

ANEXO I-C

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 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 solução independente da própria instância do banco de dados, ou seja, que não dependa apenas dos logs internos do SGBD, mas que permita a fiscalização e auditoria por mecanismos externos e confiáveis.
- 1.25.1. Nos casos em que a arquitetura não permite a instalação de agentes externos, por exemplo SaaS ou PaaS gerenciadas, a apresentação dos logs nativos, trilhas de auditoria e relatórios fornecidos pela própria plataforma de nuvem é suficiente, desde que:
- As evidências permitam a identificação inequívoca das ações administrativas,
 - Seja possível configurar alertas e respostas automatizadas,
 - A documentação técnica comprove a aderência aos requisitos da CAIXA
- 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 na seção 2.7.

- 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. SEGURANÇA DE PLATAFORMAS

- 2.1. A Contratada deve realizar a configuração dos seus ativos baseada no princípio da menor funcionalidade, segundo o qual apenas as funções e serviços necessários às operações essenciais da Contratada devem ser mantidos.
- 2.2. A Contratada deve fazer o hardening de seus servidores, endpoints e demais ativos de TI, considerando um baseline de segurança previamente definido. Esse baseline deve ser fornecido à CAIXA sempre que solicitado.
- 2.3. A Contratada deve verificar a configuração dos ativos quanto à conformidade de segurança pelo menos anualmente.
- 2.4. A Contratada deve implementar política de antivírus que garanta a atualização dos seus ativos de TI em relação a todas as vacinas disponibilizadas pelo fabricante.
- 2.5. A Contratada deve configurar e manter software de proteção de endpoints nos computadores relacionados ao objeto do contrato, para realizar as verificações ativas e responder adequadamente. A solução de proteção deve dispor de funcionalidades para interromper as conexões ativas caso seja detectada uma intrusão.
- 2.6. Exceções/exclusões de verificação e proteção de endpoint poderão ser aplicadas nos equipamentos de TI do desenvolvimento, em especial para aplicações que utilizam tecnologia web, com intuito de se obter um equilíbrio entre o desempenho e a segurança. Tais exceções devem ser baseadas em estudos e avaliações técnicas que comprovem a perda da performance, e devem ser devidamente documentadas e aprovadas pelos responsáveis da Contratada.
- 2.7. O uso de dispositivos de armazenamento móveis, e-mails recebidos e enviados, upload de informação/dados e recursos semelhantes devem permanecer sob o controle do programa de proteção de Endpoints, obedecendo a políticas de prevenção de perda de dados (DLP – Data Loss Prevention).
- 2.8. O uso de dispositivos de armazenamento móveis (como pendrives e discos externos/removíveis) deve ser controlado por perfis de acesso definidos e gerenciados pela Contratada, considerando a ampla restrição a esse tipo de dispositivos como regra geral.

- 2.9. Os dados gravados em dispositivos de armazenamento móveis devem ser previamente criptografados, levando em conta os requisitos descritos na seção 2.7.
- 2.10. A Contratada deve ter uma política para o uso, a guarda e o descarte das mídias digitais de armazenamento externo, de modo a garantir a confidencialidade dos dados nelas armazenados. O descarte das mídias deve considerar os requisitos definidos na seção 2.8.
- 2.11. A Contratada deve gerenciar dispositivos móveis, como celulares e tablets, por meio de uma solução de MAM/MDM. O processo de registro/autorização do dispositivo deve ser automatizado, com base em múltiplos fatores de autenticação. Em caso de dispositivos Apple solicita-se também o cadastro do ABM – Apple Bussines Manager - de forma a garantir as configurações de MDM sem a intervenção dos usuários finais.
- 2.12. Os dados armazenados em dispositivos móveis devem ser criptografados pela solução de MDM e a Contratada deve ter a capacidade de fazer exclusão remota (wiping) em dispositivos móveis corporativos.
- 2.13. Caso a Contratada permita BYOD ou o uso de dispositivos móveis particulares em atividades laborais, ela deve estabelecer uma separação lógica dos dados organizacionais dos dados pessoais do seu funcionário, de modo a limitar a capacidade de propagação dos dados organizacionais e facilitar a exclusão remota desses dados.

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. Caso o firewall esteja em ambiente de um Provedor de Serviços em Nuvem, este garantirá a adequação do ambiente aos itens descritos e manterá as certificações solicitadas pela CAIXA, como descrito no item 4.
- 3.6. 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).
- 3.7. O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de intrusão suspeitas ou reais.
- 3.8. A Contratada deve informar imediatamente à CAIXA em caso de intrusão real, e informar à CAIXA em relatório mensal sobre as tentativas de intrusão suspeitas.
- 3.9. A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).
- 3.10. As soluções de firewall, IPS e anti-DDoS utilizadas pela Contratada serão validadas pela CAIXA a partir de documentações do fabricante ou certificações. No caso em que a Contratada sustentar a rede através de um Provedor de Serviços em Nuvem serão aceitas as certificações descritas no item 4 como garantia de conformidade de segurança no ambiente.
- 3.11. A Contratada deve impedir o uso do protocolo Bluetooth para a transferência de dados.
- 3.12. Todas as comunicações e trocas de informações entre a Contratada e a CAIXA devem ser realizadas por meio de conexão protegida, com TLS versão 1.3.
- 3.13. Excepcionalmente, quando a versão 1.3 do TLS não for suportada, deve ser usada a versão 1.2.
- 3.14. 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. GESTÃO DE VULNERABILIDADES

- 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, assim como deve adotar as melhores práticas de mercado de análise de código automatizada, utilizando como referência os padrões do OWASP.

