

ANEXO I**TERMO DE REFERÊNCIA****1 DO OBJETO**

- 1.1 Prestação de serviços de solução integrada de cartões de débito, para personalização, manuseio, folheteria, envelopamento, inserção de folder, inclusive em braille, gravação de chip na tecnologia *Dual Interface (Chip e Contactless)*, com ou sem tarja magnética, expedição nos Correios ou outra empresa de logística definida pela CAIXA, com abrangência nacional.
- 1.2 A solução integrada deste Termo de Referência compreende:
- 1.2.1 Fornecimento do cartão plástico contendo chip, com a tecnologia *Dual Interface*, com ou sem tarja magnética, expedição nos Correios ou outra empresa de logística definida pela CAIXA.
- 1.2.1.1 Gravação de dados na tarja magnética, inicialização e personalização do chip e personalização do cartão em termografia (na frente e/ou verso do cartão), alto relevo, ou DOD (*Definition of Done*), assim consideradas também as variações de propriedade das Bandeiras que operam ou vierem a operar, ou sejam requisitadas pela CAIXA.
- 1.2.2 Fornecimento da folheteria que compõe os pacotes de comunicação, incluindo, mas não se restringindo aos pacotes de boas-vindas, considerando também aqueles destinados a portadores de deficiência visual e que atendam determinações legais.
- 1.2.3 Personalização do porta cartão, envelope e quaisquer outros documentos que venham a ser exigidos para a triagem, no padrão dos Correios ou fornecedor de serviços logísticos definido pela CAIXA.
- 1.2.4 Montagem e manuseio dos pacotes de comunicação, incluindo e não se limitando aos pacotes de boas-vindas, manuseio de envelopes, inserção de porta-cartões, folders, prospectos, encartes, filipetas, contratos, etiquetas adesivas e demais documentos que venham a fazer parte do pacote.
- 1.2.5 Preparação e postagem: preparação e entrega dos movimentos já processados, com separação dos cartões de acordo com o plano de triagem definido pelos Correios ou por fornecedor do serviço logístico contratado pela CAIXA.
- 1.2.6 Relatórios: Troca de arquivos magnéticos com a CAIXA, elaboração e disponibilização de relatórios, portal e painéis (*dashboard*) com acesso remoto via internet, para controle dos serviços e disponibilização de informações relativas a produção, estoque e a postagem dos cartões, considerando as especificações técnicas e de segurança, nos prazos

dispostos no Contrato.

1.2.7 Informações a serem enviadas de uma parte a outra, que requeiram sigilo, como por exemplo, dados de clientes da CAIXA, precisam ser criptografadas utilizando algoritmos e tamanhos de chave conforme PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC ICP – 01.01, disponível no site do Instituto de Tecnologia da Informação na Internet, ou algoritmos e tamanhos de chaves aprovados pelo NIST (*National Institute of Standards and Technology*) ou pelo padrão EMV (*Europay, Mastercard and VISA*).

1.2.8 Na criptografia citada, devem ser utilizados equipamentos HSM, padrão FIPS 140-2 Nível 3, ou outros que vier a substituir.

2 DO DETALHAMENTO DO OBJETO

2.1 QUANTIDADE ESTIMADA

2.1.1 A quantidade estimada do objeto é 40.000.000 (quarenta milhões) de cartões plásticos no modelo *Dual Interface (chip e contactless)*, para o período de 24 (vinte e quatro) meses e está distribuída em 3 (três) itens, conforme detalhamento a seguir:

ITEM	DESCRIÇÃO DO ITEM	QUANTIDADE
I	Cartões de Débito Dual Interface (Chip e Contactless)	13.333.333
II	Cartões de Débito Dual Interface (Chip e Contactless)	13.333.334
III	Cartões de Débito Dual Interface (Chip e Contactless)	13.333.333

2.1.1.1 A emissão de cartões, inclusive quanto à variação de bandeiras, será realizada a critério da CAIXA, conforme necessidade do negócio, sem custos adicionais para a CAIXA.

2.1.2 A distribuição entre os produtos e serviços contratados poderá ser alterada a critério da CAIXA, observando a volumetria global do contrato, capacidade contratada e a legislação.

2.1.2.1 O fornecedor deverá garantir capacidade diária de produção e postagem **mínima de 50.000 (cinquenta mil) cartões e mensal de 1.500.000 (um milhão e quinhentos mil) cartões**, de forma a suportar o movimento normal e eventuais ações de maior emissão definidas pela CAIXA.

2.1.2.1.1 O percentual diário / mensal de produção, poderá ser alterado pela CAIXA definitivamente e/ou temporariamente conforme item 2.1.2.1.

- 2.1.2.2 A capacidade diária de produção e postagem mínima exigida não configura a obrigatoriedade de utilização deste total pela CAIXA, mas uma referência de capacidade produtiva.
- 2.1.3 Nos casos em que a expectativa de variação exceder a média histórica da emissão de cartões dos últimos 90 (noventa) dias, a CAIXA comunicará à CONTRATADA, que deverá reorganizar a nova capacidade produtiva em até 30 (trinta) dias.
- 2.1.3.1 Na hipótese de existirem quaisquer impedimentos para o atendimento, mesmo que temporários, a CONTRATADA comunicará imediatamente a CAIXA.
- 2.1.3.1.1 A comunicação de que trata o subitem acima, não eximirá a CONTRATADA de atender a demanda da CAIXA, sob pena de aplicação das sanções previstas no contrato.
- 2.1.4 A CAIXA realizará os pagamentos das despesas de postagem do objeto contratual enviados pelos Correios ou empresa de serviços logísticos definida pela CAIXA.
- 2.1.4.1 A qualquer tempo a CAIXA poderá requerer à CONTRATADA, a recepção de materiais (encartes e outros impressos) fornecidos pela CAIXA ou empresas por ela autorizadas, para inserção e remessa junto com os pacotes de comunicação, sem ônus adicionais, podendo excepcionalmente solicitar, também, a transferência de material de uma CONTRATADA para outra.
- 2.1.5 A seu critério, a CAIXA poderá estabelecer condições diferenciadas de manuseio, expedição e postagem do objeto contratual, inclusive quanto aos itens que compõem a produção do cartão e pacote de comunicação, com 30 (trinta) dias de antecedência.
- 2.1.6 Do volume total estimado, até 0,005% dos cartões deverá ser produzido em alto relevo ou (*Braille*), não configurando a obrigatoriedade de utilização deste total pela CAIXA, mas uma referência de capacidade produtiva.
- 2.2 ESPECIFICAÇÕES TÉCNICAS E CONDIÇÕES DE PRESTAÇÃO DOS SERVIÇOS**
- 2.2.1 Personalização**
- 2.2.1.1 Cartão de débito**
- 2.2.1.1.1 Fornecimento de cartão plástico em PVC reciclado laminado e semirrígido com acabamento em película de vinil (cristal ou fosca).
- 2.2.1.1.1.1 O PVC reciclado deverá conter 100% (cem por cento) deste tipo de material em sua origem.

- 2.2.1.1.2 Serviço de personalização de cartão com impressão de até 08 cores *offset* determinadas pela CAIXA, respeitando as especificações constantes nos arquivos fornecidos pela CAIXA. Além das seguintes cores especiais, Azul (Pantone 287) e Laranja (Pantone 151).
- 2.2.1.1.2.1 As cores *offset* e as cores especiais podem sofrer alteração durante a vigência do contrato, considerando a necessidade da CAIXA de criar ou alterar a linha visual dos seus cartões de débito.
- 2.2.1.1.3 Os cartões deverão ser personalizados utilizando os hologramas aprovados pelas bandeiras com as quais a CAIXA opera ou venha a operar.
- 2.2.1.1.3.1 Atualmente, a bandeira Elo exige holograma em todos os seus cartões de débito.
- 2.2.1.1.4 O nome da empresa responsável pelo serviço de personalização, juntamente com o número do lote de produção, deve ser impresso na lateral direita do verso do cartão acompanhado da data (MM/AA).
- 2.2.1.1.4.1 Alternativamente, em casos excepcionais e com a anuência da CAIXA, a impressão do nome da empresa poderá constar em outro local do cartão, em virtude de limitações de espaço, em razão das aplicações de Bandeiras, hologramas ou demais situações relacionadas.
- 2.2.1.1.5 Todos os cartões e seus respectivos chips, antenas e fitas magnéticas deverão ter durabilidade mínima de 60 meses.
- 2.2.1.1.6 Formato do cartão CR-80, conforme os padrões da Norma ISO/IEC 7810, com espessura 0,76 mm com tolerância de +/- 0,08 mm, altura de 53,98 mm com tolerância de +/- 0,055 mm e 85,60 mm de comprimento, com tolerância de +/- 0,125 mm, cantos arredondados com raio de curvatura de aproximadamente 3,2 mm, sendo o nominal do raio de 3,18 mm com tolerância de +/- 0,3 mm.
- 2.2.1.1.7 Deve conter o indicador *Contactless*, conforme especificado pela EMVco e deve estar aderente às especificações e orientações de Card Design de suas respectivas Bandeiras.
- 2.2.1.1.8 A arte do cartão deverá ser impressa por processo de alto-relevo ou termografia com material ou tinta que não prejudique o correto funcionamento da interface *contactless*, no que diz respeito à geração e amplitude do campo eletromagnético gerado pela antena.
- 2.2.1.1.9 Os cartões conterão os dados variáveis de personalização em uma das faces do plástico e códigos de segurança (CVV/CVC/CVE) no verso do cartão.
- 2.2.1.1.9.1 A CAIXA poderá solicitar a seu critério a inclusão de QRCode para cada modelo dos cartões (verso) a serem produzidos.

2.2.1.2 Chip

- 2.2.1.2.1 Inicialização e personalização do chip com padrão EMV 4.3 ou superior, nas cores prata e/ou dourada, sendo predominantemente na cor dourada, seguindo as especificações definidas pela CAIXA e/ou Bandeiras, com modelos e fornecedores homologados, permitindo a utilização da tecnologia **O.D.A, S.D.A, C.D.A, D.D.A e/ou fD.D.A – Dual Interface** (a depender da Bandeira a ser emitida) para os cartões.
- 2.2.1.2.2 O chip fornecido seguirá as especificações apresentadas pela CAIXA e em conformidade com as determinações das Bandeiras, com memória mínima de 16KB ou outra definida pela CAIXA.
- 2.2.1.2.3 Os chips deverão estar aderentes às especificações de cada Bandeira, em suas versões atualizadas e compatíveis com a tecnologia aprovada pelas respectivas Bandeiras.
- 2.2.1.2.4 Os chips não deverão apresentar nenhuma identificação externa de seu fabricante ou empresa fornecedora.
- 2.2.1.2.5 A CONTRATADA deverá informar à CAIXA, no prazo mínimo de 90 (noventa) dias, antes do vencimento do chip, a intenção de validação de um chip substituto.

2.2.1.3 Tarja Magnética

- 2.2.1.3.1 Aplicação de banda magnética de alta coercitividade (HICO de pelo menos 2750 Oe), na cor preta ou prata ou dourada, em cores sólidas, tom sobre tom (em contraste a cor de fundo do cartão) ou customizado, com tolerância na variação de tonalidade de $\pm 15\%$, com distância máxima de 5,54 mm da margem superior do cartão à margem superior da banda magnética e distância mínima de 15,82 mm da margem superior do cartão à margem inferior da banda magnética, conforme norma ISO 7811/6 vigente e suas atualizações.
- 2.2.1.3.2 É indispensável que a banda magnética apresente um alto padrão de qualidade, isenta de falhas, rebarbas, materiais abrasivos, riscos, arranhões, má aderência, ou qualquer outra imperfeição que altere ou impeça a sua funcionalidade.
- 2.2.1.3.3 A cor da tarja magnética será especificada conforme detalhamento do card design específico para os tipos de cartões, majoritariamente nas cores prateada e preta.
- 2.2.1.3.4 Todos os cartões deverão apresentar conformidade com as normas ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7813 (Service Center), ISO/IEC 7816 (Service Center / Manufatura), ou, outras normas que vierem a substituir.

2.2.1.4 Pacote de Comunicação

2.2.1.4.1 As definições e especificações técnicas das peças de folheteria que compõem cada pacote, bem como demais variações do objeto contratual e itens que o integram e complementam estão descritas a seguir.

2.2.1.4.2 Por decisão da CAIXA poderão ser alterados os padrões dos pacotes de comunicação.

2.2.1.5 Porta Cartão

2.2.1.5.1 Papel: Carta 216 mm x 279 mm ou A4 210 mm x 297 mm, *offset*, reciclado ou de reflorestamento certificado, de 90g/m² a 150g/m², via única.

2.2.1.5.2 Formato: respeitando as especificações fornecidas pela CAIXA e aprovações dos arquivos de provas física e digital.

2.2.1.5.3 Impressão: em frente/verso respeitando as especificações fornecidas pela CAIXA e aprovações dos arquivos de provas física e digital.

2.2.1.5.4 Acabamento: sem dobra ou com dobra “V”, “U” ou “Z”, inserção/fixação do cartão que poderá ser feita por colagem, fita dupla face ou inserção em corte em V de acordo com a especificação da CAIXA.

2.2.1.5.5 Poderá ser solicitada a inserção/fixação do cartão no porta-cartão por outros métodos mediante solicitação da CAIXA.

2.2.1.5.6 Janela de endereçamento: espaço para impressão de dados variáveis do remetente, destinatário e controle de registro de postagem, de acordo com padrão da empresa de logística definida pela CAIXA, de modo a observar os limites das janelas do envelope tornando os dados visíveis externamente, além de outras informações especificadas nas provas físicas e digitais homologadas.

2.2.1.5.7 O porta-cartão deve ser ajustado no envelope, preservando a visibilidade dos dados dispostos na janela de endereçamento e leitura pela empresa de logística definida pela CAIXA.

2.2.1.6 Folder, Encarte e Filipeta

2.2.1.6.1 Papel: *offset*, reciclado ou de reflorestamento certificado, de 90g/m² a até 150g/m², via única.

2.2.1.6.2 Formato: respeitando as especificações fornecidas pela CAIXA e aprovações dos arquivos de provas física e digital.

2.2.1.6.3 Impressão: *offset*, frente/verso, respeitando as especificações fornecidas pela CAIXA e aprovações dos arquivos de provas física e digital.

2.2.1.6.4 Acabamento: sem dobra ou com dobra “U”, “V” ou “Z”.

2.2.1.7 **Envelope**

2.2.1.7.1 Envelope em papel: *offset* opaco, na cor branca ou reciclado, de 75g/ m² de reflorestamento, com certificação FSC, sem janela ou com uma ou duas janelas de acetato incolor, impressão em tinta preta para os cartões.

2.2.1.7.1.1 Dimensões: 114 mm (altura) x 240 mm (largura).

2.2.1.7.2 Das Janelas de endereçamento:

a) Envelope sem janela – Colagem de etiqueta de destinatário e remetente;

b) Envelope com 1 janela – remetente – 30 mm x 120 mm, para permitir a visualização dos dados do remetente que serão impressos no porta-cartão;

c) Envelope com 2 janelas – remetente – 30 mm x 120 mm e destinatário – 40 x 120 mm, para permitir a visualização dos dados de endereçamento que serão personalizados no porta-cartão.

2.2.1.7.2.1 Havendo necessidade a CAIXA pode determinar a alteração das dimensões das janelas.

2.2.1.7.3 O fechamento dos envelopes em papel deverá ser do tipo bancário ou diagonal, que impossibilite violação da correspondência.

