

ANEXO I
TERMO DE REFERÊNCIA

1. DESCRIÇÃO DO OBJETO

- 1.1. Contratação de empresa especializada para o fornecimento de solução tecnológica que operacionalize os serviços de controle de enquadramento dos fundos de investimento e carteiras, em conformidade com as exigências normativas dos Órgãos Reguladores, na modalidade SaaS (Software as a Service), em ambiente provisionado pela contratada, contemplando a implantação, sustentação e serviços de customização sob demanda e Transferência de conhecimento (sob demanda), para atendimento das demandas da CAIXA para Fundos de Investimento.
- 1.2. O objeto de contratação deve contemplar ainda a disponibilização segregada dos ambientes tecnológicos de produção, homologação e desenvolvimento, serviços de parametrização e configuração inicial da ferramenta, incluindo as integrações com a CAIXA, suporte técnico e atualização tecnológica, pelo prazo de 24 (vinte e quatro) meses, conforme termos e condições estabelecidos neste documento e anexos.

MODELO DE CONTRATAÇÃO		
GRUPO	DESCRIÇÃO	QTDE
GRUPO 1	Ativação da Solução – Configuração e Integrações iniciais (setup)	1
	Sustentação (valor fixo mensal)	Até 21 parcelas
GRUPO 2	Serviços de Customização (sob demanda)	5788 Horas
	Transferência de conhecimento (sob demanda)	2 Turmas

- 1.3. A especificação detalhada do objeto contendo os requisitos técnicos e as condições de prestação dos serviços, bem como as obrigações e responsabilidades específicas constam neste termo e nos anexos abaixo especificados:

ANEXO I-A	Forma de Execução e Fiscalização do Contrato
ANEXO I-B	Requisitos de Segurança Para Fornecedores
ANEXO I-C	Níveis de Serviço, Indicadores e Penalidades
ANEXO I-D	Catálogo de Serviços
ANEXO I-E	Padrão Tecnológico
ANEXO I-F	Plano de Contingência
ANEXO I-G	Segurança da Informação e Privacidade
ANEXO I-H	Requisitos De Segurança Tecnológica Para Fornecedores De Nuvem
ANEXO I-I	Infraestrutura Tecnológica – Método de conexão com a CAIXA
ANEXO I-J	Integrações Previstas na Implantação da Solução

2. DETALHAMENTO DO OBJETO**2.1. Confidencialidade da Informação**

- 2.1.1. Deverá manter a confidencialidade sobre todas as informações a respeito dos negócios, ideias, produtos, propostas ou serviços que sejam tratados no âmbito deste Termo de Referência.
- 2.1.2. A CONTRATADA não poderá revelar a terceiros, informações sobre organização, operação dos trabalhos e arquivos de dados, bem como quaisquer informações da CAIXA das quais vier a tomar conhecimento por força da natureza especial deste objeto de licitação, obrigando-se ainda a proibir que seus empregados ou prepostos o façam, assegurando sempre a necessária proteção ao sigilo destas informações.
- 2.1.3. Se obriga a revelar as informações decorrentes da contratação, exclusivamente, a seus prepostos e funcionários diretamente envolvidos nas atividades desde Termo de Referência.
- 2.1.4. A CONTRATADA deverá concordar em tomar as ações apropriadas para que os empregados e outros profissionais, sob sua direção e controle, que lidarem com as informações em questão, respeitem as restrições de uso aqui determinadas.

2.2. Forma de Atendimento

- 2.2.1. A descrição da forma de atendimento dos serviços previstos neste Termo de Referência está brevemente descrita nos itens abaixo e detalhadamente no ANEXO I-A – Forma de Execução e Fiscalização do Contrato.

2.2.2. Suporte Técnico

- 2.2.2.1. Os serviços de suporte técnico são referentes a prestação de serviços visando à reparação de eventuais falhas ou inconsistências detectadas nos componentes da solução (quer sejam produtos de hardware e/ou software e/ou serviços), de forma a garantir o pleno, correto e seguro funcionamento da solução e seus módulos ou componentes e suas integrações com o ambiente CAIXA, assim como na prestação de informações necessárias ao esclarecimento de dúvidas sobre o funcionamento da solução e dos seus módulos e/ou componentes, promovendo sua perfeita operacionalização. Os detalhes e os serviços inicialmente previstos estão disponíveis no ANEXO I-A – Forma de Execução e Fiscalização do Contrato.

2.2.3. Prazos de Atendimento e Resolução de Chamados e cálculo de multas por atraso

- 2.2.3.1. Um Nível Mínimo de Serviço objetivo e mensurável deve ser estabelecido, com a finalidade de aferir e avaliar a qualidade dos serviços contratados.
- 2.2.3.2. Para mensurar esses fatores serão utilizados indicadores de desempenho relacionados com a natureza e característica dos serviços contratados, para os quais foram estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA e que estão descritas no ANEXO I-C – Níveis de Serviço, Indicadores e Penalidades.

2.2.4. Transferência de Conhecimento

- 2.2.4.1. Consiste na transmissão de conhecimento técnico aos empregados CAIXA das funcionalidades da Solução e de seus componentes, de sua configuração, otimização, utilização e funcionamento, no momento da implantação, além de complementações quando ocorrerem alterações nos modos operacionais dos seus componentes ou, ainda, por solicitação da CAIXA,

visando aprimorar os conhecimentos da tecnologia utilizada e maximizar sua utilização conforme previsto no ANEXO I-A – Forma de Execução e Fiscalização do Contrato.

2.2.5. Atualização tecnológica

- 2.2.5.1. Consiste na atualização de versões da plataforma e seus componentes, sejam por motivos de evolução funcional, tecnológica ou correção de eventuais falhas ou erros.
- 2.2.5.2. A atualização Tecnológica a ser prestada pela CONTRATADA dar-se-á durante toda a vigência do contrato, contados a partir da entrega, instalação, testes e da emissão do Termo de Aceite da Solução pela CAIXA.
- 2.2.5.3. Na atualização de versões, a CONTRATADA deverá garantir o apoio técnico necessário para a CAIXA instalar/configurar com sucesso as últimas versões para o qual foram licenciados em seu ambiente de homologação e posteriormente em seu ambiente de produção, sem ônus adicional para a CAIXA.
- 2.2.5.4. O fornecimento de nova versão não deverá inviabilizar os demais módulos e transações da Solução.
- 2.2.5.5. A CONTRATADA deverá garantir que a Caixa tenha o acesso a todas as atualizações da solução observando que eventuais serviços sob customização, solicitados pela Caixa, não venham a impedir o correto funcionamento da solução frente às versões atualizadas do produto que forem distribuídas aos demais clientes da solução.