- 4.2. A Contratada deve possuir um processo de Gestão Contínua de Vulnerabilidades, sem custo adicional para a CAIXA, observando prazos para remediação em normativo específico estabelecido pela CAIXA, conforme a criticidade da falha encontrada.
- 4.3. 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.
- 4.4. A Contratada deve realizar testes independentes de intrusão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA, seguindo frameworks de melhores práticas aplicáveis a testes dessa natureza.
- 4.5. Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados à CAIXA sempre que solicitado.

5. GESTÃO DE INCIDENTES DE SEGURANÇA

- 5.1. 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.
- 5.2. 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.
- 5.3. Em caso de incidentes relacionados ao objeto do contrato ou à CAIXA, a contratada deverá comunicar os incidentes detectados à CAIXA dentro do prazo estabelecido, conforme os termos do Acordo de Nível de Serviço (SLA) definido no contrato.
- 5.4. A Contratada deve ter um processo de notificação de incidentes 24x7.
- 5.5. No caminho inverso, se a CAIXA detectar um incidente de segurança, a Contratada será notificada e deverá cooperar totalmente para resolver o incidente de segurança, fornecendo todas as informações relacionadas que possam levar a solução do incidente em questão (também 24x7).
- 5.6. 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.

- 5.6.1. Relacionadas abaixo algumas possibilidades, de forma exemplificativa, de como pode ser atendido o item.

1. Tabela de Casos de Uso Documentados

Caso de Uso	Finalidade	Ferramentas Utilizadas	Tipo de Evento Monitorado	Correlação com Cenários de Ataque
Detecção de login suspeito	Prevenir acessos não autorizados	SIEM (ex: Splunk, QRadar)	Tentativa de login fora do horário ou geolocalização incomum	Ataque de força bruta, credenciais comprometidas
Monitoramento de alterações em arquivos críticos	Detectar atividades maliciosas	File Integrity Monitoring (ex: Tripwire)	Mudança em arquivos de sistema	Malware, acesso não autorizado
Monitoramento de tráfego de rede	Identificar tráfego suspeito	IDS/IPS (ex: Snort, Suricata)	Anomalias em pacotes de rede	Escaneamento, exfiltração de dados
Detecção de comportamento anômalo de usuários	Prevenir ações internas maliciosas	UEBA (ex: Exabeam)	Acesso incomum a dados sensíveis	Insider threats, acesso indevido

Relatório Descritivo:

- Breve descrição de cada caso de uso
- Arquitetura da solução adotada
- Tecnologias e fabricantes envolvidos
- Procedimentos de coleta, análise e correlação de eventos
- Exemplos de alertas gerados

- Procedimentos de resposta a incidentes associados

Fluxogramas ou Diagramas

- Diagramas de fluxo das etapas de detecção e correlação de eventos
- Mapas de arquitetura de segurança mostrando integração entre ferramentas
- Representação visual de como os casos de uso estão alinhados com os padrões da CAIXA

Evidências de Conformidade

- Prints de dashboards de monitoramento
- Logs de eventos correlacionados
- Alertas gerados em cenários de testes
- Relatórios de auditoria interna

- 5.7. 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.
- 5.8. 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.
- 5.9. Atuar tempestivamente para cessar, responder e tratar incidentes, crises e ataques comunicando o contratante quando identificados os que são relacionados a Caixa e os seus dados.
- 5.10. Se a Contratada precisar envolver outras partes externas para investigar que afetem o escopo do objeto contratado com a CAIXA, 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.

6. AUDITORIA CONTÍNUA

- 6.1. 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.

- 6.2. A contratada deverá informar imediatamente à CAIXA sobre qualquer auditoria regulatória relacionada aos serviços prestados à CAIXA, bem como sua finalidade e impactos.
- 6.3. A Contratada deve informar à CAIXA caso sejam contatados por um órgão regulador e se o propósito desse contato guardar relação com/ou afetar os serviços prestados à CAIXA.
- 6.4. 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.

7. CONTROLES CRIPTOGRÁFICOS

- 7.1. Os requisitos apresentados nesta seção 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 e o Provedor deve atender, além dos requisitos a seguir, as regras descritas no item 3.3 deste Guia.
- 7.2. 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.
- 7.3. 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.
- 7.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 7.5. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 7.6. 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.

- 7.7. 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-member-services/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.
- 7.8. 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>).
- 7.9. As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 7.10. 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.
- 7.11. 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).
- 7.12. A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.
- 7.13. 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.
- 7.14. 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.
- 7.15. 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.

