

CLÁUSULAS DE 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 logon.
- 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 oferecer 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 deve 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 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. Este baseline será 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 ter 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 instalar, manter e gerenciar centralmente um software antimalware em seus ativos corporativos, configurando atualizações automáticas para arquivos de assinatura e utilizando tecnologias de detecção comportamental.
- 2.6. 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 terá funcionalidades para interromper as conexões ativas caso seja detectada uma intrusão.

- 2.7. A Contratada deve aplicar 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.
- 2.8. A Contratada deve manter sob controle do programa de proteção de endpoints o uso de dispositivos de armazenamento móveis, e-mails recebidos e enviados, upload de informações/dados e recursos semelhantes, garantindo conformidade com as políticas de prevenção de perda de dados (DLP – Data Loss Prevention).
- 2.9. A Contratada deve controlar o uso de dispositivos de armazenamento móveis (como pendrives e discos externos/removíveis) por meio de perfis de acesso definidos e gerenciados pela própria contratada, considerando como regra geral a ampla restrição a esse tipo de dispositivo.
- 2.10. A Contratada deve criptografar os dados gravados em dispositivos de armazenamento móveis, observando os requisitos descritos no item 9.
- 2.11. 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 considerará os requisitos definidos no item 12.
- 2.12. 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.
- 2.13. A Contratada deve criptografar os dados armazenados em dispositivos móveis por meio da solução de MDM, a qual deve possuir capacidade de realizar exclusão remota (wiping) desses dados.
- 2.14. Caso a Contratada permita BYOD ou o uso de dispositivos móveis particulares em atividades laborais, será estabelecida 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. 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 tratem 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 ou história de usuário.
- 5.5. A Contratada deve conduzir uma avaliação de risco e ameaças, contemplando inclusive os testes baseados em casos de uso ou história de usuário, 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 escalação 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 negociados e 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 ou ISO27001 , 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 na 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, confidencialidade e privacidade	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 segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA	Disponibilizar relatório de auditoria em nome da empresa	ANUAL
----------------------------------	--	---	--	-------

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;



Brasília, DD MM AAAA

Modelo ISCF - Incidente de Segurança Cibernética em Fornecedor

ISCF – Incidente de Segurança Cibernética em Fornecedor

ISCF Nº: xxxx/2024	TICKET Nº: Identificação interna do incidente no ambiente do fornecedor ex.: ID122024, TK012025, TH142026	
Descrição resumida da ocorrência	Ex. Ataque DDoS no sistema XPTO	
Período (data/hora) do incidente	Data início:	Hora início:
	Data fim:	Hora fim:
Severidade	Crítica ou Alta	
Característica da violação de segurança da informação apresentada.	☐ Confidencialidade ☐ Disponibilidade ☐ Integridade	
Origem do alerta	Ex. SIEM, E-mail, denúncia interna/externa, Polícia Civil etc.	
Serviço afetado: ex.: serviço de cobrança XYZ, url: http://www.teste.com	Gestor operacional CAIXA Área - ex.: CECOT, CESEG, CESET	
	Contrato CAIXA: ex: 01-2024	
Comunicado Incidente segurança	abuse@caixa.gov.br	
Comunicado ISDP	gerit10@caixa.gov.br	

1. INTRODUÇÃO

<Breve descrição ao leitor sobre o objetivo e informações que serão detalhadas a seguir nas fases do processo>.

2. ANÁLISE RESUMIDA DA OCORRÊNCIA

<As informações constantes nas seções que seguem devem ser objetivas, sem pré-julgamentos de fatos e baseada em informações evidenciadas em logs e regras.>