2.2.6. Vigência do Contrato

- 2.2.6.1. O período de vigência do contrato é de 24 (vinte e quatro) meses, podendo ser renovado até o limite permitido na legislação, conforme detalhado no ANEXO I-A - Forma de Execução e Fiscalização do Contrato.

2.2.7. Local da prestação dos Serviços

- 2.2.7.1. Os locais da prestação de serviço, quando presenciais, estão descritos no ANEXO I-A - Forma de Execução e Fiscalização do Contrato.

2.2.8. Forma de Pagamento

- 2.2.8.1. A forma de pagamento ocorrerá conforme disposto no contrato - Cláusula Forma de Pagamento e no ANEXO I-A – Forma de Execução e Fiscalização do Contrato.

2.2.9. Responsável pelo Acompanhamento Contratual

- 2.2.9.1. A CAIXA indicará, formalmente, no ato da assinatura do Contrato as pessoas responsáveis pela sua supervisão formal e operacional do contrato, a unidade gestora operacional e unidade gestora formal do Contrato, conforme descrito no ANEXO I-A - Forma de Execução e Fiscalização do Contrato.

2.2.10. Obrigações da Contratada

- 2.2.10.1. Responsabilidades da CONTRATADA por eventuais prejuízos decorrentes do descumprimento de qualquer condição estabelecida neste Termo de Referência.

2.2.10.2. Também são responsabilidades da CONTRATADA a manutenção e atualização do corpo técnico em relação às tecnologias, normas, padrões, processos, procedimentos e metodologias utilizados na prestação do serviço.

2.2.10.3. Todos os detalhes estão descritos no ANEXO I-C – Níveis de Serviço, Indicadores e Penalidades.

2.2.11. Sanções Administrativas

2.2.11.1. Trata das glosas, multas e penalizações pelo descumprimento ou prestação do serviço com qualidade abaixo do esperado, disponíveis no ANEXO I-C – Níveis de Serviço, Indicadores e Penalidades.

2.2.11.2. Os indicadores de nível de serviço servirão de base para aferição da qualidade dos serviços prestados e consequente cobrança de possíveis glosas/multas apuradas conforme detalhamento previsto no ANEXO I-C – Níveis de Serviço, Indicadores e Penalidades.

2.3. Dos Requisitos Técnicos de Segurança

2.3.1. Deverá comprovar, por meio de certificados, o atendimento aos requisitos descritos no ANEXO I-B – Requisitos de Segurança Tecnológica Para Fornecedores e ANEXO I-H - Requisitos De Segurança Tecnológica Para Fornecedores De Nuvem, e demais requisitos descritos neste item, fornecendo as comprovações quando solicitada pela CAIXA.

2.3.2. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente registrados em cartório de títulos e documentos.

2.4. Requisitos Funcionais e Não Funcionais

2.4.1. Os requisitos constam no ANEXO IX – Requisitos Funcionais e Não Funcionais, **do edital**.

2.5. Disponibilização de solução em nuvem pública

2.5.1. Consiste na disponibilização de Solução integrada de Software as a Service – SaaS, em nuvem pública, de todos os componentes necessários à operação do sistema, doravante denominada Solução, observando os requisitos funcionais e não funcionais descritos neste documento e seus anexos.

2.5.2. A Solução deverá estar disponível para funcionamento de segunda à sexta, em horário comercial (das 8hs às 17hs).

2.5.3. O período de disponibilidade total da Solução deve ser de 99,5% (noventa e nove e meio por cento) ou superior, do total de minutos/mês.

2.6. Deve ter capacidade para atender os volumes especificados neste TR.

2.6.1. A Solução deverá ser implementada em alta disponibilidade local e global.

2.6.1.1. Alta disponibilidade local é a duplicação da instalação de uma Solução em uma mesma zona de disponibilidade da infraestrutura provedora de nuvem de maneira que, na queda de metade de uma Solução local, a outra metade suporte toda a operação da Solução.

2.6.1.2. Alta disponibilidade global é a alta disponibilidade implementada em zonas de disponibilidade distintas da provedora de nuvem, de maneira que, caso uma das zonas de disponibilidade fique indisponível, a outra instalação assuma plenamente a operação de ambas.

- 2.6.2. A Solução deve prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis.
- 2.6.3. A Plataforma deve ser instalada e configurada em nuvem pública, em regime de Software as a Service (SaaS), fornecida pela empresa fornecedora da Solução.
- 2.6.4. A Solução deve implementar o uso de Link Dedicado nas integrações entre os componentes de cada Solução na nuvem e os serviços expostos pela CAIXA na internet;
- 2.6.5. O provimento da Link Dedicado é de responsabilidade da CONTRATADA.
- 2.6.6. A Solução deve seguir todas as orientações da NC14/IN01/DSIC/SCS/GSIPR, homologada por meio da Portaria nº 9, de 15 de março de 2018.
- 2.6.7. Adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações que serão tratadas em sua infraestrutura.
- 2.6.8. A camada de dados da aplicação não pode ser compartilhada com outros clientes do provedor de serviços.
- 2.6.9. O provedor deve garantir e demonstrar, quando solicitado, isolamento de recursos e de dados de seus clientes.
- 2.6.10. A Solução deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato, inclusive em situações de backup, contingência ou recuperação de desastres.
- 2.6.11. A empresa fornecedora da Solução pode prover serviços em nuvem, fora do território nacional desde que aderente à resolução CMN nº 4658 de 26/ABR/2018; neste caso, é preciso ser em países com convênio para troca de informações entre o Banco Central do Brasil com as autoridades supervisoras dos países onde os serviços poderão ser prestados.
- 2.6.12. No caso de inexistência de convênio entre os países, o Banco Central do Brasil deve autorizar a contratação, observados o prazo e as informações requeridas na resolução CMN nº 4752 de 26/NOV/2019.
- 2.6.13. Os direitos de propriedade sobre os dados enviados pela CAIXA à nuvem permanecem exclusivamente de propriedade da CAIXA, não sendo transferida para o custodiante (provedor/fornecedor do serviço).
- 2.6.14. Informações sobre Requisitos de Segurança Tecnológica para Serviços de Nuvem Pública estão descritos no Anexo I-H Requisitos de Segurança para Serviços em Nuvem.
- 2.7. Segurança da informação**
- 2.7.1. É vedado o tratamento em ambiente de nuvem de informações não autorizadas pela CAIXA.
- 2.7.2. Entende-se como Tenant, clientes em ambiente de multilocação.
- 2.7.3. Ambiente de multilocação corresponde a uma conta de cliente para usar um recurso, solução e / ou serviço de nuvem pública.