2.2.1.7.4 Dados de uso exclusivo do fornecedor de serviços logísticos definido pela CAIXA impressos no anverso.

2.2.1.7.5 Dados de uso exclusivo do fornecedor de serviços logísticos definido pela CAIXA, em etiqueta afixada no anverso.

2.2.1.7.6 A impressão dos dados do envelope em papel e na etiqueta utilizada em envelope plástico, deve ser na cor preta, ou conforme definição estabelecida pela CAIXA.

2.2.1.8 **Etiqueta Adesiva**

2.1.1.8.1 Confecção de etiquetas adesivas: para cartão.

2.1.1.8.2 No cartão deve ser fixada etiqueta adesiva de desbloqueio em formato a ser definido pela CAIXA, impressão: 2/0, em papel couchê gloss de papel reciclado ou de reflorestamento certificado, com adesivo removível, que não deixe resíduo no plástico, contendo os dados informados em arquivo enviado pela CAIXA.

2.1.1.9 **Pacote Braille**

2.1.1.9.1 O pacote Braille deve seguir os padrões de produção, impressão e postagem

estabelecidos pela CAIXA, em cumprimento à Legislação específica vigente.

2.1.1.9.2 A impressão em Braille deverá observar, no mínimo, o disposto na Portaria MEC nº 2.678/2002 e a Lei Nº 13.835/2019, publicada em 04 de junho de 2019, que trata da Grafia Braille para a Língua Portuguesa, ou qualquer legislação que atualize as normas de grafia em Braille, como também a Associação Brasileira das Empresas de Cartões de Crédito e Serviços – ABECS, seguindo as definições fornecidas pela CAIXA.

2.1.1.10 **Cartão: Embossing em alto relevo – Braille**

2.1.1.10.1 Cartão em PVC reciclado, com informações em Braille: sigla do banco, bandeira, função (débito), o número completo do cartão, data de validade e o nome do cliente, em alto relevo.

2.1.1.10.2 Kit de boas-vindas: contém filipeta de boas-vindas, com informações essenciais sobre o cartão de débito em letra de tamanho ampliado para facilitar a visualização daqueles que possuem diminuição da visão. Deve ser personalizado em Braille e impressão de escrita especial para atendimento aos portadores de deficiência visual, respeitando as especificações fornecidas pela CAIXA e aprovações dos arquivos de provas física e digital.

2.1.1.10.2.1 Deve ser ajustado no envelope revestido em plástico bolha preservando a visibilidade dos dados dispostos na janela de endereçamento (se for o caso) e leitura pela empresa de logística definida pela CAIXA.

2.1.1.11 **O Kit Braille deverá conter:**

2.1.1.11.1 O porta-cartão em Braille e alto relevo, que terá a função de capeá-lo (cartão de débito mais 2 cartões acessórios em PVC), tendo ainda as informações do número completo do cartão, do tipo de cartão, da Bandeira, do nome do Emissor, da data de validade, do código de segurança e do nome do portador do cartão.

2.1.1.11.1.1 O porta-cartão deverá possuir tamanho suficiente para que constem todas as informações descritas e deverá ser conveniente ao transporte pela pessoa com deficiência visual.

2.1.1.11.2 Etiqueta produzida com filme transparente afixado ao referido plástico, contendo as informações em Braille, com a identificação do tipo do cartão e os 06 dígitos finais do número do cartão.

2.1.1.11.2.1 Esta etiqueta deverá estar posicionada na face frontal do cartão, com tamanho 52 X 12 milímetros, a cerca de 17 milímetros da borda superior, bem como dois milímetros da borda esquerda e utilizar mais ou menos 2% de tolerância para o físico e para o local da sua fixação.

2.1.1.11.2.2 Para a fixação da etiqueta, haverá uma fita adesiva com composição “linear” de proteção siliconizada, filme de polipropileno e adesivo acrílico aderente nas duas faces e que suporte temperatura de até 30 graus Celsius.

2.1.1.11.3 Os procedimentos definidos nos itens 2.2.1.9 e 2.2.1.10, permitem o uso completo do cartão, não requerendo nenhuma alteração no layout ou no emboço dos cartões.

2.1.1.11.4 O porta-cartões e/ou a etiqueta pode(m) ser suprimido(s) se as informações constantes estiverem emboçadas diretamente no instrumento de pagamento.

2.1.1.11.5 O prospecto de informações essenciais deverá ser enviado em Braille ou em caracteres ampliados, de acordo com a opção do portador deficiente visual, ou alternativamente em mídia de áudio.

2.1.1.12 Envelope - Kit Braille

2.1.1.12.1 O envelope para encarte do porta-cartão em Braille deve ter tamanho que acomode o material sem dobras e ter resistência suficiente para que a impressão do Braille não seja prejudicada.

2.1.1.12.2 Em envelope com dimensão de no mínimo de 110 mm(altura) x 225 mm(largura) e máximo de 114 mm(altura) x 240 mm(largura) contendo duas janelas, medindo 44 x 120 mm, para permitir a visualização dos dados da destinatária e do remetente com gramatura 90g/m², impressão 1/1.

2.1.1.12.3 O envelope para o kit Braille, deverá ser confeccionado em plástico reciclado, e com acabamento interno em plástico bolha.

2.1.1.12.4 O envelope para o kit Braille deverá ser branco, revestido com plástico bolha, impresso 1 cor, formato 311mm x 226 mm. Incluso IPI e fita dupla face automatizada medindo 5 cm x 2 cm (colada na vertical do envelope) . Gramatura 90g/m² , impressão 1/1.

2.1.1.12.5 Os dados do destinatário e remetente serão inseridos em etiqueta adesiva para colagem no envelope plástico sem janela ou serão inseridos no Aviso de Recebimento (AR), quando houver, seguindo os padrões especificados para cada tipo de cartão, respeitando as especificações constantes nos arquivos fornecidos e homologados pela CAIXA.

2.1.1.13 Filipeta de boas-vindas – kit Braille

2.1.1.13.1 Papel alcalino Laser Print (Papel certificado - ou reciclado) e gramatura 90 g/m² no formato A4 (21x297 mm) sem dobra ou com dobra “U”, “V” ou “Z” com impressão em CMYK 4/4.

2.1.1.14 Capa Protetora – kit Braille

2.1.1.14.1 Confeccionada em papel, plástico ou qualquer outro material reciclado que apresente durabilidade equivalente a 10 (dez) anos.

2.1.1.14.2 Deve apresentar dimensões suficientes para comportar três cartões (um em cima e dois embaixo), com limites máximos de 56 mm de altura, 88 mm de largura e 1,2 mm de espessura. A parte interna deve possuir duas bolsas, parte inferior e superior, para acomodação dos cartões e deve ser em material transparente que permita a leitura das informações dos cartões em PVC.

2.1.1.14.3 A parte externa da capa protetora deve ser em material que permita a afixação de peça de PVC (formato de cartão), o qual terá informações impressas em alto relevo.

2.1.1.14.4 Os cartões em PVC nas dimensões do cartão de débito devem conter os seguintes dados do cartão/clientes impressos em Arial 24:

a) *Primeiro Cartão informativo:*

- Nome do cliente em até duas linhas - até 12 caracteres, tal qual como descrito no cartão;
- Nome do banco;
- Nome da bandeira do cartão.

b) *Segundo Cartão Informativo:*

- Número completo do cartão em duas linhas com até 12 caracteres em cada linha;
- Data de validade no formato MM/AA;
- Código de segurança.

2.1.1.14.5 Esse conjunto será acondicionado em envelope plástico com revestimento bolha, com ou sem a inserção de Contrato em áudio e endereçado com etiqueta do destinatário impressa pela CONTRATADA.

2.2.1.15 Pré – Emboçado

2.2.1.15.1 Os cartões poderão, conforme estratégia da CAIXA, serem emitidos na modalidade pré-emboçado, que corresponde a até 15% (quinze por cento) do volume global estimado, conforme item 2.1.1 acima, com as mesmas características, no que tange ao plástico a exceção dos campos: nome do cliente e número da conta, que deverão ser apresentados sem informações.

2.2.1.15.2 O fornecedor deverá garantir que o acondicionamento dos cartões pré-emboçados seja realizado de forma adequada, contendo etiquetas para identificação, expedição e triagem. As etiquetas deverão contemplar, no mínimo, as seguintes informações:

- Nome do banco;

- Nome do kit emboçado;
- Código da unidade;
- Endereço completo;
- Número do lote acompanhado de código de barras.

2.2.1.15.3 As informações descritas poderão ser ajustadas conforme necessidade da CAIXA, mediante solicitação formal.

2.2.1.15.4 Para esses cartões serão utilizados:

2.2.1.15.5 Porta-cartão conforme item 2.2.1.5, onde o campo destinatário deverá ter as seguintes informações: nome do banco, nome do kit emboçado, endereço, número do cartão, data de vencimento do cartão, código alfanumérico (13 posições), ou outro modelo solicitado pela CAIXA.

2.2.1.15.6 O Envelope deverá possuir apenas a janela do destinatário. A janela do box de endereçamento no formato: 120 mm x 65 mm, conforme item 2.2.1.7.

2.2.1.15.7 Os Envelopes deverão ser acondicionados em Voids - tamanho 'G' (de 100 a 300 objetos): com 62 cm de largura x 62 cm de altura) e estes em sacos de ráfias de até 30Kg.

2.2.1.15.8 Etiqueta conforme item 2.2.1.8.

2.2.1.15.9 Os cartões pré-emboçados deverão ser manuseados e separados conforme estratégia definida pela CAIXA, sendo endereçado por meio de lote único ou diversos.

2.2.1.15.10 Os cartões pré-emboçados poderão ser emitidos em quaisquer das Bandeiras e variantes, sendo essas definidas de acordo com a estratégia da CAIXA e comunicadas à CONTRATADA.

3 DO MANUSEIO E PREPARAÇÃO DOS CARTÕES

3.1 Os pacotes de comunicação devem ser personalizados com os dados do destinatário e do remetente - como informado no arquivo de dados transmitido pela CONTRATANTE e especificações dos Correios, ou empresa de logística definida pela CAIXA.

3.2 Os dados do destinatário e remetente podem ser inseridos em etiqueta adesiva para colagem no envelope plástico ou serão inseridos no porta-cartão e no Aviso de Recebimento (AR), quando houver, seguindo os padrões especificados para cada tipo de cartão, respeitando as especificações constantes nos arquivos fornecidos e homologados pela CAIXA.

3.3 A CONTRATADA deve utilizar sistemas de auditoria interna, com a finalidade de redução dos riscos de inserção duplicada no mesmo envelope, falta de documentos, inversão dos dados variáveis ou qualquer outro risco de

manuseio, programação, ajuste, recarga de maquinário e/ou processo de envelopamento, aplicação do *Chip*, personalização, gravação e postagem de sua linha de produção, sendo o manuseio passível de inspeção pela CAIXA a qualquer momento.

- 3.4 Os cartões devem ser inseridos/fixados no porta-cartão, envelopados, triados, preparados para remessa e entregues aos Correios ou empresa de logística indicada pela CAIXA.

4 DA TRIAGEM E POSTAGEM DOS CARTÕES

- 4.1 Os volumes deverão ser triados de acordo com sistema definido pela CAIXA em conjunto com os Correios ou empresa de logística indicada pela CAIXA, devendo a CONTRATADA atender de forma tempestiva eventuais alterações nos planos de triagem e postagem.
- 4.2 Os volumes deverão ser entregues pela CONTRATADA, na modalidade Remessa Econômica, Expressa ou outra que a CAIXA determinar, com Aviso de Recebimento (AR), utilizando o contrato firmado entre a CAIXA e os Correios, ou outra empresa de logística indicada pela CAIXA.
- 4.3 Caso seja necessário, a CONTRATADA deverá estabelecer conexão com os Correios ou com empresa de logística definida pela CAIXA, para realizar a troca de arquivos e atualização do *status* de postagem.
- 4.4 Os envelopes devem conter impressa a identificação do serviço de remessa contratado e número do contrato CAIXA/Correios, ou empresa de logística definida pela CAIXA, fornecidos por esta, e preparados para postagem com AR ou equivalente, respeitando as especificações constantes nos arquivos de provas física e digital fornecidos e homologados pela CAIXA.
- 4.5 Quando o arquivo enviado pela CAIXA de documentos a serem produzidos/postados possuir mais de uma localidade de postagem, sua segmentação por faixas de CEP, para atender a postagem nas localidades/regiões, definidas neste Termo de Referência e demais anexos é de responsabilidade da CONTRATADA.
- 4.6 A adequação sistêmica e operacional para eventuais localidades a serem incluídas ou suprimidas posteriormente para postagem, são de responsabilidade da CONTRATADA sem qualquer ônus adicional à CAIXA.
- 4.7 Documentos destruídos e/ou danificados durante o processo produtivo serão de responsabilidade da CONTRATADA, devendo essa garantir a entrega total dos produtos para a CAIXA sem ônus adicionais.
- 4.8 Os custos de postagem dos cartões são de responsabilidade da CAIXA e, para tanto, a CONTRATADA receberá o cartão de postagem e a autorização para realizar a entrega dos cartões ao representante dos Correios ou empresa de logística definida pela CAIXA.

- 4.8.1 Devem ser obedecidos os quesitos e parâmetros dos Correios ou empresa de logística definida pela CAIXA para não ocorrer custos adicionais à CAIXA.
- 4.8.1.1 A CONTRATADA deverá comunicar ao representante dos Correios ou empresa de logística definida pela CAIXA eventual necessidade de tipo de veículo mais adequado à coleta em volumes superiores às médias regulares.
- 4.9 A CONTRATADA responsabilizar-se-á pelos controles de entrega dos objetos, bem como, por garantir os procedimentos de segurança e sigilo, no encaminhamento dos objetos para postagem.
- 4.10 Em hipótese alguma poderá ser utilizado o contrato CAIXA/Correios ou de empresa de logística definida pela CAIXA para postagem de outras encomendas que não sejam objeto deste instrumento, e em verificando-se a postagem indevida de objetos não autorizados pela CAIXA, caberá à CONTRATADA o ressarcimento decorrente do mau uso do contrato.
- 4.11 O prazo máximo de postagem dos cartões personalizados pela CONTRATADA está descrito no item cinco deste Termo de Referência.
- 4.11.1 Em casos excepcionais, que necessitem de ajustes nos prazos, estes devem ser acordados previamente entre a CONTRADADA e a CAIXA.
- 4.12 Antes do início das postagens dos cartões e sem prejuízo aos prazos previstos neste termo, a CONTRATADA deverá realizar os testes requeridos nos prazos estipulados pelos Correios ou empresa de serviços logísticos definida pela CAIXA.
- 4.13 Após a entrega nos Correios ou empresa de logística contratada pela CAIXA, a CONTRATADA deverá retirar a Lista de Postagem e a Notificação de Recebimento (NR) devidamente assinadas para arquivo físico e disponibilização em ambiente WEB para consulta da CAIXA a qualquer tempo.
- 4.14 A CONTRATADA, na condição de preposta da CAIXA perante os Correios ou empresa de logística contratada pela CAIXA, terá a responsabilidade pela assinatura das Listas de Postagem e das Notificações de Recebimento (NR).
- 4.15 A CONTRATADA indicará à CAIXA os responsáveis pela assinatura das Listas de Postagem e Notificações de Recebimento (NR) para que a CAIXA informe aos Correios ou empresa de logística contratada pela CAIXA.