2.1. DETECÇÃO

- <Informar como o evento foi detectado (ex.: Email externo ou interno, SIEM, Teams etc.)>*
- 2.2. **ANÁLISE**
<Informar a classificação do incidente, tática utilizada pelo atacante, POP, playbook utilizado etc.>
- 2.3. **CONTENÇÃO**
<Informar todas as ações que foram necessárias para conter o incidente (ex: isolamento de máquinas, bloqueio de usuários, bloqueio de IP, takedown de páginas etc.)>
- 2.4. **ERRADICAÇÃO**
<Caso existam, informar todas as ações que foram necessárias para erradicar as fragilidades que permitiram o incidente (ex.: Atualização de patch, alteração em regras de firewall, alteração em permissionamento de acessos etc.)>
- 2.5. **RECUPERAÇÃO**
<Caso existam, informar servidores, serviços ou aplicações que foram afetadas e que precisaram ser recuperadas por todas as áreas envolvidas.>

3. CONCLUSÃO

3.1. ANÁLISE FINAL DE PÓS-INCIDENTE

<Breve descrição ao leitor sobre a finalização do incidente relatando outros desdobramentos em função da ocorrência como: comunicados externos realizados, monitoramentos criados, dificuldades encontradas na investigação, queixa crime solicitada via polícia etc.>.

4. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

4.1. FORMULÁRIO ISDP

<Nas ocorrências em que se observe qualquer tipo de violação de dados pessoais, conforme disposição da LGPD, o fornecedor deverá complementar o comunicado com as informações a seguir para os casos ISDP, comunicando também a equipe da GERIT:>

4.1.1 COMUNICAÇÃO

4.1.1.1 Tipo de Comunicação

☐ Completa.

☐ Parcial.

Comentário:

4.1.1.2 Para comunicação parcial

☐ Preliminar

☐ Complementar

Comentário:

4.1.1.3 Critério para comunicação

☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐ Não foi identificado riscos relevantes aos titulares

☐ Impacto continua sob avaliação

Comentário:

4.2 IDENTIFICAÇÃO DO AGENTE DE TRATAMENTO

4.2.1 Responsabilidade no tratamento de dados envolvido

☐ Controlador.

☐ Operador.

Comentário:

4.2.2 Comunicação ao Controlador

☐ Não necessária, o notificante é o Controlador.

☐ O Controlador já foi notificado.

☐ O Controlador não foi notificado.

Comentário:

4.2.3 Identificação da empresa

Número do CPF ou CNPJ:

Nome ou Razão Social:

Natureza da Organização (Pública ou Privada):

Endereço:

Cidade:

Estado:

CEP:

E-mail:

Comentário:

4.2.4 Dados do notificante

Nome

E-mail

Telefone

4.2.5 Dados do encarregado

☐ Mesmos do notificante

Nome

E-mail

Telefone

4.3 SOBRE O INCIDENTE DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

4.3.1.1 Breve Descrição

4.3.1.2 Quando o incidente ocorreu

Data e hora de confirmação

Comentário

4.3.1.3 Quando a organização teve ciência do incidente de segurança

Data e hora de confirmação

Comentário

4.3.1.4 Justificativa quando a comunicação inicial do incidente não ocorrer no prazo sugerido de 2 dias úteis

Comentário

4.3.1.5 Justificativa quando a comunicação não ocorrer de forma imediata

Comentário

4.3.1.6 Qual a natureza dos dados afetados

☐ Origem racial ou étnica

☐ Convicção religiosa

☐ Opinião política

☐ Filiação a sindicato

☐ Filiação a organização de caráter religioso, filosófico ou político.

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

☐ Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.

Comentário

4.3.1.7 *Qual a quantidade de titulares afetados*
Comentário

4.3.1.8 *Qual a categoria dos dados afetados*

☐ Funcionários

☐ Prestadores de serviço

☐ Clientes

☐ Consumidores

☐ Usuários

☐ Pacientes de serviço de saúde

☐ Crianças ou adolescentes

☐ Outros (Comentar)

Comentário

5 MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

5.1 *Medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança.*

Comentário

5.2 *Medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança.*

Comentário

5.3 *Medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados*

Comentário

5.4 *O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?*

Comentário

6 RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

6.1 *Quais as prováveis consequências do incidente de segurança para os titulares afetados?*

Comentário

6.2 *Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?*

☐ Sim

☐ Não

Comentário

6.3 *Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?*

☐ Sim

☐ Não

Comentário

6.4 *Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?*

Comentário