- 2.7.4. Os dados de cada cliente devem permanecer isolados e invisíveis para outros clientes, conforme os conceitos de Tenant acima.
- 2.7.5. A fornecedora da solução deverá dispor de análise e gestão de riscos de segurança de informação, conforme dispõe a Norma Complementar 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013.
 - 2.7.5.1. 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.
- 2.7.6. A fornecedora da solução deverá dispor de solução de gerenciamento e replicação de backup.
- 2.7.7. Deverá dispor de mecanismos para realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) podendo a CAIXA realizar auditorias, inclusive com apoio de terceira parte, para comprovar que a empresa mantém esse requisito.
- 2.7.8. Os testes de segurança da informação, conforme mencionado no item anterior, serão realizados a cada 12 (doze) meses e devem gerar relatório de vulnerabilidade e formas de mitigação dessas.
 - 2.7.8.1. Caso solicitado, o relatório deverá ser apresentado a CAIXA.
- 2.7.9. A Solução deverá dispor de mecanismo de acesso protegido aos dados, por meio de chave de criptografia, garantindo que apenas aplicações e usuários autorizados tenham acesso.
- 2.7.10. A Solução deverá dispor de recursos que garantam a segurança da informação dos dados da CAIXA, incluindo os seguintes itens:
 - 2.7.10.1. Solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações);
 - 2.7.10.2. Solução de prevenção e detecção de intrusão (IPS);
 - 2.7.10.3. Solução anti-DDoS, os quais deverão ser validados via documental ou certificações.
- 2.7.11. A Solução deve ser capaz de se integrar com o Cloud Access Security Broker (CASB) Microsoft, atualmente utilizado pela CAIXA, para impor políticas de segurança, conformidade e governança de aplicativos em nuvem.
- 2.7.12. Deve possuir soluções de Identity as a Service (IDaaS) que atendam aos seguintes requisitos:
 - 2.7.12.1. Ser compatível com os protocolos SAML, WS-Federation e OpenID.
- 2.7.13. A Solução deve suportar integrações com as soluções de autenticação e autorização previstas na regulação do Open Banking, e com as soluções de autenticação, autorização e SSO (Single-Sign-On) em uso na CAIXA conforme descrito no Anexo I-B utilizando os principais protocolos de segurança em uso no mercado: OAuth, OIDC, SAML.
- 2.7.14. Oferecer funcionalidade de autenticação multi-fator (Multi-factor Authentication).PARA FORNECEDOR
- 2.7.15. Oferecer gerenciamento de acesso através de APIs baseadas no protocolo OAuth 2.0.

- 2.7.16. A solução deverá dispor de sistema de hardware e dados para missão crítica com política de “Disaster Recovery”, balanceamento, conectividade e backup/restore durante toda a vigência do contrato.
- 2.7.17. A CAIXA, a qualquer tempo, poderá solicitar a realização de simulação de portabilidade das aplicações hospedadas na Nuvem para a rede interna da CAIXA e este serviço será contratado através de USTs previstos neste Edital, em prazo acordado entre as partes.

2.8. CONDIÇÕES GERAIS

- 2.8.1. Durante o contrato, caso a CONTRATADA identifique a necessidade de substituição de algum componente da Solução ofertada, essa deverá ser mantida em pleno funcionamento até a sua completa substituição.
- 2.8.2. Todos os custos para prestação dos serviços contratados são de responsabilidade da CONTRATADA.

