ANEXO VI

REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES DE NUVEM

1. REQUISITOS DE NUVEM

1.1. A CAIXA entende como PROVEDOR DE SERVIÇOS EM NUVEM, as empresas que disponibilizam serviços em nuvem pública ou privada sob demanda em hiperescala. A hiperescala é a capacidade de uma arquitetura ser dimensionada de forma adequada conforme a demanda é aumentada e adicionada ao serviço.

1.2. Os serviços em nuvem consistem em infraestrutura como Serviço (IaaS), plataforma como Serviço (PaaS) e Software como Serviço (SaaS).

1.3. O PROVEDOR deverá fornecer os serviços de computação em nuvem em aderência seguintes princípios elencados pelo NIST:

1) Auto-provisionamento sob demanda (“on-demand self-service”): o consumidor pode ter a iniciativa de provisionar recursos na nuvem, e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem a necessidade de interação com cada provedor de serviços.

2) Acesso amplo pela rede (“broad network access”): os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (tais como: estações de trabalho, tablets e smartphones) através de mecanismos padrões.

3) Compartilhamento através de pool de recursos (“resource pooling”): Os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo multi-tenant), com recursos físicos e virtuais sendo alocados e realocados dinamicamente, de acordo com a demanda dos seus consumidores. Há uma ideia geral de independência de localização, uma vez que o cliente geralmente não possui controle ou conhecimento sobre a localização exata dos recursos providos. No entanto, é possível especificar este local em um nível mais alto de abstração (por exemplo: país, estado ou data center). Os serviços são concebidos como um padrão, com a finalidade de atender à demanda de vários consumidores de maneira compartilhada, não sendo focados em necessidades customizadas de um único consumidor.

4) Rápida elasticidade: os recursos podem ser elasticamente provisionados e liberados, e, em alguns casos, de maneira automática, adaptando-se à demanda. Do ponto de vista do consumidor, os recursos disponíveis para provisionamento parecem ser ilimitados, podendo ser alocados a qualquer hora e em qualquer volume.

5) Serviços medidos por utilização (“measured service”): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado (por exemplo: armazenamento, processamento, largura de banda, e contas de usuário ativas). A utilização dos recursos pode ser monitorada, controlada e reportada, fornecendo transparência tanto para provedores como para consumidores. Portanto, a precificação, se houver, será balizada pelo uso dos serviços.”

1.4. Os requisitos deste capítulo se aplicam às empresas que prestarão serviços em nuvem para a CAIXA, ou que irão manter a estrutura de atendimento para a CAIXA em nuvem pública, incluindo o armazenamento de arquivos corporativos que tenham relação com o trabalho desempenhado na CAIXA. As empresas Contratadas para prestação de serviços em nuvem também devem observar os controles relatados nos demais capítulos deste documento.

1.5. Os serviços em nuvem do tipo SaaS poderão ser provenientes tanto do marketplace ou do catálogo de serviços do provedor de nuvem, oriundos de um contrato de Multinuvem e fornecidos pelo provedor; quanto serviços de SaaS contratados a parte e provenientes de contratos específicos com a empresa fornecedora da solução.

2. Gestão de Identidade e Controle de Acessos

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

2.2. A Contratada deve 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.

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

2.4. 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.

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

2.6. 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.

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

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

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

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

2.11. 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.

2.12. 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.

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

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

2.15. 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.

2.16. 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.

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

2.18. 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.

2.19. 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.

2.20. 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.

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

2.22. 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.

2.23. 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.

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

2.25. 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.

2.26. 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.

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

2.28. 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.

2.29. 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 2.4.

2.30. 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.

3. Controles Criptográficos

3.1. 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 6 deste Guia.

3.2. 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.

3.3. 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.

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

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

3.6. 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.

3.7. 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=0FDB6C541E7A61976625B9EAC55474D260A

7E6FD para todas as raízes de cadeias utilizadas na emissão dos certificados digitais.

3.8. 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).

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

3.10. 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.

3.11. No caso de utilização de um Provedor de Serviços em Nuvem, as certificações FIPS exigidas estão descritas na seção 6.

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

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

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

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

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

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

3.18. 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.

3.19. A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.2 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

3.20. Os parâmetros TLS Renegotiation e TLS Ressumption devem estar desabilitados.

3.21. 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.

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

4. CONTROLE DE ACESSO AO AMBIENTE DE NUVEM

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

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

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

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

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

5. REQUISITOS DE AUTORIZAÇÃO DE ACESSO AOS DADOS PELO BACEN

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

5.2. 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.

