

ANEXO I-D

REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES DE 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 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. A Contratada não deverá ter permissão de uso ou acesso direto ao ambiente de autenticação da CAIXA.
- 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;
 - IP e Porta do equipamento que originou o 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. A Contratada, por meio próprio ou do Provedor de Serviços em Nuvem, deve dispor de recurso que permita o gerenciamento centralizado de eventos e envio para a CAIXA de logs/informações para sistemas de terceiros On-Premises, por exemplo, SIEM. Caso o Provedor disponibilize o serviço de SIEM em recurso próprio, e sendo este serviço aprovado pela CAIXA, pode ser dispensada a necessidade de receber os dados no SIEM da CAIXA.
- 1.27. Os registros de logs da Contratada deverão incluir ainda todos os acessos, incidentes e eventos cibernéticos, no ambiente do mesmo, pelo período mínimo de 1 ano, sendo o prazo ideal de armazenamento o de 5 anos.
- 1.28. 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.
- 1.29. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 1.30. 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.
- 1.31. 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.
- 1.32. 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.
- 1.33. 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.
- 1.34. Quando a autenticação na nuvem for provida pela Contratada, esta deverá prover autenticação por múltiplos fatores para o acesso dos empregados da CAIXA, que precisem acessar os recursos.

- 1.35. 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 da prestadora de serviços.
- 1.36. A Contratada deve permitir que somente os usuários autorizados pela CAIXA tenham acesso aos recursos em conformidade aos respectivos perfis de uso.

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. Este 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 no item 9.
- 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 no item 11.
- 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.
- 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. 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, CASB, IPS e anti-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 1.2 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).
- 3.13. No caso em que a Contratada sustentar a rede através de um Provedor de Serviços em Nuvem serão aceitas as certificações descritas no item 8 como garantia de conformidade de segurança no ambiente quanto aos requisitos deste item 3.

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.
- 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. Para este item 6 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.
- 6.2. Se os dados estiverem exclusivamente no Provedor, a Contratada deverá comprovar por relatório de auditoria (Due Dilligence Remoto) que o armazenamento ocorre somente em ambiente de nuvem.
- 6.3. Feitas as comprovações mencionadas no item 6.2, a entrega das certificações por parte do Provedor dispensa a comprovação por auditoria de cada um dos requisitos deste item 6.
- 6.4. 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.
- 6.5. 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.

- 6.6. A Contratada deve realizar testes independentes de penetração 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.
- 6.7. A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.
- 6.8. 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.
- 6.9. A Contratada deve comunicar os incidentes detectados à CAIXA dentro do prazo acordado, conforme termos do SLA definido em contrato.
- 6.10. A Contratada deve ter um processo de notificação de incidentes 24x7.
- 6.11. 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).
- 6.12. 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.
- 6.13. 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.
- 6.14. 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.
- 6.15. 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.
- 6.16. 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. Caso a Contratada utilize um Provedor de Serviços em Nuvem para todos os serviços, a apresentação das certificações exigidas no item 8 por parte do provedor já serão consideradas suficientes para garantir os processos deste item 7.
- 7.2. 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.
- 7.3. 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.
- 7.4. 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.
- 7.5. 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;
- 7.6. A obrigatoriedade do plano de continuidade se estende para empresas que sejam subcontratadas pela Contratada.

- 7.7. 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.
- 7.8. A avaliação de riscos e dos processos críticos devem levar em consideração instrumentos específicos, como um BIA – Business Impact Analysis.
- 7.9. 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. Caso a Contratada pela CAIXA e o Provedor de Serviços em Nuvem forem empresas diferentes, a referida Contratada terá a responsabilidade de obter as documentações exigidas do Provedor junto ao mesmo, para apresentação à CAIXA.
- 8.4. Caso o prazo de validade das documentações entregues ainda esteja vigente com relação à última apresentação, não é necessária uma nova apresentação, ainda que o quadro de certificações indique uma periodicidade inferior para entrega.
- 8.5. 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.
- 8.6. 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.
- 8.7. A Contratada e o Prestador de Serviços em Nuvem deverão possuir as seguintes certificações e processos de auditoria disponíveis, apresentados periodicamente, conforme coluna Vigência:

REQUISITOS	TIPO	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Certificação CSA STAR NÍVEL 2 - CSA Security Trust Assurance Risk	OBRIGATÓRIO	Avaliação independente sobre a segurança de um provedor de serviços em nuvem.	É uma avaliação, realizada por auditores independentes sobre a segurança de um provedor de serviços de nuvem.	Apresentar certificação emitida Cloud Security Alliance - CSA O certificado deve ser em nome do provedor de serviços em nuvem e deve constar o nome das regiões de processamento certificadas	ANUAL
FIPS 140-2 nível 3	OBRIGATÓRIO	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 nível 3 para equipamento usado no ambiente do Provedor de Serviços em Nuvem.	ANUAL
Certificação SOC 1 ou ISAE 3402	OBRIGATÓRIO	Garantir que os relatórios de controle são realizados por auditoria independente com o objetivo de evidenciar o atendimento aos padrões de controles que protege a confidencialidade e a privacidade de informações	Descreve o sistema do provedor de serviços em nuvem e avalia a veracidade da descrição fornecida pelo provedor sobre seus controles, além de avaliar se os controles foram projetados	Disponibilizar relatório de auditoria em nome do Provedor de Serviços em Nuvem	SEMESTRAL

		armazenadas e processadas na nuvem.	apropriadamente, se estavam em operação em determinada data e se funcionaram de forma efetiva durante um período específico.		
Certificação SOC 2 – Tipos 1 e 2	OBRIGATÓRIO	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 do Provedor de Serviços em Nuvem	SEMESTRAL