5 DOS PRAZOS DE ATENDIMENTO E ENTREGA

- 5.1 Os prazos, em dias úteis, para atendimento e postagem que deverão ser praticados pela CONTRATADA, depois da solicitação via arquivo enviado pela CAIXA, para personalização dos cartões, com o recebimento na íntegra confirmado pela CONTRATADA, serão de:

- D+1 para o movimento emergencial e private;
- D+2 para o movimento diário (emissão / reemissão);
- D+3 para a contratação em lote e kit Braille;
- D+10 (dez) para renovação.

- 5.1.1 O primeiro dia de recebimento dos arquivos pela CONTRATADA (dia “D”) será considerado o dia de recepção até as 11:59:59 (onze horas, cinquenta e nove minutos e cinquenta e nove segundos).
- 5.1.2 Arquivos recebidos pela CONTRATADA a partir das 12 (doze) horas, o (dia “D”) será considerado o dia útil seguinte.
- 5.2 Não serão considerados dias úteis, além dos finais de semana, os feriados nacionais.
- 5.3 No caso de movimento emergencial, respeitadas as condições de produção da CONTRATADA, será feito o envio de arquivo especial, separado do movimento normal.
- 5.4 A CONTRATADA poderá receber solicitações da CAIXA para retenção de cartão durante o processo produtivo, para retenção e remessa diretamente à CAIXA ou outro endereço por ela indicado sem ônus adicional.
- 5.5 Serão considerados os prazos acima informados, independentemente da existência de feriados locais, sejam municipais e/ou estaduais.

6 MONTAGEM DE ESTOQUE BASE PELA CONTRATADA

- 6.1 A CAIXA disponibilizará à CONTRATADA os subsídios, incluindo, mas não se restringindo às imagens e especificações, sem quaisquer custos à CONTRATADA, necessários à confecção das provas digitais e físicas, de card design e de Folheteria.
- 6.2 Após a homologação da CAIXA a CONTRATADA deverá produzir estoque base, nas quantidades apresentadas pela CAIXA, quando da celebração do Contrato entre as Partes.
- 6.2.1 O estoque base inicial, nas quantidades estimadas pela CAIXA, deverá ser preparado no prazo máximo de 30 (trinta) dias corridos após a assinatura do contrato e homologação do *card design*, podendo ser prorrogado por mais 30 dias mediante solicitação fundamentada da CONTRATADA, com antecedência de 10 (dez) dias corridos e com a aprovação da CAIXA.
- 6.2.1.1 O estoque inicial de quaisquer novos produtos ou necessidades da CAIXA no decorrer do contrato, deverá ser atendido pela CONTRATADA no prazo 20 (vinte) dias corridos após a assinatura do contrato e homologação do *card design*, podendo ser prorrogado mediante solicitação fundamentada da

CONTRATADA, com antecedência de 10 (dez) dias corridos e com a aprovação da CAIXA.

- 6.2.1.2 A produção do estoque base tem como objetivo disponibilizar o volume mínimo para início da operação, sendo a CAIXA responsável por informar, antecipadamente, a necessidade de alteração da projeção.
- 6.2.1.3 Após o estoque inicial a empresa deverá garantir estoque para atender a produção de 60 dias, considerando sempre o histórico de produção dos últimos 60 dias, podendo a CAIXA sinalizar a qualquer momento a necessidade de formação de um maior estoque ou menor para atender eventuais alterações na estratégia de comercialização dos produtos.
- 6.3 Na recomposição/reposição do estoque base de cartões e/ou folheterias dos pacotes de comunicação a CONTRATADA deverá enviar 05 (cinco) amostras de cada item para a CAIXA, com envelopamento ou não, conforme solicitação da CAIXA.
- 6.4 A CONTRATADA deverá apresentar, a contar da data de solicitação, sem quaisquer custos de produção à CAIXA, provas digitais e físicas, de *card design*, por meio de FAP ou PAP e folheteria, inclusive do material Braille, nos prazos e quantidade de vias a seguir:
- CARD DESIGN
Quantidade de vias – 4 (quatro) unidades;
Prazo para provas digitais – 7 (sete) dias corridos;
Prazo para provas físicas – 10 (dez) dias corridos.
- FOLHETERIA
Quantidade de vias – 4 (quatro) vias;
Prazo para provas digitais – 7 (sete) dias corridos;
Prazo para provas físicas – 10 (dez) dias corridos.
- 6.4.1 As provas físicas e digitais de card design, devem conter pelo menos 3 amostras frente e verso demonstrando a variação da tonalidade dos plásticos.
- 6.5 Eventuais alterações na arte dos *card design* e/ou folheterias serão disponibilizadas pela CAIXA com antecedência mínima de 03 (três) dias corridos, para produção e disponibilização das provas digitais e/ou físicas, conforme prazo estabelecido no subitem 6.2.
- 6.6 O disposto nos subitens 6.2, 6.2.1 e 6.3 são aplicáveis aos novos produtos ou *card designs* e folheterias modificados pela CAIXA.
- 6.7 Uma vez aprovados pela CAIXA os modelos de card design, porta cartão, folheteria, entre outros, permanecerão vigentes até que haja nova alteração pela CONTRATANTE.

- 6.8 A CAIXA comunicará alterações de estratégia de bandeiras ou suspensão de modelos com 60 (sessenta) dias de antecedência, data na qual deverão ser suspensas novas produções e informado à CAIXA o estoque já montado.
- 6.9 A CAIXA não se responsabilizará por eventual saldo remanescente de estoque dos produtos contratuais gerados pela CONTRATADA em desacordo com o formato estipulado no contrato e respectivos anexos, sejam estes produtos acabados ou inacabados / parcialmente concluídos, especialmente após o encerramento do Contrato.
- 6.9.1 Em caso de saldo remanescente de estoque de produtos, mesmo que inacabados / parcialmente concluídos, gerados por solicitação expressa da CAIXA, de acordo com as previsões estabelecidas no contrato e respectivos anexos, estes serão remunerados em função da proporção de acabamento rateados conforme a planilha de composição de custos.
- 6.9.2 Quando da ocasião do encerramento do contrato, cabe a CONTRATADA apresentar eventual saldo remanescente no mesmo momento do último faturamento previsto, pois não será possível faturamentos posteriores diante da finalização do contrato.

7 DA GRAVAÇÃO DOS CARTÕES

- 7.1 A gravação, inicialização/personalização do cartão deverá ser feita com base no arquivo enviado pela CAIXA, obedecendo aos padrões previamente aprovados.
- 7.2 A personalização dos cartões deverá ser feita pelo processo de alto-relevo ou termografia, conforme especificações do *card design*, limites estabelecidos no presente Termo, na cor definida na especificação de cada tipo de cartão.
- 7.3 Para geração dos cartões de teste, que será realizada sob demanda, não sendo necessária a geração de estoque, a CONTRATADA deverá fornecer à CAIXA, sem custos, a quantidade de 500 (quinhentas) unidades por lote, ao ano, necessárias à homologação junto às Bandeiras e aos canais internos e externos da CAIXA.
- 7.3.1 A CAIXA arcará com o custo unitário de cada insumo solicitado, pelo mesmo valor unitário previsto no contrato, caso exceda a quantidade previstas no item 7.3.
- 7.4 O prazo para fornecimento desses plásticos é de até D+3.

8 PAINEL DE CONTROLE DE PRODUÇÃO POR MOVIMENTO – DIÁRIO, CONTENDO:

- 8.1 Data e quantidade por tipo de cartões para cada arquivo enviado pela CAIXA;

- 8.1.1 Data, tipo e quantidade de folheteria e encartes utilizados, para cada arquivo enviado pela CAIXA;
- 8.1.2 Status dos arquivos de personalização enviados pela CAIXA;
- 8.1.3 Estoque de plásticos de cada tipo de *card design*;
- 8.1.4 Estoque da folheteria, por tipo de peça, que compõem os pacotes de boas-vindas;
- 8.1.5 Identificação por imagem em arquivo PDF para cada item cadastrado (Plásticos e Folheteria);
- 8.1.6 Funcionalidade de *upload/download* das imagens dos *card design* e folheterias, permitindo a aprovação, recusa ou solicitação de ajuste;
- 8.1.7 Visualização dos níveis de estoque dos insumos (plásticos e folheteria) com mecanismos de comparação com o estoque crítico definido entre a CONTRATADA e a CAIXA, por meio de sinalização específica;
 - 8.1.7.1 Acompanhamento da produção em tempo real, permitindo a visualização dos processos, desde o envio do arquivo até a postagem.
 - 8.1.7.2 Módulo de ateste, contendo planilha Resumo e também de Faturamento, contemplando o mês de competência.
- 8.1.8 A CONTRATADA deverá apresentar relatórios de resumo e de faturamento mensais, semestrais e anuais.
- 8.1.9 Lista de Postagem dos objetos entregues para remessa junto aos Correios ou empresa de logística definida pela CAIXA.
 - 8.1.9.1 Notificações de Recebimento (NR), diário, com carga de até 5 dias úteis da data de postagem.
 - 8.1.9.2 A contratada deverá disponibilizar no portal de gestão web ferramenta de consulta do status de postagem e encaminhamentos até a entrega do objeto aos Correios ou empresa de logística definida pela CAIXA, mantendo registro do código de postagem com data e horário de entrega.
 - 8.1.9.2.1 O acesso dos usuários ao portal citado no subitem anterior ocorrerá por meio do recurso SSO – “Single Sign On”, utilizando protocolo “OAuth”, com validação de tokens no sistema SSO.
- 8.2 A critério da CAIXA, a CONTRATADA deverá disponibilizar e transmitir as informações existentes no módulo WEB em arquivo “.txt”, “.xlsx” ou outros formatos / leiaute definido pela CAIXA, podendo sofrer ajustes.

- 8.3 O acesso ao Módulo de Gestão WEB deve ser permitido, mediante cadastramento de usuários indicados pela CAIXA à CONTRATADA, com níveis de acesso restritos e diferenciados entre os usuários (Master, Consulta, dentre outros).
- 8.4 A CONTRATADA deverá viabilizar o módulo de gestão WEB para CAIXA disponibilizando os acessos e programas compatíveis e necessários, no prazo de até 150 dias corridos após a assinatura do Contrato.
- 8.5 Todos os sistemas e/ou soluções de software da CONTRATADA devem garantir a gravação de trilha de auditoria para reconstituição de eventos ocorridos a qualquer tempo durante a vigência do contrato, incluindo, mas não se limitando a: acessos individuais aos dados, ações executadas por indivíduos com ou sem privilégios administrativos, tentativas de acesso inválidas, uso de mecanismos de identificação e autenticação, inicialização dos logs, criação e eliminação de componentes de sistema, inserção ou troca de chaves criptográficas.

9 INFRAESTRUTURA NECESSÁRIA À CONTRATADA

- 9.1 O acesso padrão para conexão com a Rede CAIXA (conexão entre a CONTRATADA e a CAIXA) é mediante o uso de circuito privado dedicado nas tecnologias LAN-to-LAN ou MPLS.
- 9.1.1 A instalação do circuito dedicado deve ser direcionada para o Centro Tecnológico Datacenter – DTC e/ou Centro Tecnológico CAIXA – CTC, de acordo com a indicação da equipe de Rede de Telecomunicações.

Os endereços de instalação são:

PRQ TECNOLOGICO CAPITAL DIGITAL LOTE 03 – S/N
Bairro: Granja do Torto
Cidade: Brasília UF: DF
CEP: 70.636-000

Setor de Indústrias Gráficas – SIG Quadra 1 – Lote 685/705
Bairro: SIG
Cidade: Brasília UF: DF
CEP: 70.610-410

- 9.1.2 Nos casos em que o ambiente da CONTRATADA esteja hospedado em ambiente de nuvem ou nos Datacenters de interconexão Multicloud da CAIXA em São Paulo ou Rio de Janeiro, as conexões poderão ser feitas através do FABRIC/Golden Jumper desses Datacenters.

Os endereços de instalação são:

Equinix SP IBX SP3
Av. Marcos Penteado de Ulhoa Rodrigues, 249

Santana de Parnaíba – SP – CEP: 06543 001

Equinix RJ IBX RJ2
Estrada Adhemar Bebiano, 1380
Del Castilho - RJ - CEP: 21051 070

- 9.2 O circuito WAN de contingência deve ser instalado em localidade e operadora de telecomunicações diferente do circuito principal.
- 9.2.1 Caso a CONTRATADA disponha de duas ou mais localidades de processamento deve-se considerar a contratação de circuitos para todas essas localidades direcionados aos Datacenters da CAIXA.
- 9.2.2 A CAIXA poderá alterar seus endereços de conexão, inclusive de cidade e/ou de estado, de acordo com as suas necessidades, o que deverá ser atendido sem ônus para a CAIXA.
- 9.3 Características gerais da conexão:
- 9.3.1 O dimensionamento do link de comunicação é de responsabilidade da CONTRATADA.
- 9.3.2 A responsabilidade pelo fornecimento e pela negociação junto à operadora do roteador CPE na ponta da CONTRATADA é integralmente da CONTRATADA.
- 9.3.3 A operadora deverá fornecer, caso ainda não tenha, concentrador na ponta da CAIXA conforme padrões estabelecidos. Caso a operadora já disponha de infraestrutura e equipamentos nos SITE da CAIXA, ou pretenda utilizar o FABRIC dos ambientes de Multicloud, esta deverá fazer uso compartilhado destes equipamentos/conexões.
- 9.3.4 A operadora deve adotar arquitetura de compartilhamento de conexões físicas, ou seja, não será autorizado o uso de conexões físicas exclusivas. Este compartilhamento deve ser observado na conexão entre o equipamento da operadora e da CAIXA, garantindo ativação de diversas conexões lógicas na mesma interface física.
- 9.3.5 Nova conexão física independente poderá ser solicitada pela CAIXA, no caso da conexão atender a ambientes internos segregados, tais como ambiente de desenvolvimento ou homologação.
- 9.3.6 A conexão com os equipamentos da CAIXA deverá ser feita através de interface ethernet (mínimo gigabitethernet).
- 9.3.7 O endereçamento IP para trânsito WAN e de serviço (range para hosts) serão definidos pela CAIXA.
- 9.3.8 As conexões devem possibilitar a ativação de roteamento dinâmico baseado em BGP (Border Gateway Protocol).