ANEXO I-A**FORMA DE EXECUÇÃO E FISCALIZAÇÃO DO CONTRATO****1. CONDIÇÕES GERAIS**

- 1.1. As atividades para implementação e ativação da solução tecnológica que operacionalize os serviços de controle de enquadramento dos fundos de investimento e carteiras deverão iniciar mediante solicitação da CONTRATANTE, conforme etapas descritas neste documento, e compreendem todas as atividades necessárias à sua disponibilização, as integrações e customizações iniciais, as parametrizações, e demais atividades necessárias ao pleno funcionamento da Solução.
- 1.1.1. As integrações e customizações iniciais são aquelas para o uso inicial da Solução consistindo na criação e implementação de interfaces com a CONTRATANTE e parceiros, bem como as customizações para atendimento ao escopo definido para a fase de ativação descrita neste documento.
- 1.1.2. As integrações com os sistemas da CAIXA deverão seguir os padrões citados no ANEXO I-J - INTEGRAÇÕES PREVISTAS NA IMPLANTAÇÃO DA SOLUÇÃO.
- 1.1.3. A Solução ofertada deverá ser a mesma daquela analisada na fase de qualificação técnica do certame, não sendo admitidas alterações dos produtos previamente avaliados pela CONTRATANTE.
- 1.1.4. Para execução do contrato será adotado o modelo de trabalho baseado no conceito de delegação de responsabilidade, que define a CAIXA como responsável pela gestão do contrato e pelo ateste da aderência aos padrões de qualidade exigidos dos serviços entregues, e a CONTRATADA como responsável pela execução operacional dos serviços, gestão de recursos humanos, de infraestrutura de hardware e software necessários para atendimento do contrato.
- 1.1.5. Caberá à CONTRATADA dimensionar corretamente suas equipes de forma a cobrir todos os turnos de trabalho de acordo com o respectivo volume de demandas/atendimentos, mantendo a qualidade e os níveis de serviço exigidos em quaisquer datas/horários, bem como os clientes, usuários e parceiros assistidos sobre todos os aspectos.
- 1.1.6. Para execução dos serviços, a CONTRATADA deverá disponibilizar equipe técnica plenamente capacitada para executar as atividades dentro dos prazos previstos.
- 1.1.7. Caberá a CONTRATADA dimensionar a estrutura necessária, o perfil e a qualificação dos seus profissionais, com vistas a atender as necessidades da CAIXA, tendo como base as características, a especificidade dos serviços e as atividades a serem executadas.
- 1.1.8. Os profissionais da CONTRATADA exercerão suas atribuições sob gestão direta e exclusiva dos PREPOSTOS da CONTRATADA.
- 1.1.9. A CONTRATADA se obriga a manter PREPOSTOS nos locais onde serão executados os serviços, para o atendimento imediato das solicitações, com a responsabilidade pelo pleno gerenciamento e execução dos serviços, pelo controle das entregas no prazo definido e pela distribuição das tarefas entre as equipes.
- 1.1.10. O PREPOSTO será o principal responsável por fazer a ligação entre a CONTRATADA e a CAIXA e deve ser apresentado na data de assunção dos Serviços.

- 1.1.11. Todas as demandas serão solicitadas pela CAIXA à CONTRATADA por ferramenta de gestão da CAIXA e/ou outro recurso que venha a ser definido, contendo informações necessárias para sua realização.
- 1.1.12. A execução dos serviços será gerenciada pela CONTRATADA, que fará o acompanhamento da qualidade e dos níveis mínimos de serviços alcançados com vistas a efetuar eventuais ajustes e correções de rumo.
- 1.1.13. A CAIXA também deverá fiscalizar a execução dos serviços prestados, atendo-se fielmente aos parâmetros de qualidade e respectivos níveis de serviço especificados no edital.
- 1.1.14. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviços acordados devem ser imediatamente comunicados à CAIXA.
- 1.1.15. A cada solicitação dos serviços, a CONTRATADA deverá avaliar se as informações constantes são suficientes para a execução das atividades solicitadas, caso as informações não sejam suficientes, a CONTRATADA deverá solicitar as complementações pertinentes.
- 1.1.16. Qualquer inviabilidade detectada no atendimento da demanda deverá ser comunicada formalmente à CAIXA, por meio da ferramenta de gerenciamento de demandas ou pelo mesmo meio recebido com o registro do resultado da avaliação, descrição da inviabilidade encontrada e sugestão para retificações.
- 1.1.17. Caso a CAIXA julgue improcedente a manifestação/comunicação da CONTRATADA quanto à inviabilidade no atendimento, permanecerá o prazo inicial definido.
- 1.1.18. Para efeito de aceitação pela CAIXA dos serviços prestados pela CONTRATADA, serão considerados realizados e atendidos aqueles serviços entregues que estiverem em conformidade com as especificações e com o CONTRATO.
- 1.1.19. A conformidade da execução das atividades visa verificar de forma inequívoca a integridade, correteza, completeza, sequência, prazo, tempestividade e geração de produto.
- 1.1.20. Eventuais atrasos em atividades que estejam sob responsabilidade da CAIXA, não serão imputados à CONTRATADA.
- 1.2. A CONTRATADA deverá manter ao longo do contrato todas as condições que garantiram sua habilitação e qualificação no processo licitatório.
- 1.3. Nenhuma regra, condição ou referência externa ao contrato será considerada para regular a sua execução, valendo, para tanto, os estritos termos transcritos no contrato e seus anexos, inclusive neste instrumento.
- 1.4. A CONTRATADA deverá garantir a atualização tecnológica da solução durante o período de vigência do contrato. No caso de descontinuidade da solução a CONTRATADA deve avisar previamente a CAIXA e substituir a solução por outra que atenda aos processos de negócios em uso e sem ônus para a CONTRATANTE.
- 1.5. A Solução deverá adequar-se a todo e qualquer requisito já definido ou que venha a ser definido pelos Órgãos Reguladores e/ou convenção celebrada pelas instituições participantes do Sistema Financeiro Nacional, sem custo adicional à CONTRATANTE, durante toda a vigência do contrato.
- 1.5.1. Neste caso, o prazo para conclusão da adequação da Solução corresponderá ao prazo limite definido pelo Órgão Regulador Externo.

- 1.6. A CONTRATADA deverá providenciar a documentação completa e suficiente, sempre que solicitado, para validação do modelo/metodologia junto à área responsável da CAIXA.
- 1.7. Todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados, deverá ser disponibilizado pela CONTRATADA à CONTRATANTE ou empresa por ela designada durante a execução do contrato.
- 1.8. Durante a vigência do contrato, caso a CONTRATADA identifique a necessidade de substituição de algum componente subcontratado, a Solução deverá ser mantida em pleno funcionamento até a sua completa migração.
- 1.8.1. Neste caso, todos os dados, configurações e jornadas construídas ao longo do contrato deverão ser passíveis de migração entre fornecedores, devendo, ainda, a CONTRATADA disponibilizar equipe para providenciar junto à CONTRATANTE e eventual novo fornecedor, plano e operação assistida na efetiva migração.
- 1.9. A CONTRATADA deverá participar, sempre que solicitado pela CONTRATANTE, de pesquisa para avaliação de desempenho da execução contratual, que poderá ser realizada, a critério da CAIXA, no decorrer da vigência contratual, podendo abordar aspectos tais como:
- Qualidade dos produtos/serviços;
 - Qualificação dos profissionais;
 - Execução das atribuições do gerente e/ou preposto do contrato;
 - Aspectos de negociação;
 - Cumprimento de ações de melhorias;
 - Satisfação geral;
 - Outros aspectos relativos à execução do contrato.
- 1.9.1. Havendo a avaliação de desempenho, a CAIXA informará o conceito obtido pela Contratada e poderá indicar a necessidade de apresentação de Plano de Melhoria pela Contratada, caso ela obtenha avaliação inferior ao limite definido pela CAIXA e previamente informado à Contratada.
- 1.9.2. O Plano de Melhoria, a ser homologado pela CAIXA, deve propor ações objetivas e com prazos determinados, com vistas a elevar o desempenho da Contratada.
- 1.9.3. Quando definida a necessidade de apresentação do Plano de Melhoria, o não atendimento no prazo estabelecido pela CAIXA sujeitará a Contratada às sanções previstas no Contrato.
- 1.10. A CONTRATADA deverá estar disponível para reuniões sempre que a CONTRATANTE requisitar.
- 1.11. Todos os custos referentes ao fornecimento da Solução e à prestação dos serviços contratados serão de responsabilidade exclusiva da CONTRATADA.

