade**<br>**Não relacionado neste documento.**<br>**Link externo:** CWE-330 |
| | | **Referências**<br>**3.3) Controle de Acessos**<br>**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**<br>**Não relacionado neste documento.**<br>**Link externo:** CWE-804 |
| | | **Referências**<br>**3.5) Autenticação e gerenciamento de credencias** |

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | |
|---|---|---|
| ☐ | Assegurar que as *strings* de conexão da aplicação com as bases de dados utilizem usuários específicos e estejam em arquivos devidamente criptografados. | **Ataque/Vulnerabilidade**<br>**Não relacionado neste documento.**<br>**Link externo:** CWE-311, CWE-319 |
| | | **Referências**<br>**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**<br>**Não relacionado neste documento.**<br>**Link externo:** CWE-778 |
| | | **Referências**<br>**3.3) Controle de Acessos**<br>**3.5) Autenticação e gerenciamento de credencias** |

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

**ADENDO 7**

**MATRIZ DE RISCOS**

| Riscos | Definição | Alocação | Impacto | Probabilidade | Mitigação |
|---|---|---|---|---|---|
| 1.Contratado praticar ou participar de ações ilegais ou antiéticas. | O contratado envolve-se em atividades ilegais, antiéticas ou que possam prejudicar a reputação/imagem do Banpará. | Contratado | Alto | Remoto | - Realizar rigorosa fiscalização durante a fase de execução contratual;<br>- Incluir cláusulas contratuais que estabeleçam padrões de conduta e ética. |
| 2.Descumprimento das obrigações contratuais. | O contratado não cumpre as obrigações estabelecidas no contrato assinado. | Contratado | Alto | Ocasional | - Estabelecer cláusulas contratuais claras e detalhadas que definam as obrigações do contratado;<br>- Monitorar regularmente o desempenho da prestação do serviço;<br>- Definir as penalidades contratuais em caso de não cumprimento das obrigações. |
| 3.Desconformidade regulatória, não atendimento às legislações pertinentes ao serviço por | O contratado não cumpre as leis, regulamentos, normativos, instruções ou políticas dos órgãos | Contratado | Alto | Remoto | - Realizar uma *due diligence* completa do contratado antes da assinatura do contrato; |

Este documento foi visto digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

| | | | | | |
|---|---|---|---|---|---|
| negligência ou omissão por parte do contratado. | reguladores, bem como os normativos internos do Banpará, resultando na violação legal ou regulatória. | | | | - Estabelecer cláusulas contratuais que exijam a conformidade regulatória e o cumprimento das políticas internas do Banpará. |
| 4.Embargo ou interdição do serviço por órgão público/reguladores | Suspensão ou paralisação dos serviços por descumprimento das exigências legais. | Contratado | Alto | Remoto | - Monitoramento contínuo da regularidade da contratada perante os órgãos reguladores. |
| 5.Problemas de liquidez financeira. | Empecilhos relacionados ao fluxo de caixa da empresa que impeçam a prestação do serviço. | Contratado | Alto | Remoto | - Exigência de qualificação econômico-financeira adequada ao aporte e prestação do serviço contratado. |
| 6. Licitação deserta. | Quando nenhuma empresa participa do processo licitatório. | Banpará | Médio | Ocasional | - Realizar em todos os canais obrigatórios ampla publicação/divulgação do edital de licitação. |
| 7.Licitação fracassada. | Quando não há empresa com expertise no tipo de contratação. | Banpará | Médio | Ocasional | - Realizar em todos os canais obrigatórios ampla publicação/divulgação do edital de licitação. |

**Obs.:** Este modelo segue os parâmetros estabelecidos no Regulamento de Licitações e Contratos (RILC) do Banpará, Seção 7, artigo 35, item 3:

- Impacto: Alto - Médio - Baixo
- Probabilidade: Frequente - Ocasional – Remoto
- Alocação: Banpará – Contratado - Terceiro – Compartilhado.

Este documento foi vistado digitalmente por MAIRA G A VIEIRA.
Para verificar as assinaturas vá ao site https://portaldeassinaturas.banpara.b.br:443 e utilize o código C1A4-C064-E141-3A19.

# PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Banpará. Para verificar as assinaturas clique no link: https://portaldeassinaturas.banpara.b.br/Verificar/C1A4-C064-E141-3A19 ou vá até o site https://portaldeassinaturas.banpara.b.br:443 e utilize o código abaixo para verificar se este documento é válido.

## Código para verificação: C1A4-C064-E141-3A19

**Hash do Documento**

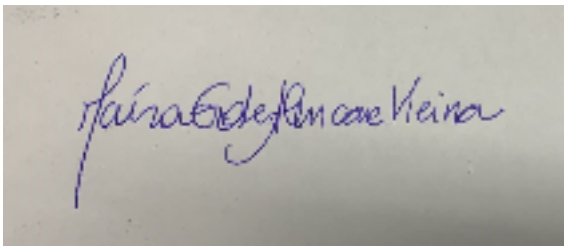
D308E42F9083417CC8B19A1917D27AFA0C4779D29045FCF03D3F0BC1F8253F3B

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 10/01/2024 é(são) :

☑ MAIRA G A VIEIRA - ***.226.282-** em 10/01/2024 16:34 UTC-03:00
**Tipo:** Assinatura Eletrônica
**Identificaçao:** Autenticação de conta

**Evidências**

**Client Timestamp** Wed Jan 10 2024 16:34:33 GMT-0300 (GMT-03:00)
**Geolocation** Latitude: -1.4209375 Longitude: -48.4815276 Accuracy: 48.9
**IP** 10.0.1.184
**Assinatura:**



**Hash Evidências:**

44A39222F1C511EA877BBEE4AC345CDDA2F9A4A5671626D66E7CC0E2B40ACA89