- 9.3.9 Não é permitida a instalação de equipamentos da CONTRATADA no ambiente da CAIXA.
- 9.3.10 É admitida a instalação de equipamentos de operadora instalados para uso na modalidade compartilhada, exceto nos ambientes de Multicloud.
- 9.3.11 Caso a CONTRATADA já disponha de conexão com a CAIXA, para o mesmo ambiente deste contrato, a mesma poderá fazer uso desta desde que efetue o upgrade correspondente ao novo serviço e atenda aos padrões definidos nesta especificação.
- 9.4 Permite-se conexão para ambientes de DESENVOLVIMENTO / HOMOLOGAÇÃO por VPN IPSEC, via Internet, conforme abaixo:
- a) VPN site-to-site via Internet;
 - b) O acesso à Internet da empresa deverá possuir IP Fixo;
 - c) O dimensionamento deste acesso é responsabilidade da Empresa;
 - d) A CONTRATADA deverá dispor de roteador e concentrador VPN sob sua inteira responsabilidade;
 - e) A CAIXA fornecerá as definições de padrões para estabelecimento da VPN, porém não proverá suporte e manutenção na ponta da CONTRATADA;
 - f) Deverá utilizar no mínimo protocolo IPSEC 3DES-SHA1 IKE com 112bits.
- 9.5 Permite-se conexão para ambientes de DESENVOLVIMENTO / HOMOLOGAÇÃO por VPN IPSEC, via Internet, conforme abaixo:
- 9.5.1 O endereçamento IP WAN e o de serviço serão definidos entre CAIXA e CONTRATADA.
- 9.5.2 Não é permitida a instalação de equipamentos do cliente no ambiente da CAIXA.
- 9.5.3 Caso a CONTRATADA já disponha de conexão com a CAIXA para o mesmo ambiente deste contrato, a mesma poderá fazer uso desta, desde que efetue o upgrade correspondente ao novo serviço e atenda aos padrões definidos nesta especificação.
- 9.6 Permite-se o acesso excepcional para ambientes de DESENVOLVIMENTO e HOMOLOGAÇÃO e contingência de ambiente de PRODUÇÃO, por VPN IPSEC, via Internet, conforme abaixo:
- a) VPN site-to-site via Internet;
 - b) O acesso à Internet da CONTRATADA deverá possuir IP Fixo;
 - c) Dimensionamento deste acesso é responsabilidade da empresa CONTRATADA;

- d) A CONTRATADA deverá dispor de roteador e concentrador VPN sob sua inteira responsabilidade;
- e) A CAIXA fornecerá as definições de padrões para estabelecimento da VPN, porém não proverá suporte e manutenção na ponta da CONTRATADA;
- f) Deverá utilizar no mínimo protocolo IPSEC 3DES-SHA1 IKE com 112bits;
- g) O acesso por VPN IPSEC ao ambiente de PRODUÇÃO como contingência deve ser autorizado pela equipe de Rede de Telecomunicações da CAIXA.

- 9.7 A CAIXA suporta o seguinte software para envio e recebimento de arquivos: IBM Sterling Connect: Direct.
- 9.7.1 A transmissão de arquivos deverá ser realizada utilizando as proteções de segurança disponíveis no software selecionado, devendo ser configurada de acordo com os padrões de segurança vigentes na CAIXA.
- 9.8 Os custos decorrentes da contratação de softwares, acessos e equipamentos serão totalmente assumidos pela empresa CONTRATADA.
- 9.9 Para atender aos padrões de segurança da CAIXA, bem como garantir a qualidade dos serviços, objeto desse Contrato, a infraestrutura de segurança necessária no ambiente da CONTRATADA em termos de criptógrafos, também comumente denominados HSM (Hardware Security Module) deve ser providenciada exclusivamente pela CONTRATADA.
- 9.10 Os HSM devem ser compatíveis com o padrão FIPS 140-2, nível 3, e com suporte ao PKCS11.
- 9.11 As chaves da CAIXA, eventualmente instaladas nos HSM, devem ser usadas exclusivamente pela CAIXA e pela CONTRATADA, devendo ser garantida a confidencialidade daquelas e sua completa remoção do ambiente da CONTRATADA no término da vigência do Contrato ou, antes disso, por solicitação da CAIXA.
- 9.11.1 A CONTRATADA receberá os arquivos para produção criptografados no padrão especificado acima, e este arquivo somente poderá ser aberto com a chave de segurança a ser repassada pela CAIXA constante no HSM local.
- 9.11.2 Os detalhes de utilização dessa chave serão repassados após assinatura do Contrato.
- 9.12 As chaves da CAIXA serão inseridas no ambiente da CONTRATADA por meio de cerimônias específicas, a serem acordadas entre a CAIXA e a CONTRATADA.
- 9.13 A CONTRATADA deverá suportar a inserção de chaves no modo presencial, em sala segura no território brasileiro, por meio de componentes de chaves distintos e custodiantes distintos (*split knowledge*), bem como a inserção de chaves cifradas por chaves de transporte (KEK – *Key Encryption Key*) previamente compartilhadas entre a CAIXA e a CONTRATADA.

- 9.14 As chaves deverão ser mantidas no HSM da CONTRATADA no modo não exportável, condicionando as transações que as utilizam a ocorrerem dentro do HSM.
- 9.14.1 Além da criptografia para a proteção dos dados em trânsito, implementada nas camadas de rede e nos softwares XFB/*Connect Direct*, a CONTRATADA receberá os arquivos para produção criptografados no padrão especificado pela CAIXA.
- 9.14.1.1 O arquivo de produção criptografado somente poderá ser aberto, na camada da aplicação, com a chave de segurança a ser inserida pela CAIXA no HSM da CONTRATADA.
- 9.14.2 Os detalhes da criptografia dos arquivos de produção serão repassados após assinatura do Contrato.
- 9.15 A CONTRATADA deverá estar preparada para recepção de arquivos em formato AFP, Spool LCDS, e TXT.
- 9.16 A CONTRATADA deverá averiguar nos arquivos de produção e comunicar à CAIXA a identificação das seguintes informações, a fim de evitar fraudes e devoluções ao remetente:
- 9.16.1 **Nome do Cliente:**
- Nome do Cliente com apenas um caractere
Exemplo: M
Nome do Cliente com caracteres repetidos
Exemplo: Isabbbbbeellaaa
Nome do Cliente com numerais
Exemplo: Mari1
150 envelopes para o mesmo endereço
- 9.16.2 **Número da Conta:**
- Número da Conta com apenas um caractere
Exemplo: 5
Número da Conta com letras
Exemplo: axvbc-4
- 9.17 O prazo para adequação e atendimento às especificações relativas à infraestrutura necessária à CONTRATADA, inclusive homologação junto à Tecnologia da CAIXA, é de até 60 dias a partir da data de assinatura do Contrato, podendo ser prorrogado por igual período, mediante acordo entre as Partes.
- 9.18 A CONTRATADA deverá manter os certificados de transmissão de arquivos e outros que possam ser utilizados para a continuidade da prestação dos serviços sempre atualizados, sendo necessário comunicar à CAIXA com pelo

menos 30 dias de antecedência, encaminhando novo certificado para instalação, assim como, informando do andamento e prazos de renovação, que em hipótese alguma deve permitir período sem certificado válido.

10 VERSÕES DOS CHIP CAIXA:

10.1 A contratada deverá observar as versões e características dos CHIP utilizados pela CAIXA, conforme informações abaixo:

10.2 Chip ELO Débito Puro – S.D.A, C.D.A e D.D.A – Dual Interface

ISO 7816(T=0)

- O produto deverá conter a aplicação de pagamento conforme modelo de implementação adotado pelo Emissor.
- A aplicação de pagamento deve ser compatível com a especificação D-PAS Connect V2.0 ou superior
- O produto (chip) deve ter o Certificado (LoA -Letter of Approval) emitido pela bandeira Elo.
- O produto deve suportar o método de *Offline Data Authentication* na função C.D.A. (*Combined D.D.A./Application Cryptogram Generation*).
- O produto deve suportar o método de *Offline Data Authentication* na função S.D.A. (*Static Data Authentication*).
- Ter Memória com capacidade para gravação do PSE (Payment System Environment) e das aplicações de pagamento Débito Elo e Débito D-PAS, conforme Template de Personalização emitido pela Elo para este Emissor e Produto.
- O Bureau de Personalização deve constar na lista de fornecedores homologados (auditados) pela Elo.

ISO14443A

- Para produtos Dual-Interface a interface com contato pode processar as tecnologias NoO.D.A, D.D.A, C.D.A e S.D.A respectivamente, enquanto a interface sem contato (contactless) opera por NoO.D.A e C.D.A conforme contexto transacional.
- Desta forma, na aquisição de chip para Wearable ou Dual-Interface o produto elegível sempre terá habilidade C.D.A.
- O produto deverá suportar uma aplicação de pagamento contactless personalizada, compatíveis com a especificação D-PAS Connect v2.0 ou superior.
- O produto (chip) deve ter o Certificado (LoA -Letter of Approval) emitido pela bandeira Elo.
- O produto deve suportar o método de *Offline Data Authentication* na função C.D.A. (*Combined D.D.A./Application Cryptogram Generation*)
- Ter Memória com capacidade para gravação do PPSE (Proximity Payment System Environment) e da aplicação de pagamento Débito Elo e Débito D-PAS Connect conforme Template de Personalização emitido pela Elo para este Emissor e Produto.

- O Bureau de Personalização deve constar na lista de fornecedores homologados (auditados) pela Elo.

10.3 **Chip Visa Débito – *Dual Interface***

- Qualquer cartão com carta de aprovação (LoA) válido pode ser utilizado.

ISO 7816 (T=0 ou T=1) para interface de contato:

- EMV Contactless Interface Level 1 (Type A ou Type B);
- Aderência às especificações EMV 4.3, VIS 1.5.4 e VCPS 2.1.3 ou superior;
- Aplicação VSDC (Visa Smart Debit Credit) residente em memória ROM ou Flash;
- Aplicação qVSDC;
- Applet VSDC v2.8.1f1 ou v2.8.1g ou v2.8.1g1 para GlobalPlatform DDA;
- Tipo de autenticação f/DDA (*Dyanmic Data Authentication*).

11 **PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS**

- 11.1 O Plano de Contingência objetiva registrar procedimentos que permitam assegurar a continuidade das atividades de personalização e postagem previstas neste Termo, durante a ocorrência de um evento que impossibilite a utilização no todo ou em parte do conjunto de recursos físicos, humanos, materiais e tecnológicos dos seus centros de produção.
- 11.2 Os centros de produção alternativos deverão ser conectados por links de alta velocidade compatíveis com a necessidade de transferência de dados para os processos de produção e personalização.
- 11.3 A CONTRATADA deverá apresentar Plano de Continuidade dos Negócios (PCN) para os serviços contratados, em até 90 (noventa) dias úteis contados da assinatura do Contrato, para aprovação da CAIXA.
- 11.4 Com vistas a garantir a plena execução dos serviços, a CONTRATADA deverá apresentar o plano de contingência de acordo com as exigências deste Termo de Referência ou outro centro de produção, próprio, para produção do objeto da CAIXA, onde a operação deverá ser totalmente interconectada entre esses centros através de rede de dados de alta velocidade, garantindo a CAIXA a contingência imediata para execução dos processos sempre que necessário.
- 11.5 Também devem ser consideradas situações de contingência: desastres naturais, interrupção de serviços públicos, entre outras eventualidades alheias à atuação da CONTRATADA, que impactem na entrega do objeto do Termo de Referência.

12 **DAS FISCALIZAÇÕES E GARANTIAS**

- 12.1 A CAIXA poderá solicitar a qualquer tempo e sem aviso prévio, a retirada de amostras aleatórias, por lotes produzidos, para análise do produto e teste de qualidade.
- 12.1.1 Para esse fim, a CAIXA designará empregado (s) para verificar o quantitativo produzido e retirada das amostras para análise.
- 12.1.2 Constatada a inconformidade em relação às amostras, a CAIXA poderá reprovar todos os lotes correspondentes aos cartões analisados, solicitando formalmente a sua retirada de produção.
- 12.1.3 Sempre que necessário, a CAIXA solicitará novos testes e amostras adicionais de cartões, de forma a garantir a prestação do serviço nos padrões definidos neste Termo de Referência.
- 12.2 A CAIXA poderá, a qualquer tempo, realizar auditoria nas instalações da CONTRATADA de forma a verificar se os padrões de produção, segurança da informação e segurança física atendem aos requisitos definidos nas normas e padrões das Bandeiras e deste Termo de Referência.
- 12.3 A CONTRATADA prestará à CAIXA garantia de 5 (cinco) anos sobre qualquer defeito de fabricação que o material, objeto da CONTRATAÇÃO venha a apresentar.

13 DO GERENCIAMENTO E CONTROLE DOS SERVIÇOS E DISPONIBILIZAÇÃO DO MÓDULO DE GESTÃO WEB

- 13.1 A CONTRATADA deverá contar com técnicas de produção que possibilitem a gestão de um grande volume de objetos e processos, disponibilizando, por acesso pela internet, o acompanhamento pela CONTRATANTE de todas as etapas entre o recebimento do arquivo e a postagem dos objetos personalizados.
- 13.2 Deverá ser disponibilizado portal para acesso, mediante login e senha, pela CONTRATANTE com as funcionalidades elencadas abaixo:
- 13.3 Painel de Controle de Produção por movimento – diário, contendo:
- Data e quantidade por tipo de cartões para cada arquivo enviado pela CAIXA;
 - Data, tipo e quantidade de folheteria e encartes utilizados, para cada arquivo enviado pela CAIXA;
 - Status dos arquivos de personalização enviados pela CAIXA;
 - Estoque de plásticos de cada tipo de card design;
 - Estoque da folheteria, por tipo de peça, que compõem os pacotes de boas-vindas;
 - Identificação por imagem em arquivo PDF para cada item cadastrado (Plásticos e Folheteria);

- Funcionalidade de *upload/download* das imagens dos card design e folheterias, permitindo a aprovação, recusa ou solicitação de ajuste.
- 13.3.1 Visualização dos níveis de estoque dos insumos (plásticos e folheteria) com mecanismos de comparação com o estoque crítico definido entre a CONTRATADA e a CAIXA, por meio de sinalização específica.
- 13.4 A codificação dos itens de controle tais como plásticos, folheteria, kits de boas-vindas e outros que a CAIXA indicar, deve ser desenvolvida em conjunto com a CAIXA e compatível com os sistemas corporativos da mesma.
- 13.4.1 Para identificar o estágio da produção corrente, bem como compor histórico da produção, a CONTRATADA deve criar codificação de serviços executados para homologação pela CAIXA, os quais serão considerados para identificação do estágio de produção de cada item demandado.
- 13.4.2 O Módulo de ateste, deverá conter Planilha Resumo e também de Faturamento, contemplando o mês de competência.
- 13.4.2.1 O Controle deverá ser por Tipo de Objeto/Planilha Resumo (semanal).
- 13.4.2.1.1 A consolidação das informações da Planilha Resumo e de Faturamento deverá ser apresentada, também, por períodos (mensal, semestral e anual).
- 13.4.2.1.2 A CONTRATADA deverá apresentar a Planilha Resumo e a Planilha de Faturamento contemplando o período de faturamento do primeiro ao último dia do mês corrente (mensal).
- 13.4.3 A CONTRATADA deverá apresentar Lista de Postagem dos objetos entregues para remessa junto aos Correios ou empresa de logística definida pela CAIXA (diário).
- 13.4.4 As Notificações de Recebimento (NR), diário, deverão apresentar carga de até 5 (cinco) dias úteis da data de postagem.
- 13.4.4.1 A CONTRATADA deverá disponibilizar no portal de gestão WEB, ferramenta de consulta do status de postagem e encaminhamentos até a entrega do objeto postado por meio de interface ao sistema SRO dos Correios ou de empresa de logística definida pela CAIXA.
- 13.5 A critério da CAIXA, a CONTRATADA deverá disponibilizar e transmitir as informações existentes no módulo WEB em arquivo “txt”, “xlsx” ou outros formatos / leiaute definido pela CAIXA, podendo sofrer ajustes.
- 13.6 O acesso ao Módulo de Gestão WEB deve ser permitido, mediante cadastramento de usuários indicados pela CAIXA à CONTRATADA, com níveis de acesso restritos e diferenciados entre os usuários (Master, Consulta, dentre outros).

13.7 A CONTRATADA deverá viabilizar o módulo de gestão WEB para a CAIXA, disponibilizando os acessos e programas compatíveis e necessários, no prazo de até 90 (noventa) dias corridos após a assinatura do Contrato.