2. VIGÊNCIA DO CONTRATO

- 2.1. O presente contrato terá a duração de 24 (vinte e quatro) meses, a contar da assinatura, podendo ser prorrogado por sucessivos períodos nos limites definidos na Lei nº. 13.303/2016.

3. LOCAL DE ENTREGA/EXECUÇÃO DOS SERVIÇOS

- 3.1. As atividades que exigirem atuação in-loco da CONTRATADA deverão ser realizadas em unidades da CONTRATANTE em Rio de Janeiro/RJ, São Paulo/SP e Brasília/DF ou em outra localidade previamente comunicada no decorrer do contrato.

UF	Endereços dos prédios administrativos CAIXA
RJ	Rua do Passeio, 38/40 – Centro - Rio de Janeiro/RJ - CEP: 20021-290.
SP	Av. Dr. Martin Luther King, 762, Jd. Umuarama, Osasco-SP, CEP: 06030-900. Av. Guido Caloi, 1000, Jd. São Luís, São Paulo – SP – CEP 05802-140. Largo da Concórdia, 211, Brás, São Paulo – SP – CEP 03012-010. Av. Paulista, 750, São Paulo – SP – CEP 01310-100.
DF	CTC: SIG – Quadra 01 – Lote 685/705 - Setor de Indústrias Gráficas – Brasília - DF DTC: Parque Tecnológico Capital Digital Lote 3, S/N - Granja do Torto – Brasília – DF Matriz I – Setor Bancário Sul, Q. 4, LT 3/4, Asa Sul, Brasília – DF - CEP 70070-140 Matriz II - Setor de Autarquias Sul, Q. 3 - Asa Sul, Brasília – DF - CEP 70297-400 Matriz III – Setor Bancário Sul, Q. 1, BLC L – Asa Sul, Brasília – DF – CEP 70070-110 Matriz IV - SEPN 512 CJT C LOTE 9/10 – Asa Norte, Brasília – DF – CEP 70760- 500

4. **SETUP E SUSTENTAÇÃO**

- 4.1. Consiste em executar as atividades necessárias para implementação e sustentação da Solução, no modelo *Software as Service* (SaaS), de seus módulos e componentes, resultando em seu pleno funcionamento, de acordo com os requisitos e volumetria estabelecidos no Termo de Referência e seus anexos, incluindo a transferência de conhecimento às equipes da CONTRATANTE.
- 4.2. Contempla todas as ações necessárias para ativação, integração, parametrização e disponibilização da Solução atendendo integralmente os requisitos definidos no Termo de Referência e seus anexos
- 4.3. A ativação da plataforma deverá contemplar também a disponibilização dos requisitos funcionais e não funcionais descritos no Anexo IX – REQUISITOS FUNCIONAIS E NÃO FUNCIONAIS.
- 4.4. O *setup* terá duração máxima de 90 dias corridos, devendo a CONTRATADA se programar para atendimento nesse prazo.
- 4.5. As etapas do *setup*, descritas a seguir, poderão ser revistas e/ou alteradas pela CONTRATANTE, durante o planejamento da implementação, de forma a refletir as necessidades, detalhes e particularidades da Solução.
- 4.6. A CONTRATADA deverá apresentar relatório do Fabricante comprovando a ativação das licenças em conformidade com o período de vigência do contrato, como condição do aceite do licenciamento da Solução pela CAIXA.
- 4.7. **Etapas 1: Planejamento - Elaboração do plano de ativação da Solução**

- 4.7.1. Consiste em disponibilizar à CONTRATANTE um plano de ativação da Solução que deverá detalhar todas as ações, atividades, entregas e serviços necessários para o atendimento integral aos requisitos funcionais e técnicos definidos no Termo de Referência e seus anexos, bem como à volumetria estabelecida, incluindo as etapas de levantamento de necessidades de integrações iniciais, customizações e jornadas.
- 4.7.2. A CONTRATADA deverá acionar a CONTRATANTE para obter as informações que sejam necessárias para elaboração do plano de ativação.
- 4.7.3. Em até 30 dias corridos a partir da solicitação da CAIXA a CONTRATADA deverá elaborar e entregar à CONTRATANTE o **plano de ativação** devendo estar aderentes aos marcos de entrega definidos neste documento.
- 4.7.3.1. A CONTRATADA deverá neste período apresentar as funcionalidades nativas da Solução.
- 4.7.3.2. O **plano de ativação** deverá conter a descrição formal e detalhada das atividades (inclusive aquelas relacionadas às integrações iniciais necessárias à ativação da solução), recursos envolvidos e prazos para execução das atividades.
- 4.7.3.3. O **plano de ativação** deverá ser elaborado pela CONTRATADA e entregue para a equipe de projeto da CAIXA, sendo responsabilidade da CONTRATADA agendar reuniões com a equipe da CAIXA para obter as informações necessárias para elaboração do documento, bem como promover quaisquer ajustes ou adequações que lhe forem solicitadas. Este documento será submetido à aprovação da CAIXA.
- 4.7.3.4. Caso se verifique algum fato novo, não previsto por ocasião da elaboração original do **plano de ativação**, e que justifique a sua revisão, este poderá ser alterado por acordo entre as partes.
- 4.7.4. A etapa será considerada concluída após aprovação e ateste do plano de ativação pela CONTRATANTE ou por profissional por ela contratado para este fim.
- 4.8. **Etapas 2: Execução do plano de ativação da Solução**
- 4.8.1. A execução dessa fase considera o plano de trabalho aprovado na Etapa 1, que contém cronograma com a programação detalhada de todas as atividades a serem desenvolvidas pela CONTRATADA para consecução dos serviços descritos, que deve considerar todos os módulos, estudo e execução de integrações, análise e documentação dos processos de negócio, configuração, parametrização da solução, homologação, migração de bases legadas, implantação e transferência de conhecimento para a equipe que fará a operacionalização dos processos implantados na solução.
- 4.8.2. Disponibilização dos componentes configurados na solução e disponível em ambiente de homologação para a equipe responsável realizar os testes e homologação da solução. Todos os requisitos devem estar presentes, assim como os processos de negócio com a documentação das funções definidas, podendo para isso, inclusive, utilizar a ferramenta de modelagem de processos da CAIXA. Essa documentação servirá de base para a configuração, implementação, testes e transferência de conhecimento.
- 4.8.3. Eventuais soluções complementares, correções e/ou adequações da plataforma realizadas durante esta fase não terão custos adicionais para a CAIXA e serão de responsabilidade da CONTRATADA.
- 4.8.4. A CONTRATADA disponibilizará quantidade de profissionais suficientes e capacitados para realizar as customizações e parametrizações nos aplicativos para que estes possam atender as necessidades CAIXA.