9. CONTROLES CRIPTOGRÁFICOS

- 9.1. Caso a Contratada utilize um Provedor de Serviços em Nuvem para armazenar e processar dados criptográficos, os controles deste item 9 deverão ser seguidos pelo Provedor sempre que couber.
- 9.2. A Contratada, por meio próprio ou através do Prestador de Serviços em Nuvem, 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.
- 9.3. 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.

- 9.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 9.5. A Contratada, por meio próprio ou através do Prestador de Serviços em Nuvem, deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 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, por meio próprio ou através do Prestador de Serviços em Nuvem, 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, por meio próprio ou através do Prestador de Serviços em Nuvem, 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, por meio próprio ou através do Prestador de Serviços em Nuvem, 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, por meio próprio ou através do Prestador de Serviços em Nuvem, deve permitir a auditoria da segurança de chaves criptográficas.
- 9.12. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados, com autenticação mútua, por meio do TLS 1.2 ou versão superior, esta exigência se estende para as comunicações entre o Provedor e a Contratada e entre o Provedor e a CAIXA.
- 9.13. A solução deverá prover a criptografia de arquivos em repouso utilizando chave simétrica usando, no mínimo, algoritmo AES com chaves de 128 bits ou 3DES com 168 bits.
- 9.14. Caso haja uso de chave simétrica, deverá estar disponível função para que a CAIXA mantenha o controle desta chave, ainda que a chave esteja armazenada no Provedor de Serviços em Nuvem.

- 9.15. A chave simétrica no ambiente do Provedor de Serviços em Nuvem deverá ser armazenada em HSM, homologado em FIPS 140-2 nível 3.
- 9.16. Caso haja a publicação de URLs da CAIXA no ambiente da Contratada ou do Provedor, a gestão dos certificados digitais deve ser feita de acordo com um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pela CAIXA.
- 9.17. O compartilhamento de chaves entre o Provedor de Serviços em Nuvem e a CAIXA deve ser feito de acordo com processos e tecnologias de gerenciamento de chaves que sigam um padrão internacional reconhecidamente aceito.
- 9.18. 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 privadas envolvidas.
- 9.19. Todas as chaves privadas, associadas aos certificados digitais emitidos, devem ser armazenadas no ambiente do provedor, em key vaults baseados em HSM, certificados no padrão FIPS 140-2 nível 3.
- 9.20. Após a instalação dos certificados, deverão ser realizados testes utilizando a ferramenta Qualys SSL Labs <https://www.ssllabs.com/ssltest>, na qual deverá ser obtida a qualificação “A” para todas as URLs.
- 9.21. Os Certificados Digitais A1 SSL/TLS para Servidor Web poderão ser individualizados para cada URL implantada ou do tipo SAN (Subject Alternative Name), onde um único certificado pode conter várias URL, conforme definição da CAIXA.
- 9.22. A CAIXA definirá a Autoridade Certificadora que será utilizada na emissão dos certificados e fornecerá a cadeia certificadora para a Contratada sempre que necessário.
- 9.23. A CAIXA controlará o prazo de expiração dos certificados fornecidos à Contratada.
- 9.24. O Prestador de Serviços em Nuvem deverá possuir a capacidade de configuração das cifras criptográficas e da versão de TLS 1.2 ou superior utilizadas pela CAIXA, suportando, no mínimo, 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

- 9.25. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão mTLS, por exemplo – o Prestador de Serviços em Nuvem deverá fazer todas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.
- 9.26. O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.
- 9.27. 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.
- 9.28. O Provedor de Serviços em Nuvem deve permitir que a própria chave de objeto ou recurso seja criptografada por uma chave separada.
- 9.29. O Provedor de Serviços em Nuvem deve permitir que dados criptografados, chaves de criptografia e chaves mestras sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.
- 9.30. O Provedor de Serviços em Nuvem deverá possibilitar comunicação criptografada e protegida para transferência de dados.
- 9.31. 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.

10. POLÍTICA DE BACKUP

- 10.1. Caso os dados fiquem armazenados somente em um Provedor de Serviços em Nuvem, a garantia de backup é realizada pelo Provedor, de forma que a Contratada deve apresentar as certificações mencionadas no item 8 deste Guia em nome do Provedor, como ateste da realização deste processo.
- 10.2. 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.
- 10.3. 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.
- 10.4. 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 seção 7.