13.8 Todos os sistemas e/ou soluções de software da CONTRATADA devem garantir a gravação de trilha de auditoria para reconstituição de eventos ocorridos a qualquer tempo durante a vigência do contrato, incluindo, mas não se limitando a: acessos individuais aos dados, ações executadas por indivíduos com ou sem privilégios administrativos, tentativas de acesso inválidas, uso de mecanismos de identificação e autenticação, inicialização dos logs, criação e eliminação de componentes de sistema, inserção ou troca de chaves criptográficas.

14 QUANTITATIVOS ESTIMADOS

14.1 As quantidades de itens estimados podem sofrer variações devido à exclusão ou lançamento de novos produtos, campanhas promocionais, entre outras causas que possam ensejar a divergência dos valores estimados.

15 SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

15.1 A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (<https://www.caixa.gov.br/Downloads/caixa-governanca/politica-seguranca-informacao.pdf>), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto deste Termo.

15.2 A CONTRATADA deve proteger as informações corporativas da CAIXA e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.

15.3 A CONTRATADA deve garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações obtidas durante a prestação dos serviços ou em função deles e somente as utilizem no âmbito dos serviços contratados.

15.4 A CONTRATADA deve garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social.

15.5 A CONTRATADA deve garantir que as práticas de segurança da informação por ela executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento.

15.6 A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.

- 15.7 A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação.
- 15.8 A CONTRATADA fica ciente de que deve guardar o mais completo e absoluto SIGILO em relação às informações e dados que tiver conhecimento em razão do serviço a ser prestado, observadas as solicitações de órgãos de regulação, fiscalização, supervisão e de controle, bem como as determinações judiciais que deverão ser comunicadas imediatamente, pois ambas somente poderão ser atendidas mediante prévia autorização da área jurídica da CAIXA.
- 15.9 A CONTRATADA fica ciente que, por força da lei, é responsável civil e criminalmente pela divulgação indevida, descuidada ou incorreta utilização das informações corporativas da CAIXA e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.
- 15.10 A CONTRATADA deve comunicar imediatamente à CONTRATANTE qualquer descumprimento às cláusulas acima, principalmente para os casos em que ficar comprovado o comprometimento de informação corporativa da CAIXA ou sob sua responsabilidade.
- 15.11 A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações, inclusive dados pessoais/sensíveis da CAIXA, assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço (MO19607), anexo.
- 15.12 A CONTRATADA deve enviar, anualmente, à CAIXA a versão vigente do(s) Termo(s) de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, disponível no Portal Licitações CAIXA, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).
- 15.13 A CONTRATADA deve realizar ou contratar treinamento para seus dirigentes, empregados e colaboradores, visando à sensibilização e à conscientização em relação à segurança da informação e à privacidade de dados, abordando no mínimo o seguinte conteúdo:
- i. conhecimento da Política de segurança da informação da empresa CONTRATADA e da CAIXA, mencionada no subitem 15.1 deste Termo de Referência;
 - ii. uso seguro de informações corporativas a que tiver acesso;
 - iii. proteção de dados e privacidade – LGPD – direitos do titular dos dados;
 - iv. proteção de dados e privacidade – LGPD – responsabilidades do controlador, operador e do agente de tratamento dos dados;
 - v. uso seguro de dispositivos;
 - vi. uso seguro de *e-mails*;
 - vii. uso seguro de soluções em nuvem;
 - viii. uso seguro de redes sociais e comunicadores instantâneos;
 - ix. adoção da política de “mesa limpa”, “tela limpa” e “impressora limpa”;

- x. formas defensivas contra *phishing* e *smshing*;
- xi. formas defensivas contra códigos maliciosos recebidos em dispositivos;
- xii. formas defensivas contra engenharia social;
- xiii. formas de reporte de incidentes de segurança da informação na empresa e na CAIXA;
- xiv. vazamento de dados e proteção de senhas;
- xv. metodologia e princípios da *Privacy by Design* e *Secure by Design*.

- 15.14 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento da realização do treinamento referido no item 15.13 deste Termo de Referência.
- 15.14.1 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do período, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA.
- 15.15 A CONTRATADA deve se adequar às normas e à legislação vigente inerentes à Segurança da Informação relacionadas às atividades da CAIXA, enquanto empresa pública e instituição financeira.
- 15.16 A CAIXA poderá exercer o direito de exigir alterações nos controles de segurança da CONTRATADA à medida que os ambientes externos e internos se modifiquem.
- 15.17 A CONTRATADA deve solicitar formalmente autorização para subcontratação de serviços, cabendo a CONTRATANTE autorizar ou não.
- 15.17.1 Em caso de concretização de subcontratação de serviços, previamente autorizada pela CONTRATANTE, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.
- 15.18 A CONTRATADA deverá informar à CAIXA, periodicamente, os resultados dos indicadores:
- a) Quantidade de empregados e colaboradores que atuam na prestação de serviço objeto do contrato, **treinados** em SI, conforme disposto no subitem 15.13, acima, no último semestre dividido pela Quantidade total de empregados que atuam na prestação de serviço objeto do contrato, em percentual, medido semestralmente e informado à CAIXA, anualmente até o último dia útil do mês subsequente ao ano base;
 - b) Quantidade de empregados que assinaram o **Termo de Responsabilidade** Segurança da Informação, previsto no subitem 15.9 acima dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CAIXA até o último dia útil do mês subsequente ao ano base.

- 15.19 O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente Instrumento implicará multa de 0,3% (zero vírgula três por cento), por infração, calculado sobre o valor global do contrato.
- 15.19.1 Em caso de reincidência, na mesma violação ou não saneamento da violação no prazo de 60 (sessenta) dias haverá rescisão por descumprimento de contrato.
- 15.20 Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a atender o Plano de Continuidade de Negócios conforme Item 11 do presente Termo de Referência – DO PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS.
- 15.21 Quaisquer materiais ou documentos com informações confidenciais que tenham sido fornecidos à CONTRATADA pela CAIXA serão devolvidos, acompanhados de todas as cópias, em até 5 (cinco) dias contados a partir da formalização de solicitação de devolução das informações confidenciais, pela CAIXA.
- 15.22 A CONTRATADA é responsável por realizar o tratamento das informações da CAIXA e as sob sua responsabilidade, observando sua classificação de sigilo, bem como as demais regras internas da CAIXA estipuladas na versão vigente do Manual Normativo OR016 – Tratamento da Informação, disponível no Portal Licitações CAIXA.
- 15.23 A CONTRATADA, durante a execução dos serviços contratados, deve adotar a mesma classificação da informação adotada pela CONTRATANTE, observar e cumprir as regras internas da CONTRATANTE quanto ao tratamento de informações sensíveis e confidenciais da CAIXA, previstas no Manual Normativo OR016 – Tratamento da Informação.
- 15.24 A CONTRATADA é responsável pelas informações que obtiver, em razão de acesso aos recursos computacionais da CAIXA e se compromete a tomar conhecimento e cumprir as regras de uso aceitável e não aceitável da informação.
- 15.25 O treinamento de segurança da informação e proteção de dados referido no item 15.13 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 08 (oito) horas.
- 15.26 A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento do treinamento referido no item 15.25 e, caso estabelecido pela CAIXA.
- 15.27 A CONTRATADA deve emitir relatório, anualmente, até o último dia útil do mês subsequente ao término do ano base, relacionados aos seus riscos de

segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CAIXA.

- 15.27.1 O relatório referidos no item anterior deve proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.
- 15.28 A CONTRATADA garantirá que a CAIXA, ou a auditoria independente indicada pela CONTRATANTE, ou os órgãos de regulação/fiscalização das atividades de atuação da CAIXA tenham acesso físico e lógico ao seu ambiente e às informações relacionadas ao objeto do contrato, para realizar verificações relativas aos padrões de segurança da informação
- 15.29 A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.
- 15.30 A CONTRATADA notificará à CAIXA de qualquer incidente de segurança da informação identificados em seu ambiente ou operação e em toda sua cadeia produtiva, imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência à CAIXA. No caso de incidente de segurança com dados pessoais, essa notificação deve ser acompanhada de todos os dados necessários para eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao(s) titular(es) de dados pessoais.
- 15.30.1 A CONTRATADA deve enviar à CAIXA, em até 05 (cinco) dias úteis da detecção da ocorrência, relatório detalhado sobre o incidente de segurança da informação identificado, seus impactos, medidas corretivas implantadas e a implantar.
- 15.31 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores mencionados no item 15.18 e dos demais a seguir:
- a) Quantidade de empregados e colaboradores que atuam na prestação de serviço objeto do contrato que obtiveram nota mínima de aprovação no treinamento relacionado à Segurança da Informação mencionado no subitem 15.14 dividido pela Quantidade total de empregados e colaboradores que atuam na prestação de serviço objeto do contrato, em percentual, medido semestralmente e informado à CAIXA anualmente, até o último dia útil do mês subsequente ao ano base;
 - b) Quantidade de relatórios referidos no subitem 15.27 deste Termo de Referência e enviados à CAIXA dentro do prazo estipulado divididos pela Quantidade esperada de relatórios a serem emitidos, pela CONTRATADA, em percentual, medido semestralmente e informado à CAIXA, semestralmente. até o último dia útil do mês subsequente ao semestre base;
 - c) Quantidade de relatórios relacionados no subitem 15.27 deste Termo de Referência e enviados à CAIXA dentro do prazo estipulado / Quantidade

esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido semestralmente e informado à CAIXA semestralmente, até o último dia útil do mês subsequente ao semestre base.

- 15.32 A CONTRATADA deve garantir a continuidade do processamento das informações críticas de negócios no caso de contratação de bem ou de serviço de suporte às atividades críticas da CAIXA.
- 15.33 A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos
- 15.34 A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.
- 15.35 A CONTRATADA deve apresentar, sempre que requerido pela CONTRATANTE, relatórios emitidos por empresas de auditoria especializada independente que tenha realizado trabalho de auditoria em segurança da informação na CONTRATADA e certificações que atestem o nível de confiança nos princípios de segurança da informação.
- 15.36 A CONTRATADA se responsabiliza pelos incidentes de segurança detectados em sua infraestrutura ou na infraestrutura de empresa subcontratada.
- 15.37 A CONTRATADA deve tomar conhecimento dos termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD e de suas regulamentações, bem como das orientações da ANPD – Autoridade Nacional de Proteção de Dados, reconhecendo sua responsabilidade objetiva e de seus empregados/colaboradores em observar o disposto na LGPD no exercício de suas atividades no tratamento de dados pessoais de clientes, empregados e colaboradores da CAIXA.
- 15.37.1 A CONTRATADA se compromete a notificar a CAIXA, assim que detectada, a violação de dados relacionados à privacidade, de forma a permitir à CAIXA o cumprimento das determinações da LGPD – Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18 e da ANPD.
- 15.38 Para fins deste contrato, a CAIXA, doravante denominada de “CONTRATANTE”, assume o papel de Controladora de dados pessoais, e a empresa contratada doravante denominada “CONTRATADA”, assume o papel de operadora de dados pessoais.
- 15.39 Para a execução da finalidade prevista no presente contrato, a CONTRATANTE colocará à disposição da CONTRATADA:
- a) os dados pessoais envolvidos: Nome, Endereço, nº do cartão e nº da conta cartão;
 - b) a categoria dos dados: dados sensíveis dos clientes da CAIXA que pode ter, também, de adolescentes;

c) a natureza das operações realizadas: coleta, armazenamento, gravação, manuseio e eliminação.

- 15.40 A CONTRATADA se compromete a tratar os dados pessoais a que tiver acesso, única e exclusivamente para cumprir a finalidade a que se destina seu tratamento, responsabilizando-se por qualquer acesso indevido.
- 15.41 A CONTRATADA deve garantir a confidencialidade no tratamento de dados pessoais, protegendo-os contra acesso, modificação, destruição ou divulgação não autorizada.
- 15.42 A CONTRATADA está autorizada a tratar, em nome da CONTRATANTE, os dados pessoais a que tiver acesso em decorrência do instrumento contratual para a seguinte finalidade: fornecimento de cartões de débito, inclusive em Braille, personalização, manuseio, fornecimento de folheteria, envelopamento, inserção de folder, gravação de chip na tecnologia *Dual Interface (Chip e Contactless)*, com ou sem tarja magnética, expedição nos Correios ou outra empresa de logística definida pela CAIXA.
- 15.43 A CONTRATADA deverá, ao final do TERMO, eliminar ou devolver, a critério da CAIXA, todas as informações, inclusive os dados pessoais, acompanhados de todas as cópias.
- 15.44 A CONTRATADA deve manter, por escrito, o registro das operações de tratamento realizadas em nome da CONTRATANTE.
- 15.45 A CONTRATADA deve colaborar com a CONTRATANTE no cumprimento de sua obrigação de responder às solicitações de exercício dos direitos dos titulares.
- 15.46 A CONTRATADA deve comunicar imediatamente a CONTRATANTE o recebimento de requisição do titular de dados no exercício de seus direitos.
- 15.47 A CONTRATADA garantirá à CAIXA a disponibilização de todas as informações necessárias para que esta consiga demonstrar o cumprimento de suas obrigações nos termos da LGPD, mantendo a documentação disponível para a realização de auditorias e quaisquer inspeções.
- 15.48 A CONTRATADA deve obrigatoriamente adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- 15.49 A CONTRATADA notificará a CAIXA de qualquer violação de dados pessoais imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência ao gestor operacional do contrato. Essa notificação deve ser acompanhada de todos os dados necessários para

eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao(s) titular(es) de dados pessoais.

- 15.50 A CONTRATADA auxiliará a CAIXA com as informações necessárias para cumprimento de suas obrigações junto à Autoridade Nacional de Proteção de Dados (ANPD) e quaisquer órgãos reguladores, de fiscalização, de supervisão e de controle, inclusive na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).
- 15.51 A CONTRATADA deverá notificar imediatamente a CAIXA em caso de solicitações judiciais e de órgãos reguladores, de fiscalização, de supervisão e de controle para disponibilização de dados pessoais.
- 15.52 A CONTRATADA deverá solicitar autorização prévia da CONTRATANTE para subcontratação de outra empresa para quaisquer atividades que envolvam o tratamento de dados pessoais relativos ao presente contrato.
- 15.52.1 Em caso de concretização de subcontratação ou de sua rescisão, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.
- 15.52.2 A CONTRATADA é responsável por quaisquer descumprimentos deste contrato pela empresa SUBCONTRATADA, inclusive em relação a incidentes de segurança com dados pessoais.
- 15.52.3 A CONTRATADA somente poderá realizar transferência de dados pessoais para terceiros seguindo as instruções da CONTRATANTE ou mediante prévia autorização.
- 15.53 A CONTRATADA deverá observar os requisitos de privacidade desde a concepção em seus produtos, processos, serviços e soluções tecnológicas relacionadas ao tratamento de dados pessoais referentes ao instrumento contratual.
- 15.54 No encerramento/extinção do contrato a CONTRATADA se compromete a:
- a) entregar a versão mais atualizada de todos os artefatos, componentes e demais produtos produzidos durante a vigência do contrato;
 - b) executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CAIXA ou a quem ela indicar, observada a regulamentação vigente;
 - c) devolver ou transferir a quem for designado, pela CAIXA, todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.

16 SEGURANÇA CIBERNÉTICA

- 16.1 As cláusulas referentes a esse item encontram-se nos seguintes documentos anexos a este Termo de Referência, a saber: Anexo I A – Cláusulas de Requisitos de Segurança Tecnológica para Fornecedores e o Anexo I B – Cláusulas de Requisitos de Segurança Tecnológica para Solução em Nuvem.