5.3. 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;

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

5.5. 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.

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

5.7. 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.

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

5.9. 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.

5.10. 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.

5.11. 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:

5.12. 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;

5.13. 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 3.2 por parte da Provedor de Serviços em Nuvem, seja por meio de declaração própria durante o processo de contratação, seja por meio de aditivo contratual, caso não previsto inicialmente no contrato original.

6. PROTEÇÃO DOS DADOS ARMAZENADOS EM NUVEM

6.1. Além dos requisitos descritos na seção 3, a Contratada também deve permitir trabalhar com chaves simétricas e assimétricas geradas e armazenadas pela CAIXA. Para tanto, ela deve prover meios que permitam o envio das chaves da CAIXA para o seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.

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

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

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

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

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

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

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

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

6.10. 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.

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

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

7. MONITORAÇÃO DOS DADOS TRATADOS EM NUVEM

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

7.2. A trilha de auditoria deve conter, minimamente, itens descritos no item 2 deste documento.

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

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

8. SEGURANÇA DO TRÁFEGO DE DADOS COM A NUVEM

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

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

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

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

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

8.6. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela CAIXA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, com pelo menos uma cópia atualizada de segurança também no Brasil.

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

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

10. EVIDÊNCIAS DE CONFORMIDADE E PROCEDIMENTOS OPERACIONAIS PARA A FISCALIZAÇÃO DO FORNECEDOR

10.1. Com a existência de vários controles de segurança, muitos deles de caráter técnico, torna-se necessário que as áreas gestoras de Segurança da Informação, Segurança Cibernética, Arquitetura de TI e Risco de TI definam os procedimentos adequados de como realizar e registrar a fiscalização.

10.2. A seguir são definidas as formas de validação dos requisitos de segurança cibernética listados neste Guia e a etapa do ciclo de vida do fornecedor em que elas devem ser aplicadas. Trata-se de uma série de certificações reconhecidas no mercado, aplicáveis a fornecedores de solução em nuvem.

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

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

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

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança do presente Guia	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 descrição do Guia	Conjunto de documentos listados na seção 5, combinados com qualquer outro que se faça necessário para comprovar atendimento dos requisitos do Guia. Quando não comprovados por certificação, os itens exigidos no Guia devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens do Guia, desde que ratificados por empresa de auditoria independente Relatório de empresa de auditoria independente, a ser apresentado pela Contratada	SOB DEMANDA

10.6. CERTIFICAÇÕES APLICÁVEIS AOS FORNECEDORES DE SERVIÇOS EM NUVEM:

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

11. GLOSSÁRIO

11.1. 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.

11.2. 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).

11.3. BYOD (Bring Your Own Device) – política que prevê a utilização de recursos do próprio empregado para realização das atividades laborais.

11.4. CASB (Cloud Access Security Broker) – Agente de segurança em nuvem que monitora as atividades e aplica políticas de segurança.

11.5. 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.

11.6. Fornecedor – pessoa física ou jurídica, contratada para fornecer bens ou serviços para a CAIXA, o qual se encontra integrado à cadeia produtiva da empresa.

11.7. 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.

11.8. 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.

11.9. 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.

11.10. HSM (Hardware Security Module) – equipamento para o armazenamento seguro de chaves criptográficas.

11.11. 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.

11.12. Informação Pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem abrangendo clientes ou empregados da CAIXA.

11.13. Key Vault – Estrutura segura de armazenamento para chaves criptográficas e certificados.

11.14. LGPD – Lei Geral de Proteção de Dados, no 13.709 de 14 de agosto de 2018.

11.15. MAM (Mobile Application Management) – Solução que permite controlar os dados de negócios nos dispositivos pessoais dos usuários.

11.16. 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.

11.17. 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.

11.18. NIST (National Institute of Standards and Techology) – Instituto de padrões de tecnologia do governo dos Estados Unidos da América.

11.19. OTP (One Time Password) – Senha de uma única utilização.

11.20. OWASP (Open Web Application Security Project) – Fundação que orienta internacionalmente ações para melhoria da segurança de software.

11.21. 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.

11.22. 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.

11.23. 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.

11.24. SOC (Service Organization Controls) – Serviço de auditoria independente que avalia requisitos de conformidade e geração de relatórios.

11.25. SSO – Ferramenta de Single Sign-On