- 4.8.5. Nesta Fase a CONTRATADA deverá executar o piloto no ambiente de produção para que os usuários finais possam utilizar e validar a Solução com todos os requisitos necessários em funcionamento.
- 4.8.6. Dentro do prazo estabelecido para esta fase, caberá à CONTRATADA formalizar a sua finalização à CAIXA, por meio de um relatório de conclusão detalhado, evidenciando o atendimento desta fase e consequentemente a entrega da solução.
- 4.8.7. O documento de Ateste de verificação será produzido pela CONTRATADA, e emitido para a aprovação dessa fase pela CAIXA.
- 4.8.8. O Prazo limite para conclusão da Etapa 2 é de até 60 (sessenta) dias corridos contados a partir da conclusão da Etapa 1, podendo ser prorrogado a critério e/ou necessidade da CAIXA.
- 4.8.9. Caberá à CAIXA determinar, com a devida antecedência, a melhor data para a Implantação da solução em produção, considerando, por exemplo, as datas críticas de fechamentos mensais ou trimestrais.
- 4.9. **Etapa 3: Sustentação da Solução**
- 4.9.1. Consiste em prestar todo e qualquer serviço necessário para manter a Solução em produção e perfeito funcionamento, incluindo a manutenção dos módulos e o suporte funcional da ferramenta, de forma a preservar a utilização plena da Solução.
- 4.9.2. Consiste ainda em reparar falhas, erros e inconsistências, solucionar incidentes em definitivo, aplicando solução de contorno quando necessário, analisar, detalhar e solucionar problemas, monitorar, prestar suporte durante testes e validação de novas versões e atualizar a solução.
- 4.9.3. Os serviços deverão ser prestados em português do Brasil e, caso seja necessário suporte em idioma diferente, a CONTRATADA deve disponibilizar técnico para intermediar a comunicação.
- 4.9.4. Os manuais da Solução também devem ser atualizados com informações que assegurem a plena utilização dos serviços sem custo adicional para a CONTRATANTE.
- 4.9.4.1. Nos casos em que houver atualização e/ou inovação metodológica nos processos da Solução, inclusive para atendimento de alterações na legislação, a CONTRATADA deverá atualizar a versão do manual da Solução e prestar esclarecimentos necessários caso haja necessidade de nova validação interna.
- 4.9.5. Toda e qualquer intervenção realizada pelas equipes da CONTRATADA e que possa causar indisponibilidade da Solução, mesmo que parcial, deve ser executada somente mediante prévia notificação à CONTRATANTE, contendo informações claras dos procedimentos que serão adotados/executados pela CONTRATADA.
- 4.9.6. A CONTRATADA deverá disponibilizar acesso nos ambientes de operação da Solução para a CONTRATANTE portanto o acesso aos ambientes deverá se dar de forma compartilhada.
- 4.9.7. A CONTRATADA deverá dispor de recursos para monitoramento de disponibilidade e desempenho da solução, que deverá funcionar de segunda à sexta, em horário comercial (das 8hs às 17hs) bem como ser capaz de gerar indicadores relacionados à disponibilidade, desempenho e atendimento aos níveis de serviço acordados, bem como comunicar um alerta quando a Solução estiver indisponível, ainda que parcialmente.
- 4.9.8. **O serviço de sustentação compreende:**
- **Manter a Solução**