17 PENALIDADES E OUTRAS CONSIDERAÇÕES FINAIS

- 17.1 A CONTRATADA deve responder por todo e qualquer dano que causar à CAIXA e a terceiros, ainda que culposos, praticados por seus prepostos, empregados ou mandatários, não excluindo ou reduzindo a sua responsabilidade à fiscalização ou ao acompanhamento exercido pela CAIXA.
- 17.1.1 Inclui-se também arcar com os custos e prejuízos com as postagens indevidas que eventualmente ocorram.
- 17.2 A CONTRATADA deve responder por eventuais prejuízos causados à CAIXA ou aos Parceiros Comerciais da CAIXA, por erro na inserção dos encartes, seja pela não inserção, troca, duplicidade ou outros, ficando responsável por eventuais ressarcimentos de gastos com produção e transporte dos encartes e danos que possam vir a ocorrer.
- 17.2.1 Inclui-se, também, arcar com os custos e prejuízos com as postagens indevidas, que eventualmente ocorram.
- 17.2.2 Por eventuais danos ou prejuízos provocados por ineficiência, negligência, erros ou irregularidades cometidas na execução dos serviços contratados, a CONTRATADA autoriza a CAIXA a descontar o valor correspondente aos referidos danos, diretamente nas faturas pertinentes aos pagamentos mensais que lhe forem devidos ou da garantia contratual, independentemente de qualquer procedimento judicial ou extrajudicial, após análise prévia e posicionamento das partes.
- 17.3 A CAIXA, a qualquer tempo, tem a prerrogativa de acompanhar *IN LOCO* os serviços executados pela CONTRATADA, inclusive realizar auditorias, respeitando as regras de segurança do ambiente de produção.
- 17.3.1 A CONTRATADA deverá elaborar, juntamente com a CAIXA, *Check-List* para realização de auditorias.
- 17.4 A CAIXA fiscalizará a execução dos serviços contratados e verificará o cumprimento das especificações técnicas, de segurança e prazos contratados, podendo rejeitá-los, em até 10 (dez) dias úteis, contados da data da fiscalização, por meio de comunicado escrito à CONTRATADA, quando, no todo ou em parte, não corresponderem ao contratado.
- 17.4.1 A fiscalização dos serviços pela CAIXA não desobriga a CONTRATADA de sua responsabilidade quanto à perfeita execução nos moldes descritos neste Termo de Referência e Contrato entre as Partes.

- 17.5 Quaisquer outras ações e omissões da CONTRATADA ou de seus empregados que causarem prejuízos financeiros, operacionais e à imagem da CAIXA deverão ser ressarcidos pela CONTRATADA, conforme a legislação em vigor.
- 17.6 Na vigência do contrato haverá troca diária de arquivos de dados, por via remota entre a CAIXA e a CONTRATADA, contendo as informações necessárias à gravação de tarja magnética, personalização do chip e inserção de dados variáveis a serem inseridos na folheteria dos pacotes de comunicação, inclusive dados do remente e do destinatário, observados os leiautes previamente definidos.
- 17.6.1 Havendo erro que impossibilite o processamento do arquivo de dados, a CONTRATADA deve comunicar a ocorrência à Centralizadora de Operações Tecnológicas, no prazo de até 4h (quatro horas), contados da hora do seu recebimento, com a indicação do erro encontrado e solicitação de nova transmissão.
- 17.7 Todas as despesas de contratação, licenciamento, atualização, suporte técnico e outros custos diretos e indiretos de tais produtos e (Links) são de responsabilidade da CONTRATADA.
- 17.8 A CONTRATADA deverá manter o completo e absoluto sigilo sobre quaisquer dados, informações, materiais, pormenores, documentos, especificações técnicas ou comerciais, inovações e aperfeiçoamentos de que venha a ter conhecimento ou acesso, ou que venha a ser confiada em razão da prestação dos serviços contratos, não podendo, sob qualquer pretexto, reproduzir, divulgar, ceder, dar conhecimento a terceiros, sem anuência expressa da CAIXA, sob as penas da Lei, mesmo após o término do Contrato.
- 17.9 A CONTRATADA deve assumir a responsabilidade por todos os seus atos e de seus empregados e/ou prepostos, declarando-se ciente de que deve guardar, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma tenha tomado conhecimento, o completo sigilo, em razão dos serviços prestados, ficando, portanto, por força da Lei, Civil ou Penal, responsável por sua indevida divulgação, descuidada ou incorreta utilização, sem prejuízo da responsabilidade por perdas e danos a que der causa.
- 17.10 A CONTRATADA deverá proceder à destruição total dos arquivos de dados enviados pela CAIXA para a personalização dos cartões e pacotes de Boas-Vindas, imediatamente após a postagem dos objetos.
- 17.11 O descarte de insumos deve ser provido sob responsabilidade socioambiental, com vistas à sustentabilidade, sendo exigida também a aquisição da matéria prima para a produção das folheterias e plásticos sob certificados ambientais vigentes ao longo do contrato, cujos documentos comprobatórios poderão ser solicitados a qualquer tempo pela CAIXA e remetidos pela CONTRATADA em até 05 (cinco) dias úteis.

- 17.12 Quando não for possível o cumprimento dos prazos, a CONTRATADA deverá comunicar à CAIXA, via E-mail, as justificativas e providências para solução do problema e a previsão de atendimento dos serviços.
- 17.12.1 A comunicação do subitem anterior não exime a CONTRATADA das penalidades previstas em Contrato.
- 17.13 Uma vez aprovados pela CAIXA os modelos de card design, porta cartão, folheteria, entre outros, permanecerão vigentes até que haja nova alteração pela CONTRATANTE.
- 17.14 A CONTRATADA deverá seguir as especificações disponibilizadas pelas Bandeiras para a correta personalização do chip e homologação dos cartões por ela produzidos, evitando risco de não funcionamento do produto, conforme descrito neste Termo de Referência.
- 17.14.1 A CONTRATADA manterá atualizada a sua habilitação durante todo o prazo do Contrato firmado com a CAIXA, junto às Bandeiras para a produção e a personalização dos cartões, assim como apresentará à CAIXA os documentos comprobatórios, a qualquer momento.
- 17.14.2 A CAIXA será a responsável pelos custos da primeira homologação, junto às Bandeiras, bem como homologações decorrentes de alterações no sistema de data *processing*.
- 17.14.3 A CONTRATADA arcará com os custos de homologação quando der causa às alterações que incorram na necessidade de nova certificação dos chips produzidos, ou necessite homologar novos lotes ou modelos de chip
- 17.14.3.1 A CONTRATADA deverá informar o custo supramencionado, com documentos comprobatórios, no prazo máximo de 30 (trinta) dias corridos a contar do fato gerador, que por sua vez será deduzido do pagamento da fatura pela CAIXA.
- 17.14.3.2 A CONTRATADA deverá informar à CAIXA, no prazo mínimo de 90 (noventa) dias o vencimento de *chips* das Bandeiras.
- 17.15 A CONTRATADA deverá interagir sempre que necessário diretamente com as Bandeiras e com a CAIXA, para o cumprimento das atividades do objeto previsto neste Termo de Referência.
- 17.16 Em caso de perda, extravio ou furto dos produtos objeto deste Termo de Referência, a CONTRATADA comunicará à CAIXA, em prazo não superior a 24 (vinte e quatro) horas, a contar do incidente, para as providências necessárias de cancelamento dos cartões.
- 17.17 Demais incidentes que afetem a produção, manuseio, remessa e entrega dos produtos objeto deste Termo de Referência, deverão ser comunicados à

CAIXA pela CONTRATADA, em prazo não superior a 48 (quarenta e oito) horas, da data do incidente.

- 17.18 A CAIXA deve ser ressarcida pela CONTRATADA, em valor atualizado pelo IGPM, na ocorrência de eventuais prejuízos com origem na confecção de cartões sem condições de uso, ou quando, comprovadamente, os cartões produzidos pela CONTRATADA tenham sido perdidos, extraviados ou furtados nas suas instalações, após análise prévia e posicionamento das partes.
- 17.18.1 A CAIXA considerará no cômputo do valor a ser ressarcido, o valor dos cartões produzidos e faturados, quanto às perdas decorrentes de sua utilização fraudulenta, nas próprias Notas Fiscais, Faturas ou meios acordados em Termo de Ressarcimento da Dívida, após análise prévia e posicionamento das partes.
- 17.19 A CONTRATADA ressarcirá à CAIXA de eventuais despesas com postagens, resultantes do reenvio de cartões, desde que o motivo para o reenvio tenha sido gerado exclusivamente pela CONTRATADA, ou, após autorização expressa da CAIXA, poderá realizar a postagem na mesma modalidade da realizada pela CAIXA, considerando o tipo de cartão que fora objeto do incidente, após análise prévia e posicionamento das partes.
- 17.19.1 Se os valores nas Notas Fiscais/Faturas forem insuficientes para a dedução, será feita a cobrança direta à CONTRATADA, após análise prévia e posicionamento das partes.
- 17.20 Os custos com as caixas para acondicionamento para a expedição, quando essas, eventualmente, não forem fornecidas pelos Correios ou empresa indicada pela CAIXA, e confecção de amostras para a realização de ATC (Avaliação Técnica Comercial) e ATO (Avaliação Técnica Operacional), bem como outras avaliações e/ou testes que os Correios venham a solicitar, serão integralmente da CONTRATADA, não podendo ser repassados à CAIXA.
- 17.21 A não observância dos procedimentos de postagem/expedição implicará no repasse dos custos adicionais à CONTRATADA, caso esses venham a ser imputados à CAIXA pelos Correios, ou empresa de logística definida pela CONTRATANTE, a qualquer tempo.
- 17.22 A CONTRATADA deverá acatar os pedidos de alterações tecnológicas da TI da CAIXA no prazo de 15 dias úteis.
- 17.22.1 Caso a CONTRATADA não possa cumprir o prazo estipulado no item 17.17 acima, esta deverá apresentar cronograma com novo prazo e justificativas para o não cumprimento do prazo original.

ANEXO I-A**DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA PARA FORNECEDORES****REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES****1 GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS**

1.1 A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

1.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

1.3 A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

1.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

1.5 Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.

1.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.

1.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.

1.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.

1.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.

1.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.

1.11 Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.

1.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

1.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.

1.14 A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

1.15 A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

1.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.

1.17 A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.

1.18 As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

1.19 A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

1.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

1.21 Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

1.22 A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

- O tipo de evento (inclusão, alteração, exclusão, consulta);
- O autor do evento;
- A data e hora do evento;
- IP e Porta do equipamento que originou o evento.

1.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

1.24 A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

1.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.

1.26 A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para fornecer este acesso de forma segura.

1.27 A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9.

1.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

2 SEGURANÇA DE ATIVOS

2.1 A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

2.2 A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

2.3 A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

2.4 A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

- 2.5 Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.
- 2.6 As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 2.7 Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 2.8 A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 2.9 A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 2.10 A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.
- 2.11 Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.
- 2.12 A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 2.13 A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 2.14 A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.
- 2.15 A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.
- 2.16 A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 2.17 A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 2.18 As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo,

"administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

2.19 A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

2.20 A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

2.21 Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

2.22 A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

- O tipo de evento (inclusão, alteração, exclusão, consulta);
- O autor do evento;
- A data e hora do evento;
- IP e Porta do equipamento que originou o evento.

2.23 A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

2.24 A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

2.25 A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.

2.26 A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.

2.27 A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9.

2.28 A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

3 SEGURANÇA DE REDES

3.1 Todo o tráfego de rede associado ao objeto do contrato deve ser mediado por uma solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações).

3.2 O conjunto de regras do firewall deve se basear na negação de todos os serviços, exceto aqueles especificamente permitidos.

3.3 O processo para instalação e adaptação de regras de firewalls deve ser feito com duplo controle.

3.4 A Contratada deve revisar as regras de firewall pelo menos semestralmente, guardando evidências dessas revisões e dos ajustes eventualmente realizados, comunicando à CAIXA sobre a realização desta revisão.

3.5 Todos os componentes de gateway de perímetro e sistemas de computadores devem ser monitorados contra tentativas de intrusão, por meio de solução de prevenção e detecção de intrusão (IPS).

3.6 O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de intrusão suspeitas ou reais.

3.7 A Contratada deve informar imediatamente à CAIXA em caso de tentativa de intrusão real, e informar à CAIXA em relatório mensal sobre as tentativas de intrusão suspeitas.

3.8 A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).

3.9 As soluções de firewall, IPS e-DDoS utilizadas pela Contratada serão validadas pela CAIXA a partir de documentações do fabricante ou certificações.

3.10 A Contratada deve impedir o uso do protocolo Bluetooth para a transferência de dados.

3.11 Todas as comunicações e trocas de informações entre a Contratada e a CAIXA devem ser realizadas por meio de conexão protegida, com TLS 1.3 ou superior.

3.12 Para os casos aplicáveis, os acessos diretos de diferentes equipamentos ao serviço da Contratada devem ser gerenciados por ferramentas de gerenciamento de dispositivos e/ou aplicativos (MDM/MAM) ou controle de acesso à rede (NAC).

4 CICLO DE VIDA DE DESENVOLVIMENTO SEGURO

4.1 A Contratada deve adotar o princípio de *security by design* para garantir que as aplicações de TI por ela desenvolvidas sejam seguras desde a concepção.

4.2 A Contratada deve fazer análise de código automatizada com base nas melhores práticas de mercado, utilizando como referência os padrões do OWASP.

4.3 A Contratada deve fazer análise de código estática (SAST) e dinâmica (DAST) periodicamente e de forma integrada ao ciclo de desenvolvimento como um todo para a solução Contratada. Essas análises precisam ser executadas pelo menos uma vez por ano ou quando houver uma mudança considerada significativa nas funcionalidades do sistema/aplicação (como a inclusão de uma nova funcionalidade crítica ou manutenção em módulos que tratam informações sensíveis e confidenciais). A bateria de testes deve incluir testes de resistência, injeções de falhas, teste de penetração e teste de vulnerabilidades onde aplicável.

4.4 A Contratada deve incluir a análise e a remediação das vulnerabilidades detectadas como parte do ciclo de vida de desenvolvimento de software padrão, sem custo adicional para a CAIXA, dentro de um período razoável e de acordo com a criticidade da falha encontrada.

4.5 A Contratada deve estabelecer critérios de escala e prazo para correção das vulnerabilidades e deve definir as alçadas para aceitação de riscos. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.

4.6 A Contratada deve submeter suas políticas de desenvolvimento seguro à aprovação da CAIXA.

4.7 Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados à CAIXA sempre que solicitado.

5 GESTÃO DE SERVIÇOS E MUDANÇAS

5.1 A Contratada deve ter um processo de Gestão de Mudanças para garantir a proteção contínua dos ativos de informação e dados, em particular aqueles que fazem parte do escopo do objeto do contrato.

5.2 A Contratada deve revisar periodicamente as atividades de gestão de mudanças, incluindo a acurácia da Base de Dados de Gerenciamento de Configuração (*Configuration Management Database – CMDB*).