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

11. ENCERRAMENTO DO CONTRATO

- 11.1. 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.
- 11.2. A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.
- 11.3. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.
- 11.4. 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.
- 11.5. 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.
- 11.6. Caso os dados estejam armazenados exclusivamente em nuvem, caberá à Contratada interagir junto ao Provedor de Serviços em Nuvem para garantir o cumprimento dos requisitos deste item 11.

12. REQUISITOS DE PRIVACIDADE

- 12.1. A Contratada deve instituir e manter programa de governança em privacidade, a ser homologado pela CAIXA, estabelecendo, minimamente, a capacitação de seus colaboradores, controles técnicos e administrativos apropriados para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais objeto de tratamento, além de garantir a conformidade com a LGPD e demais normas que versem sobre privacidade e proteção de dados pessoais.
- 12.2. Ao final do contrato, ou quando cumprida ou encerrada a finalidade instruída pela CAIXA, a Contratada deve utilizar técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir a sua recuperação.

- 12.3. Na ocorrência de qualquer incidente (perda, deleção ou exposição indesejada ou não autorizada, entre outros) que envolva as informações tratadas em razão da presente relação contratual, deverá a Contratada comunicar imediatamente a CAIXA através dos canais de comunicação específicos disponíveis, cabendo à CAIXA notificar o titular e/ou outras unidades competentes, nos termos da LGPD.
- 12.4. Deve ser garantido pela Contratada o direito ao esquecimento dos dados pessoais dos clientes CAIXA, de forma que a empresa esteja preparada para atuar neste sentido quando comunicada da requisição feita por um cliente específico para a remoção dos dados a serem esquecidos do ambiente da Contratada, nos termos da LGPD.
- 12.5. A Contratada deverá assinar Termo de Confidencialidade 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.
- 12.6. 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.
- 12.7. 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.

13. REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

- 13.1. A Contratada deve garantir que a prestação dos serviços não causará prejuízo ao funcionamento regular da CAIXA nem embaraço à atuação do Banco Central do Brasil, assegurando que os serviços prestados não restringem nem impedem o acesso da CAIXA nem do Banco Central do Brasil aos dados e às informações.
- 13.2. 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.
- 13.3. 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;

- 13.4. Esta mesma Contratada deve assegurar que os dados da CAIXA processados e armazenados na Contratada são de propriedade exclusiva da CAIXA.
- 13.5. 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.
- 13.6. A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.
- 13.7. 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;
- 13.8. Deve ainda atender à solicitação de Due Diligence sempre que formalmente demandada pela CAIXA.
- 13.9. 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.
- 13.10. 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.
- 13.11. 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:
- 13.12. 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;
- 13.13. 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 13 por parte do 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.

14. CONTROLES DE SEGURANÇA

- 14.1. A Contratada deverá adotar medidas para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações que serão tratadas na sua infraestrutura.
- 14.2. A Contratada, por meio próprio ou através do 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.
- 14.3. A Contratada deverá assegurar que o Provedor de Serviços em Nuvem dispõe de análise e gestão de riscos de segurança de informação, conforme dispõe a IN 5 PR/GSI, de 30 de agosto de 2021. A análise deve ter periodicidade mínima mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes.
- 14.4. A Contratada, por meios próprios ou do Provedor de Serviços em Nuvem, deve disponibilizar um meio para garantir a rastreabilidade dos documentos armazenados, para identificação em caso de vazamentos.
- 14.5. A Contratada deverá possuir ou criar uma política de atualização de versão de software, indicando sua criticidade e deve comunicar previamente a CAIXA a data da aplicação da atualização.
- 14.6. A Contratada deve fornecer o fluxo de acionamento e contato com a equipe de respostas a incidentes da CAIXA para acionamento em caso de ataques cibernéticos, ou indicar o fluxo adotado pelo Provedor de Serviços em Nuvem.
- 14.7. O Provedor de Serviços em Nuvem deve dispor de recurso centralizado que garanta a imposição contínua das políticas de segurança definidas para os recursos provisionados no ambiente de nuvem.
- 14.8. O Provedor de Serviços em Nuvem deve dispor de recurso que permita a monitoração, detecção e resposta a ameaças nos componentes hospedados na nuvem.
- 14.9. O Provedor de Serviços em Nuvem deverá possuir políticas de segurança e diretrizes para garantir o controle de acesso físico e lógico do seu ambiente.
- 14.10. A Contratada deverá, ainda, garantir que os dados da CAIXA estejam sendo tratados e armazenados de acordo com a legislação vigente, conforme IN 5 PR/GSI.
- 14.11. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o Provedor de Serviço em

Nuvem, devem estar hospedados em território brasileiro, com pelo menos uma cópia atualizada de segurança também no Brasil.

- 14.12. O uso de informações da CAIXA por parte do Provedor, ou da Contratada, para realização de propaganda, otimização de inteligência artificial, ou qualquer outro uso secundário, depende de autorização específica por parte da CAIXA.
- 14.13. 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.