- **Suporte funcional da ferramenta.**

4.9.9. Manter a Solução

- 4.9.9.1. Consiste na execução das atividades necessárias para garantir o pleno funcionamento da Solução, incluindo operação, monitoração, manutenção, correção, atualização e evolução necessárias para seu correto funcionamento.
- 4.9.9.2. Inclui a prestação de assistência especializada aos técnicos da CONTRATANTE, orientando-os quanto ao planejamento, homologação de processos, produção, monitoração, segurança da informação, identificação e correção de problemas e incidentes, execução de eventuais alterações nas rotinas da Solução, correção e atualização tecnológica.
- 4.9.9.3. Deverá ser prestado remotamente de segunda à sexta, em horário comercial (das 9hs às 17hs) por especialistas da CONTRATADA com notório conhecimento da Solução e serviços ofertados.
- 4.9.9.4. A CONTRATADA deverá, em conjunto com os técnicos da CONTRATANTE:
- a) Orientar e atuar no planejamento e análise do processamento da Solução;
 - b) Orientar e monitorar a qualidade e níveis de serviços com vistas a propor eventuais ajustes e correções;
 - c) Orientar e resolver problemas ocorridos na Solução;
 - d) Orientar e realizar a monitoração da Solução e ambiente de produção, garantindo o atendimento dos níveis mínimos de serviço;
 - e) Orientar e comunicar imediatamente à CONTRATANTE os incidentes identificados;
 - f) Orientar e realizar a manutenção de rotinas de apoio aos processos em produção da Solução;
 - g) Orientar e realizar a atualização dos processos de automatização de rotinas;
 - h) Orientar e realizar a atualização das rotinas de produção da Solução, mantendo a documentação atualizada;
 - i) Orientar e realizar as atualizações das rotinas de recuperação, reinício de processos, fluxos produtivos e rotinas eventuais, mantendo a documentação atualizada;
 - j) Orientar e realizar a atualização das rotinas de *backup* e *recovery* de catálogos, bases de dados, tabelas, arquivos, programas e demais informações da Solução, nos ambientes de produção, testes e desenvolvimento, mantendo a documentação atualizada;
 - k) Propor e executar medidas para correção de quaisquer incidentes/problemas ou deficiências observadas na produção da Solução;
 - l) Orientar, elaborar e analisar os relatórios de desempenho da Solução, com emissão de pareceres;
 - m) Orientar e executar a instalação de atualizações e correções da Solução;
 - n) Orientar e realizar o diagnóstico de problemas e ocorrências diárias da Solução;
 - o) Orientar, executar e acompanhar as tarefas de suporte;

- p) Sugerir e implantar procedimentos para a Solução a fim de identificar problemas, analisar desempenho ou planejar capacidade;
- q) Orientar, planejar e executar os testes de rotinas da Solução;
- r) Prestar apoio e atendimento às equipes técnicas da CONTRATANTE;
- s) Arcar com todos os custos e despesas com seus técnicos oriundos do deslocamento, passagens, estadia, alimentação, horas técnicas e outras despesas diretas e indiretas, pelo período necessário para o atendimento de serviços de sustentação, com objetivo de detectar/solucionar problemas em ambiente de produção.
- t) Manter equipe de técnicos com conhecimentos específicos e capacitados a assistir aos técnicos da CONTRATANTE quanto ao planejamento das rotinas de produção da Solução.
- u) Elaborar os relatórios relacionados na tabela a seguir, contendo a descrição da resolução das ocorrências:

RELATÓRIO	CONTEÚDO	PRAZO DE ENTREGA
Relatório de ocorrências	Informações técnico/gerenciais, descrevendo a ocorrência e as providências adotadas ou a serem adotadas para a regularização, incluindo ações paliativas, se for o caso, e definitivas.	Até 02 (duas) horas a partir da identificação inicial da ocorrência, com atualizações a cada hora, até a solução da ocorrência. No dia subsequente à solução definitiva, deverá ser apresentado relatório final, consolidado e revisado.
Relatório semanal	Informações técnico/gerenciais sobre a execução dos serviços e resumo das ocorrências e providências adotadas, bem como com as orientações definidas para o serviço de sustentação, detalhando as ocorrências diárias da semana, incluindo as mudanças.	Semanalmente, às segundas-feiras, contendo as informações referentes à semana anterior (de segunda-feira a domingo).
Relatório mensal	Informações técnico/gerenciais consolidadas sobre a execução dos serviços, resumo das ocorrências, tempo de resposta das transações, quantidade de usuários simultâneos versus tempo de resposta, contendo gráficos e estatísticas, análises e orientações.	Deverá ser entregue à CAIXA, até o dia 05 (cinco) do mês subsequente à prestação do serviço de sustentação.

4.9.9.5. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviços acordados devem ser imediata e formalmente comunicados à CONTRATANTE.

4.9.10. **Serviço de Suporte Funcional da Ferramenta**

4.9.10.1. O serviço de suporte funcional da ferramenta consiste no atendimento aos chamados abertos pelos usuários da CONTRATANTE para reparação de falhas e/ou inconsistências detectadas, inclusive nas suas configurações, parametrizações, integrações e customizações, também se aplicam na prestação de informações necessárias ao esclarecimento de dúvidas, tratamento de problemas, de forma a garantir o pleno, correto e seguro funcionamento e utilização da Solução e dos seus módulos e componentes.

4.9.10.2. O público-alvo do serviço de suporte funcional da ferramenta é de, aproximadamente, 10 usuários.

4.9.10.3. Será prestado remotamente, quando possível, e presencialmente, sempre que se fizer necessário, conforme prazos e horários de atendimento estabelecidos.

4.9.10.4. A definição da necessidade de prestação de serviço presencial caberá à CONTRATANTE em conjunto com a CONTRATADA e será adotado nos casos em que a presença física for necessária para viabilizar determinado atendimento.

4.9.10.5. A CONTRATADA deverá disponibilizar central de atendimento (HELP DESK) para abertura e acompanhamento dos chamados de suporte funcional da ferramenta de segunda à sexta, em horário comercial (das 8hs às 17hs).

4.9.10.6. Todos os prazos para atendimento dos serviços de sustentação começarão a ser contados de forma corrida a partir da abertura do chamado, inclusive, independentemente da forma de acionamento.

4.9.10.7. O termo “forma corrida” indica que a contagem de tempo se dará de maneira contínua sem interrupções, exceto aquelas que sejam provocadas pela CAIXA. Os níveis de serviço descritos abaixo devem ser cumpridos no atendimento dos chamados abertos junto ao suporte técnico remoto (HELP DESK):

Tipo do chamado	Criticidade	Período de atendimento	Tempo máximo para início do atendimento	Tempo máximo de solução paliativa	Tempo máximo de solução definitiva
Suporte funcional da ferramenta	Severidade 1	Dias úteis das 08h00 às 17h00	30 min	2 horas	12 horas
	Solução está parada ou fora de funcionamento e não há meios de contornar a falha. Número significativo de usuários foi afetado ou impacto operacional significativo foi causado.				
	Severidade 2	Dias úteis das 08h00 às 17h00	40 min	3 horas	24 horas
	Solução está apresentando falhas de funcionamento, sem causar interrupção do serviço, mas afetando significativamente seu desempenho. Impacto crítico aos usuários.				