5.3 A Contratada deve cumprir com os procedimentos de registros de informações relacionadas ao processo de gestão de mudanças, no contexto do contrato, incluindo:

- Referência da mudança

- Data de implementação
- Avaliação de impactos
- Resultados do teste
- Procedimentos de rollback
- Alterações de emergência
- Atualizações relacionadas ao inventário de ativos de informação
- Armazenamento Seguro de mídia de backup produzidos durante a atualização
- Atualização dos procedimentos de Documentação e de trabalho
- Atualizações aos documentos de Plano de Continuidade dos Negócios / Recuperação de Desastres se for o caso;
- Categorização, priorização e procedimentos de emergência
- Autorização de mudança
- Gerenciamento de liberação
- Link para incidentes / problemas (conforme apropriado).

5.4 A Contratada só deve promover os aplicativos e sistemas relacionados ao escopo do objeto do contrato para o ambiente de Produção após a realização com sucesso dos testes predefinidos baseados em caso de uso.

5.5 A Contratada deve conduzir uma avaliação de risco e ameaças, contemplando inclusive os testes baseados em casos de uso, quando da implantação de uma mudança.

5.6 A Contratada deve realizar uma avaliação de risco:

- Quando o escopo do sistema é expandido para incluir novos ativos de informação com novas funcionalidades;
- Quando uma nova comunidade de usuários é introduzida; ou
- Anualmente, por se tratar de risco cibernético, nos termos do art. 8º da Resolução BACEN 4.893/2021.

5.7 A Contratada deve disponibilizar os documentos de avaliação de risco à CAIXA sempre que solicitado.

6 GESTÃO DE INCIDENTES DE SEGURANÇA

6.1 A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.

6.2 A Contratada deve realizar testes independentes de penetração/invasão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus

adicional para a CAIXA. O escopo dos testes será previamente combinado e aprovado pela CAIXA, dentro dos limites do contrato.

6.3 Os testes de penetração/invasão terão como escopo, rede, aplicação web, *Application Programming Interface* (API), serviços hospedados e; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente, dentre outros.

6.4 Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções necessárias, serão fornecidos à CAIXA sempre que solicitado.

6.5 A Contratada deverá possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.

6.6 A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.

6.7 O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.

6.8 A Contratada deverá ter um processo de notificação de incidentes 24x7.

6.9 A Contratada deverá comunicar à CAIXA incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.

6.10 Os incidentes serão comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA, que opera 24x7, por meio do endereço de e-mail: abuse@caixa.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.

6.11 A Contratada deverá comunicar à CAIXA, dentro do prazo acordado, todos os incidentes detectados que envolvam os serviços prestados, conforme a classificação abaixo:

Nível de severidade	Descrição do nível de severidade	Prazo Máximo
Severidade 1 (Crítica)	Eventos cujo contexto principal é a segurança cibernética, tais como: - Impacto em ativos ou serviços críticos de TI; - Violação significativa de dados sensíveis; - Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente. Exemplos não exaustivos: ataque de <i>Ransomware</i> , ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.	2 horas após o início da ocorrência.
Severidade 2 (Alta)	Eventos cujo contexto principal é a segurança cibernética, tais como: - impacto em ativos ou serviços de TI de alta criticidade; - Detecção de acesso não autorizado e/ou alterações em sistemas de informação; - Infecção persistente por código malicioso; - Intrusão persistente na rede; - Incidentes de segurança cibernética envolvendo dirigentes; - Ameaça significativa à disponibilidade e/ou integridade do ambiente; - Ameaça significativa à imagem da CAIXA. Exemplos não exaustivos: ataques de escalção de privilégio em servidores, ataques do tipo <i>brute force</i> e <i>password spray</i> . Dentre outros.	4 horas após o início da ocorrência.

6.12 Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA.

6.13 A Contratada deverá fornecer descrição detalhada dos incidentes, incluindo informações suficientes para classificá-los por nível de severidade, conforme a definição dos eventos. As informações sobre incidentes podem ser enriquecidas utilizando o modelo do MITRE ATT&CK®.

6.14 A contratada deverá seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, Anexo IIA, que também contempla situações de incidentes de segurança com dados pessoais.

6.15 Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, a CAIXA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.

6.16 A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.

6.17 A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.

6.18 A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.

6.19 Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência da CAIXA por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA.

7 CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

7.1 A Contratada deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

7.2 O referido plano de continuidade deverá ser informado para a CAIXA como parte das ações de acompanhamento do contrato, e deverá ser atualizado e testado anualmente, ou em qualquer mudança significativa do ambiente.

7.3 A atuação, em caráter de contingência, causada por uma eventual indisponibilidade do serviço prestado, considera as seguintes premissas:

a) Interrupção total ou parcial dos serviços

- b) Ter infraestrutura alternativa: física e lógica em local distante do ambiente central de produção, com o objetivo de minimizar o risco de perda de ambas as instâncias;
- c) Manter os serviços essenciais suportados pelo contrato
- d) Manter a lista de integrantes das equipes e o Plano de Recuperação de Desastres atualizados;
- e) Ter local seguro para guarda de backups fora do local atingido;
- f) Assegurar a disponibilidade dos serviços essenciais dentro do tempo previsto para recuperação do serviço, de acordo com o contrato;
- g) Procedimento documentado e evidenciado de testes das mídias armazenadas *offsite*;
- h) Cópias de todos os procedimentos abordando backup, restauração e reconstituição de armazenamento de dados.

7.4 O plano de continuidade deve possuir os seguintes elementos em sua composição:

- a) Identificação do serviço suportado pelo contrato;
- b) A forma de conectividade usada e os direitos de acesso;
- c) A arquitetura do ambiente de produção;
- d) As interfaces de aplicações e suas dependências;
- e) O SLA contratado e os limites suportados para interrupção;
- f) A forma de replicação dos dados com o site alternativo;
- g) Procedimentos adotados para recuperação de desastres;
- h) Lista de contatos das equipes responsáveis pelo restabelecimento do serviço, divididos por tipos de atividades executadas;

7.5 A obrigatoriedade do plano de continuidade se estende para empresas que sejam subcontratadas pela Contratada.

7.6 A Contratada deve considerar, como parte do plano de continuidade, os diferentes ambientes de risco e o grau de mitigação de riscos necessários para proteger a Instituição, caso seja necessário colocar o plano em prática.

7.7 A avaliação de riscos e dos processos críticos devem levar em consideração instrumentos específicos, como um BIA – Business Impact Analysis.

7.8 A Contratada, visando a continuidade dos negócios, deve implantar uma política de backup, conforme exposto no item 10.

8 AUDITORIA CONTÍNUA

8.1 A Contratada deve apresentar à CAIXA, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

8.2 A Contratada deve informar imediatamente à CAIXA sobre qualquer auditoria regulatória, sua finalidade e como ela se relaciona com os serviços prestados à CAIXA.

8.3 A Contratada deve informar à CAIXA caso sejam contatados por um órgão regulador e se o propósito desse contato pode estar relacionado com/ou afetar os serviços prestados à CAIXA.

8.4 A Contratada deve fornecer os subsídios necessários para que a CAIXA implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.

8.5 A Contratada deverá disponibilizar, caso a CAIXA solicite, acesso às instalações da Contratada para realização de processo de *Due Dilligence* Presencial, para verificar o cumprimento dos requisitos de segurança.

8.6 Caso a Contratada não tenha certificação SOC Nível 2, ela deverá fazer auditoria externa independente, pelo menos uma vez por ano, em relação ao cumprimento dos requisitos de segurança estabelecidos neste documento, e apresentar os relatórios à CAIXA sempre que solicitado.

9 CONTROLES CRIPTOGRÁFICOS

9.1 A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.

9.2 A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.

9.3 A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.

9.4 A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.

9.5 Caso a Contratada hospede uma página com uma URL e um certificado gerados pela CAIXA, a Contratada deverá armazenar este certificado em dispositivo seguro com bloqueio para exportação da chave.

9.6 As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.

9.7 A Contratada deve permitir a criptografia de volume (por exemplo: a criptografia de um disco inteiro) e a criptografia de estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).

9.8 A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.

9.9 A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.

9.10 A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.

9.11 A Contratada deve permitir a auditoria da segurança de chaves criptográficas.

9.12 A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3 e superior.

10 POLÍTICA DE BACKUP

10.1 A Contratada deve possuir e implementar política de backup das informações e dos registros de log associados ao objeto do contrato, em conformidade com os dispositivos legais aplicáveis.

10.2 A política de backup deve assegurar a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica e os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha, ou por solicitação da CAIXA.

10.3 A Contratada deve prover pelo menos um site de armazenamento alternativo – e geograficamente distinto - como parte de sua política de backup, permitindo o armazenamento e a recuperação da informação sempre que necessário e de acordo com os requisitos definidos no item 7.

10.4 A Contratada deve garantir que o site de armazenamento alternativo conta com os mesmos controles de segurança do site de armazenamento primário.

11 RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS REQUERIMENTOS MÍNIMOS DE SEGURANÇA

11.1 Sempre que a CAIXA julgar necessário, poderá realizar *Due Diligence* presencial ou remota para verificar os requisitos de segurança presente nas cláusulas, são atendidos pela Contratada. O *Due Diligence* presencial é facultativo e será feito a critério da CAIXA.

11.2 Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, que comprovam o cumprimento dos requerimentos de segurança cibernética conforme estabelecido nas cláusulas e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança presente nas cláusulas	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada pela CAIXA	SOB DEMANDA
Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrito nas cláusulas	Documentos previstos nas cláusulas e demais comprovantes de seus requisitos. Quando não comprovados por certificação, os itens exigidos nas cláusulas devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens das cláusulas, desde que ratificados por empresa de auditoria independente. Relatório de empresa de auditoria independente, a ser apresentado pela Contratada	SOB DEMANDA
Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade,	SOC TYPE 2. Fornece relatórios com descrição do ambiente de controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de	Disponibilizar relatório de auditoria em nome da empresa	ANUAL

	confidencialidade e privacidade	segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA		
--	---------------------------------	---	--	--

12 ENCERRAMENTO DO CONTRATO

12.1 A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.

12.2 A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.

12.3 Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

12.4 A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 *Guidelines for Media Sanitization*, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

12.5 Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (*Certificate of Electronic Equipment Destruction* – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

13 NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS

13.1 O não cumprimento, pela Contratada, de qualquer um dos seguintes requisitos de segurança, definidos neste instrumento contratual, ensejará a aplicação das penalidades previstas neste contrato e poderá, a critério da Contratante, ensejar a rescisão imediata do contrato, sem prejuízo de outras medidas cabíveis:

- a) Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
- b) Não comunicar a revisão das regras de firewall;
- c) Não comunicar ocorrências de intrusão real;
- d) Não fornecer relatório mensal sobre as tentativas de intrusão;
- e) Não fornecer o planejamento de correção de vulnerabilidades;
- f) Não fornecer os relatórios dos testes SAST e DAST realizados e o planejamento das correções a serem feitas;

- g) Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
- h) Não fornecer os relatórios de incidentes conforme SLA;
- i) Não prestar as informações e relatórios solicitados pela CAIXA;
- j) Não fornecer os relatórios de auditoria externa independente;
- k) Não fornecer relatório indicando conformidade com o NIST SP 800-88;
- l) Não atender a convocação da CAIXA para *Due Diligence* presencial ou remoto;
- m) Não fornecer a documentação solicitada em decorrência do *Due Diligence* presencial ou remoto, conforme prazo acordado entre as partes;

ANEXO I-B**REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA SOLUÇÃO EM NUVEM****1. GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS**

1.1. A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.

1.2. A Contratada deve manter rígido controle de acesso de seus colaboradores baseado nas informações de contratação, dispensa e controle de ausências (férias, licenças, atestados, admissão, demissão etc.) impedindo o acesso ao ambiente computacional, local ou remoto, quando o colaborador não estiver em pleno exercício de suas atividades.

1.3. A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.

1.4. A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.

1.5. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

1.6. Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.

1.7. As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.

1.8. Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no logon.

1.9. A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.

1.10. A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.

1.11. A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.

1.12. Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.

1.13. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.

1.14. A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.

1.15. A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

1.16. A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.

1.17. A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.

1.18. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.

1.19. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

1.20. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.

1.21. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.

1.22. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.

1.23. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:

O tipo de evento (inclusão, alteração, exclusão, consulta);

O autor do evento;

A data e hora do evento;

O endereço lógico do equipamento de origem do tipo do evento.

1.24. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.

1.25. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.

1.26. Devem ser observadas as boas práticas de segregação e diferenciação entre ambientes de não produção e produtivo, estabelecendo-se acessos pertinentes para cada etapa do ciclo de desenvolvimento/manutenção e alinhado com o princípio do privilégio mínimo.

1.27. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.

1.28. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.

1.29. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 2.

1.30. A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

2. CONTROLES CRIPTOGRÁFICOS

2.1. Os requisitos apresentados devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá comprovar por

relatório de auditoria (Due Dilligence Remoto) que o armazenamento/processamento dos dados ocorre somente em ambiente de nuvem.

2.2. A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.

2.3. A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.

2.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.

2.5. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.

2.6. A Contratada deve fazer a geração e a renovação de certificados digitais expostos na Internet junto a autoridades certificadoras reconhecidas internacionalmente, cujas raízes de cadeias utilizadas na emissão dos certificados digitais façam parte do repositório de cadeias confiáveis dos principais navegadores e versões de sistemas operacionais, como: iOS 7 e superiores; Android 4 e superiores; Microsoft Edge 12 e superiores; Mozilla Firefox 45 e superiores; Google Chrome 49 e superiores; Apple Safari 8 e superiores; Linux Ubuntu 14 e superiores; Linux Mint 15 e superiores; MAC OS X 10.10 e superiores; e Windows 7 e superiores.

2.7. A Autoridade Certificadora deve possuir o selo Web Trust dentro do prazo de validade e a certificação Web Trust deve estar de acordo com, no mínimo, os Princípios e Critérios para Autoridades Certificadoras – versão 2.2.1, disponível em <https://www.cpacanada.ca/-/media/site/operational/ms-memberservices/docs/webtrust/WT100aWebTrust-for-CA-221-110120-finalaoda.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6FD> para todas as raízes de cadeias utilizadas na emissão dos certificados digitais.

2.8. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).

2.9. As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.

2.10. Caso haja a necessidade do compartilhamento de chaves simétricas entre a CAIXA e a Contratada, essas chaves devem ser geradas pela CAIXA e levadas para o ambiente da Contratada, onde devem ser armazenadas por meio de soluções FIPS 140-2 nível 3, sem possibilidade de exportação das chaves. Nesse caso, a Contratada deve prover meios que permitam a inserção das chaves da CAIXA no seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

2.11. No caso de utilização de um Provedor de Serviços em Nuvem, as certificações FIPS exigidas estão descritas no item 10.

2.12. A Contratada deve permitir a criptografia de dados em repouso, considerando volumes (por exemplo: a criptografia de um disco inteiro) e estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).

2.13. A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.

2.14. A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.

2.15. A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.

2.16. A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.

2.17. A Contratada deve permitir a auditoria da segurança de chaves criptográficas.

2.18. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3.

2.19. A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.3 e as cifras a seguir:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

2.20. Os parâmetros TLS Renegotiation e TLS Resumption devem estar desabilitados.

2.21. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão TLS, por exemplo – a Contratada deve fazer todas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.

2.22. O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.

3. CONTROLE DE ACESSO AO AMBIENTE DE NUVEM

3.1. Quando viável tecnicamente, o acesso de empregados CAIXA à nuvem deverá ser integrado com ferramenta de SSO da CAIXA, ou com o AD, para garantir o uso das credenciais internas, isso deve garantir que o usuário não acesse o ambiente do parceiro, caso seja desligado ou esteja ausente da CAIXA por qualquer motivo por período determinado.