- 7.16. A Contratada deve permitir a auditoria da segurança de chaves criptográficas utilizadas para fornecimento do objeto da contratação.
- 7.17. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3, ou, quando não for suportado, 1.2.
- 7.18. A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.2 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
- 7.19. Os parâmetros TLS Renegotiation e TLS Resumption devem estar desabilitados.
- 7.20. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão mTLS, por exemplo – a Contratada deve fazer todas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.
- 7.21. O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.

8. ENCERRAMENTO DO CONTRATO

- 8.1. Os requisitos apresentados nesta seção 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 ocorre somente em ambiente de nuvem.
- 8.2. 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.
- 8.3. A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

- 8.4. A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer os 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.
- 8.5. 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.

9. GLOSSÁRIO

- 9.1. AICPA (American Institute of Certified Public Accountants) - Instituto Americano de Contadores Públicos Certificados - É a associação profissional nacional dos contadores dos Estados Unidos, com mais de 330.000 membros, incluindo contadores com atuação em negócios, indústria, governo e educação, estudantes e associados estrangeiros.
- 9.2. Atividades críticas - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo (Adaptado da portaria PR/GSI nº 93, de 26 de setembro de 2019).
- 9.3. BYOD (Bring Your Own Device) – política que prevê a utilização de recursos do próprio empregado para realização das atividades laborais.
- 9.4. CASB (Cloud Access Security Broker) – Agente de segurança em nuvem que monitora as atividades e aplica políticas de segurança.
- 9.5. Dados estratégicos – dados que subsidiam a tomada de decisão, planos estratégicos, planejamentos, diretrizes, análise de riscos, oportunidades e ambições da CAIXA, podendo estar relacionados a processos e/ou produtos estratégicos/prioritários para a empresa. A perda, modificação ou divulgação não autorizada desses dados pode afetar a competitividade e a governança corporativa da CAIXA.
- 9.6. Fornecedor – pessoa física ou jurídica Contratada para fornecer bens ou serviços para a CAIXA, o qual se encontra integrado à cadeia produtiva da empresa.
- 9.7. FIPS (Federal Information Processing Standards) – padrões desenvolvidos pelo NIST para uso em sistemas de computador por agências do governo americano não-militares e contratantes do governo.

- 9.8. Gestor de TI – empregado com atribuições gerenciais designado pela Unidade Executora para coordenar e comandar a utilização e execução no tocante aos aspectos técnicos do contrato, conforme TE165.
- 9.9. Hardening - é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- 9.10. HSM (Hardware Security Module) – equipamento para o armazenamento seguro de chaves criptográficas.
- 9.11. Informação Corporativa - informação não pública que possui valor para o negócio da CAIXA e sua perda, modificação ou divulgação não autorizada pode gerar impactos para a CAIXA.
- 9.12. Informação Pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem abrangendo clientes ou empregados da CAIXA.
- 9.13. Key Vault – Estrutura segura de armazenamento para chaves criptográficas e certificados.
- 9.14. LGPD – Lei Geral de Proteção de Dados, no 13.709 de 14 de agosto de 2018.
- 9.15. MAM (Mobile Application Management) – Solução que permite controlar os dados de negócios nos dispositivos pessoais dos usuários.
- 9.16. MDM (Mobile Device Management) – Solução que permite configurar políticas de proteção de dados em seus dispositivos móveis. Quando um dispositivo está sob o gerenciamento de dispositivo móvel, é possível controlar todo o dispositivo, apagar dados dele e também redefini-lo para as configurações de fábrica.
- 9.17. NAC (Network Access Control) – Tecnologia que viabiliza a implementação de políticas para controlar o acesso à rede corporativa. Tais políticas podem ser baseadas em autenticação do dispositivo, configuração do endpoint (postura) ou identidade do usuário.
- 9.18. NIST (National Institute of Standards and Technology) – Instituto de padrões de tecnologia do governo dos Estados Unidos da América.
- 9.19. OTP (One Time Password) – Senha de uma única utilização.

- 9.20. OWASP (Open Web Application Security Project) – Fundação que orienta internacionalmente ações para melhoria da segurança de software.
- 9.21. Regime de Resolução - quando uma instituição financeira apresenta grave comprometimento do seu patrimônio ou dificuldade de honrar seus compromissos, o Banco Central (BC) pode determinar aos seus controladores que aportem os recursos necessários, transfiram o controle, reorganizem a sociedade ou adotem medidas de recuperação.
- 9.22. Relacionamento com Fornecedor – conjunto de ações realizadas previamente e durante a vigência dos contratos que favoreçam a gestão dos mesmos, mantendo-se um clima de parceria, sem prejuízo do acompanhamento do cumprimento das cláusulas contratuais.
- 9.23. Tratamento de Dados - toda operação realizada com dados pessoais ou corporativos, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- 9.24. SOC (Service Organization Controls) – Serviço de auditoria independente que avalia requisitos de conformidade e geração de relatórios.
- 9.25. SSO – Ferramenta de Single Sign-On