3.2. Como apresentado no item 2.4, quando a autenticação for provida pela Contratada ou pelo Provedor de Serviços em Nuvem, deverá ser realizada autenticação por múltiplos fatores para o acesso dos empregados da CAIXA, que precisem acessar os recursos em nuvem.

3.3. O acesso aos recursos da CAIXA deverá ser realizado em tenant designado especificamente, sem que estes recursos sejam compartilhados com qualquer outra entidade, bem como a camada de dados da aplicação não pode ser compartilhada com outros clientes do Provedor de Serviços em Nuvem.

3.4. O Provedor de Serviços em Nuvem deve permitir que somente os usuários autorizados pela CAIXA tenham acesso aos recursos em conformidade aos respectivos perfis de uso.

3.5. Os acessos administrativos aos recursos do Provedor de Serviços em Nuvem, nos tenants que atendam à CAIXA, deverão ser feitos através de rede privada, tanto para empregados CAIXA quanto para representantes do Provedor.

4. REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

4.1. A Contratada deve garantir que a prestação dos serviços não causará prejuízo ao funcionamento regular da CAIXA nem embaraço à atuação da Banco Central do Brasil, assegurando que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços serão prestados não restringem nem impedem o acesso da CAIXA nem do Banco Central do Brasil aos dados e às informações.

4.2. A Contratada deve assegurar que os dados sujeitos a limites geográficos não serão migrados para além das fronteiras definidas em contrato, incluindo dados de backup,

dados em produção, dados em repouso, contingência ou recuperação de desastre sem prévio conhecimento da CAIXA por meio comunicação formal.

4.3. Deve ainda garantir acesso à CAIXA, a qualquer tempo, aos dados e às informações processadas, armazenadas e geradas pela atividade de processamento, Log, sob responsabilidade da Contratada;

4.4. Esta mesma Contratada deve assegurar que os dados da CAIXA processados e armazenados na Contratada são de propriedade exclusiva da CAIXA.

4.5. A Contratada deve assegurar também que o acesso aos dados processados e armazenados na Contratada é de acesso exclusivo da CAIXA, não sendo autorizado acesso da Contratada ou terceiros sem autorização formal da CAIXA.

4.6. A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.

4.7. Também deve assegurar à CAIXA acesso aos relatórios e documentos elaborados por empresa de auditoria especializada independente, contratada pelo provedor de serviço em nuvem, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados a qualquer tempo.

4.8. A Contratada deve assegurar à CAIXA, acesso a toda documentação comprobatória, em nome do provedor, que esclareça a Região/Zona de Disponibilidade escolhidos pela CAIXA para hospedagem de seus recursos.

4.9. A Contratada deve assegurar a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.10. A Contratada deve garantir, em caso de decretação de regime de resolução da CAIXA pelo Banco Central do Brasil, acesso pleno e irrestrito aos contratos e acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.11. A Contratada deve garantir notificação prévia ao responsável pelo regime de resolução sobre a intenção da empresa Contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observado que:

4.11.1. A Contratada assegura o atendimento de eventual pedido de prazo adicional de (30) trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução.

4.11.2. Caso haja subcontratação do serviço em nuvem, desde que explicitamente autorizado pela CAIXA, é obrigatório a Contratada apresentar a garantia formal do atendimento das cláusulas deste item 4 por parte da Provedor de Serviços em Nuvem, seja por meio de declaração própria durante o processo de contratação, seja por meio de aditivo contratual, caso não previsto inicialmente no contrato original.

5. PROTEÇÃO DOS DADOS PROCESSADOS E ARMAZENADOS EM NUVEM

5.1. Além dos requisitos descritos no item 2, a Contratada também deve permitir trabalhar com chaves simétricas e assimétricas geradas e armazenadas pela CAIXA. Para tanto, ela deve prover meios que permitam o envio das chaves da CAIXA para o seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

5.2. Caberá à CAIXA decidir quem fará a geração e a gestão de cada chave: se a própria CAIXA ou a Contratada.

5.3. Caso a CAIXA decida fazer a geração de chaves assimétricas, ela definirá a Autoridade Certificadora que será utilizada na emissão dos certificados digitais e fornecerá a cadeia certificadora para a Contratada sempre que necessário. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).

5.4. O modelo Third Party Certificates pode ser oferecido para o caso de certificados digitais utilizados no estabelecimento de conexões TLS. Nesse caso específico, as chaves devem ficar armazenadas exclusivamente em repositórios de chaves da Contratada e esta deve emitir o CSR (Certificate Signing Request) e enviá-lo para a CAIXA, que providenciará a emissão dos certificados digitais correspondentes. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).

5.5. Quando a Contratada for diferente do Provedor de Serviços em Nuvem e estiver agindo em nome deste, as chaves devem ser compartilhadas diretamente entre o Provedor e a CAIXA e a Contratada não deverá ter qualquer acesso às chaves envolvidas.

5.6. Quando se tratar de contratação no modelo IaaS, exige-se a certificação FIPS 140-2 nível 3.

5.7. Quando se tratar de contratação no modelo PaaS ou SaaS, exige-se a certificação FIPS 140-2 nível 2.

5.8. O Provedor de Serviços em Nuvem deve permitir que os usuários criptografem seus dados e objetos antes de enviá-los para o serviço de armazenamento.

5.9. A Contratada, assim como o Provedor de Serviços em Nuvem, deve tratar com rigor as informações sigilosas, não podendo ser usadas ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal da CAIXA.

5.10. A Contratada deverá assinar Termo de Responsabilidade de Segurança e Informação da CAIXA, resguardando que os recursos, dados e informações de propriedade da CAIXA, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

5.11. Os dados, metadados, informações e conhecimento tratados pela Contratada, não poderão ser fornecidos a terceiros e/ou usados por esta para fins diversos do previsto, sob nenhuma hipótese, sem autorização formal da CAIXA.

5.12. A CAIXA e a Contratada obrigam-se por seus empregados, sócios, diretores e mandatários, manter total sigilo e confidencialidade no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ela relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

6. MONITORAÇÃO DOS DADOS PROCESSADOS E ARMAZENADOS EM NUVEM

6.1. A Contratada deverá fornecer, sempre que solicitado pela CAIXA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de APIs para análise de segurança e auditorias.

6.2. A trilha de auditoria deve conter, minimamente, itens descritos no item 1.23 deste documento.

6.3. O Provedor de Serviço em Nuvem, deve dispor de recurso que permita o gerenciamento centralizado de eventos e envio para a CAIXA, sempre que solicitado, de logs/informações de trilha.

6.4. Os registros do Provedor de Serviço em Nuvem deverão incluir ainda todos os acessos, incidentes e eventos cibernéticos, no ambiente do mesmo, pelo período 5 (cinco) anos.

7. SEGURANÇA DO TRÁFEGO DE DADOS COM A NUVEM

7.1. A comunicação entre a CAIXA e a Contratada deve suportar criptografia TLS, com autenticação mútua, na versão 1.3.

7.2. Caso a aplicação não suporte TLS 1.3, será admitida a compatibilidade para TLS 1.2.

7.3. A necessidade de TLS também se aplica a qualquer comunicação entre a Contratada e o Provedor de Serviços em Nuvem ou entre a CAIXA e o Provedor de Serviços em Nuvem, para todos os casos em que a Contratada e o Provedor forem entidades distintas.

7.4. O Provedor de Serviços em Nuvem deverá prover segurança relacionada ao tráfego de dados, provendo aplicações de firewall, IPS e CASB para garantir a segurança de todos os fluxos, sejam externos ou em trânsito com a CAIXA.

7.5. O Provedor de Serviços em Nuvem não deverá ter permissão de uso ou acesso direto ao ambiente de autenticação da CAIXA.

7.6. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o provedor de serviço de nuvem, devem estar, preferencialmente, hospedados em território brasileiro.

7.7. Na hipótese de armazenamento em infraestrutura localizada no exterior, a Contratada deverá, sempre que solicitada:

7.7.1. Disponibilizar cópia completa dos dados, de forma contínua e atualizada com periodicidade mínima de 24 (vinte e quatro) horas entre cada atualização e/ou;

7.7.2. Manter cópia atualizada de segurança obrigatoriamente em território brasileiro.

8. ALTA DISPONIBILIDADE DOS SERVIÇOS EM NUVEM

8.1. Para assegurar a continuidade dos serviços e a resiliência das operações críticas da CAIXA, as soluções em nuvem fornecidas pela Contratada deverão ser projetadas com foco em alta disponibilidade.

8.2. Para tanto, é obrigatória a adoção de arquiteturas que contemplem a distribuição geográfica das cargas de trabalho (*workloads*) em múltiplas zonas de disponibilidade, de forma a mitigar riscos de indisponibilidade, de integridade e de continuidade, garantindo a operação ininterrupta dos serviços essenciais.

8.3. Além disso, a Contratada deve assegurar que:

8.3.1. Os dados e serviços estejam replicados de forma síncrona ou assíncrona entre as zonas, conforme a criticidade da aplicação;

8.3.2. Os mecanismos de balanceamento de carga e *failover* estejam devidamente configurados e testados periodicamente;

8.3.3. Toda a infraestrutura esteja em conformidade com os requisitos regulatórios e legais aplicáveis no Brasil;

8.3.4. Haja documentação clara sobre os procedimentos de recuperação e continuidade em caso de falhas regionais.

9. OUTROS CONTROLES DE SEGURANÇA NO AMBIENTE DA CONTRATADA DO SERVIÇO DE NUVEM

9.1. O Provedor de Serviços em Nuvem deve habilitar o registro completo do Hypervisor que suporta os serviços da CAIXA, e deve suportar o uso de máquinas virtuais (Trusted VM) fornecidas pela CAIXA, desde que estas máquinas estejam em conformidade com as políticas e práticas de segurança de rede exigidas pelo Provedor.

10. GESTÃO DE INCIDENTES DE SEGURANÇA

10.1. A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.

10.2. A Contratada deve realizar testes independentes de penetração/invasão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA. O escopo dos testes deve ser previamente combinado e aprovado pela CAIXA, dentro dos limites do contrato.

10.3. Os testes de penetração/invasão devem ter como escopo, rede, aplicação web, Application Programming Interface (API), serviços hospedados e; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; dentre outros.

10.4. Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções a serem feitas, devem ser fornecidos à CAIXA sempre que solicitado.

10.5. A Contratada deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.

10.6. A Contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.

10.7. O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.

10.8. A Contratada deve ter um processo de notificação de incidentes 24x7.

10.9. A Contratada deve comunicar à CAIXA incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.

10.10. Os incidentes devem ser comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA, que opera 24x7, por meio do endereço de e-mail: abuse@caixa.gov.br. Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.

10.11. A Contratada deve comunicar à CAIXA, dentro do prazo acordado, todos os incidentes detectados que envolvam os serviços prestados, conforme a classificação abaixo:

Severidade 1 (Crítica)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços críticos de TI; -Violação significativa de dados sensíveis; -Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente. Exemplos não exaustivos: ataque de Ransomware, ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.	2 horas após o início da ocorrência.
-----------------------------------	--	--------------------------------------

Severidade 2 (Alta)	Eventos cujo contexto principal é a segurança cibernética, tais como: -Impacto em ativos ou serviços de TI de alta criticidade; -Detecção de acesso não autorizado e/ou alterações em sistemas de informação; -Infecção persistente por código malicioso;- Intrusão persistente na rede; -Incidentes de segurança cibernética envolvendo dirigentes; -Ameaça significativa à disponibilidade e/ou integridade do ambiente; -Ameaça significativa à imagem da CAIXA. Exemplos não exaustivos: ataques de escalação de privilégio em servidores, ataques do tipo brute force e password spray. Dentre outros	4 horas após o início da ocorrência.
----------------------------	---	--------------------------------------

10.12. Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA.

10.13. A Contratada deve fornecer descrição detalhada dos incidentes, incluindo informações suficientes para classificá-los por nível de severidade, conforme a definição dos eventos. As informações sobre incidentes podem ser enriquecidas utilizando o modelo do MITRE ATT&CK®.

10.14. A Contratada deve seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, Anexo III A, que também contempla situações de incidentes de segurança com dados pessoais.

10.15. Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, a CAIXA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente

de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.

10.16. A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.

10.17. A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.

10.18. A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.

10.19. Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência da CAIXA por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA.

11. CERTIFICADOS E RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS REQUERIMENTOS MÍNIMOS DE SEGURANÇA.

11.1. Para serviços de nuvem, caso a Contratada pela CAIXA e o Provedor de Serviços em Nuvem sejam empresas diferentes, a referida Contratada terá a responsabilidade de obter as documentações exigidas do Provedor, para apresentação à CAIXA.

11.2. Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo. O Due Diligence presencial é facultativo e será feito a critério da CAIXA.

11.3. Caso o prazo de validade da certificação ainda esteja vigente com relação à última apresentação, não é necessária uma nova apresentação.

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada	SOB DEMANDA

	Contratada para verificar os requisitos de segurança presente nas cláusulas	relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	pela CAIXA	
Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrito nas cláusulas	Documentos previstos nas cláusulas e demais comprovantes de seus requisitos. Quando não comprovados por certificação, os itens exigidos nas cláusulas devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens das cláusulas, desde que ratificados por empresa de auditoria independente	SOB DEMAND A

11.4. CERTIFICAÇÕES APLICÁVEIS AOS FORNECEDORES DE SERVIÇOS EM NUVEM:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
FIPS 140-2 Nível 2 para SaaS e PaaS e FIPS 140-2 nível 3 para IaaS	Garantir que o provedor tenha mecanismo seguro para proteção de chaves criptográficas que sustentem os seus processos	Certificação do NIST que atesta um nível elevado de segurança para o HSM	Apresentar certificado FIPS 140-2 para equipamento utilizado no Provedor de Serviços em Nuvem	ANUAL
Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de	SOC TYPE 2 Fornece relatórios com descrição do ambiente de	Disponibilizar relatório de auditoria em nome do Provedor de Nuvem	ANUAL

	auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade, confidencialidade e privacidade	controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA		
--	---	--	--	--

12. ENCERRAMENTO DO CONTRATO

12.1. A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.

12.2. A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.

12.3. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

12.4. A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

12.5. Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

13. NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS

13.1. O não cumprimento, pela Contratada, de qualquer um dos seguintes requisitos de segurança, definidos neste instrumento contratual, ensejará a aplicação das penalidades

previstas neste contrato e poderá, a critério da Contratante, ensejar a rescisão imediata do contrato, sem prejuízo de outras medidas cabíveis:

- a) Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
- b) Não comunicar ocorrências de intrusão real;
- c) Não fornecer relatório mensal sobre as tentativas de intrusão;
- d) Não fornecer o planejamento de correção de vulnerabilidades;
- e) Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
- f) Não fornecer os relatórios de incidentes conforme SLA;
- g) Não prestar as informações e relatórios solicitados pela CAIXA;
- h) Não fornecer relatório indicando conformidade com o NIST SP 800-88.
- i) Não atender a convocação da CAIXA para Due Diligence presencial ou remoto;
- j) Não fornecer a documentação solicitada em decorrência do Due Diligence presencial ou remoto, conforme prazo acordado entre as partes;
- k) Não fornecer os relatórios de auditoria externa independente, para as empresas que não possuem a certificação SOC2;
- l) Não fornecer certificação SOC2;
- m) Não fornecer certificação FIPS 140-2 Nível 3 ou FIPS 140-2 nível 2.