	Severidade 3				
	Solução está parada ou fora de funcionamento. O problema pode ser contornado. Impactos operacionais moderados a pequenos. Impacto moderado aos usuários.				
	Severidade 4	Dias úteis das 08h00 às 17h00	02 horas	6 horas	36 horas
	Consultas técnicas e dúvidas				

- 4.9.10.8. A CONTRATADA deve disponibilizar, sem custo adicional, software para acompanhamento de solicitações de serviço, consultas técnicas, acompanhamento de atendimento remoto e informe relacionado à solução.
- 4.9.10.9. A CONTRATADA deve cumprir os níveis de atendimento da solução acima descritos para as solicitações de serviços em que a CAIXA obrigatoriamente formalizará suas dúvidas, inconsistências, problemas e/ou erros porventura detectados na solução.
- 4.9.10.10. A CAIXA definirá o nível de atendimento do chamado quando da sua abertura junto à CONTRATADA. Os tempos serão contados a partir do registro, por parte da CAIXA, da solicitação de serviços na solução de Help Desk disponibilizada pela CONTRATADA e só serão considerados terminados quando da aceitação da solução pela CAIXA.
- 4.9.10.11. A CONTRATADA se obriga a realizar a administração das solicitações de serviços com profissionais devidamente treinados.
- 4.9.10.12. Será definido um grupo de profissionais da equipe de TI da CAIXA autorizado para abrir chamados de Suporte Remoto junto à CONTRATADA.
- 4.9.10.13. A central de atendimento (HELP DESK) poderá ser acionada por meio de:
- Ligação telefônica gratuita ou local a partir do Rio de Janeiro/RJ, São Paulo/SP ou Brasília/DF;
 - Mensagem de texto via *WhatsApp*;
 - Sítio na Internet;
 - E-mail;
- 4.9.10.14. No momento da abertura do chamado, a CONTRATANTE informará à CONTRATADA, no mínimo, o seguinte:
- Nome do usuário;
 - Unidade do usuário;
 - Contato do usuário (telefone, *e-mail*);
 - Relato do incidente/problema/dúvida;
 - Envio de arquivos anexados com outras informações necessárias para o entendimento do chamado.

- 4.9.10.15. Na abertura do chamado, a CONTRATADA deverá fornecer um número de registro único para acompanhamento de cada chamado, devendo ser o mesmo para acompanhamento por telefone, *WhatsApp*, sítio na Internet e e-mail.
- 4.9.10.16. Caso requisitado pela CONTRATANTE, o sistema de controle de chamados da CONTRATADA deverá enviar e-mail automático comunicando a abertura, alteração e fechamento dos chamados.
- 4.9.10.17. A CONTRATADA deverá atualizar o chamado ao longo do seu atendimento, registrando todas as informações sobre as ações em andamento.
- 4.9.10.18. As informações referentes a chamados, incluindo providências e ações de resolução tomadas, devem ser armazenadas em sistema de controle de chamados da CONTRATADA, cujo acesso deve estar disponível à CONTRATANTE e a CONTRATADA deverá realizar a transferência de conhecimento relacionado.
 - 4.9.10.18.1. Nesse sentido, devem ser criadas contas de acesso para os usuários indicados pela CONTRATANTE, para fins de acompanhamento e auditoria de chamados, sendo possível a extração de relatórios compreendendo o período integral do contrato, permitindo informar intervalos de datas – dia, mês, ano.
 - 4.9.10.18.2. Caso solicitado pela CONTRATANTE, a base de chamados atendidos pela CONTRATADA deve ser disponibilizada por meio de interface, ao final de cada período de referência, para fins de apuração dos índices de chamados e demandas atendidos no prazo.
- 4.9.10.19. Ao final do atendimento do chamado a CONTRATADA realizará, em conjunto com empregados da CONTRATANTE, testes para verificação dos resultados obtidos e ateste da efetividade da solução apresentada.
- 4.9.10.20. Ao término dos testes a CONTRATADA deverá deixar registrado no chamado as causas da ocorrência, as ações realizadas para a resolução, as evidências de teste, o roteiro de teste e o nome do empregado CONTRATANTE que atestou a resolução.
 - 4.9.10.20.1. A CONTRATADA somente realizará o fechamento do chamado após o sucesso nos testes realizados em conjunto com a CONTRATANTE.

5. SERVIÇO DE CUSTOMIZAÇÃO – Sob Demanda

- 5.1. O serviço de customização consiste em qualquer alteração ou complementação no código-fonte da solução, ou desenvolvimento de novos blocos ou módulos completos de código, relativos a novas funcionalidades, relatórios, melhorias, interfaces, integrações, parametrizações e formulários e telas para atendimento de requisitos técnicos e funcionais, bem como na atualização da respectiva documentação.
 - 5.1.1. Com o serviço de customização poderá ser incluído novos elementos, não constantes no Termo de Referência, como requisitos e/ou integrações.
 - 5.1.2. As alterações por meio de customização só devem ser realizadas se mantidas as características originais da Solução e garantidas a continuidade e suporte.
 - 5.1.3. Para a execução do serviço deverá ser observado as complexidades e mensurações de níveis de serviço neste anexo e no Anexo I-J – Integrações Previstas na implantação da solução.
 - 5.1.4. O serviço não poderá ser utilizado para realizar evoluções para se adaptar a legislação mandatória ou demais evoluções previstas no serviço de atualização tecnológica.

- 5.1.5. O serviço de customização ocorrerá sob demanda da CONTRATANTE, durante a vigência do contrato.
- 5.1.6. Excluem-se destes serviços sob demanda, as customizações e integrações iniciais, cuja execução deve ocorrer na etapa de Ativação da solução sem custo adicional para a CONTRATANTE.
- 5.1.7. As demandas de serviço de customização ocorrerão mediante chamado aberto pela CONTRATANTE.
- 5.1.8. Após a abertura do chamado, a CONTRATADA deverá buscar o devido entendimento da demanda e iniciar as ações necessárias para o atendimento.
- 5.1.9. A CONTRATADA deverá apresentar à CONTRATANTE um plano de execução do serviço em até 10 dias úteis a partir da abertura do chamado contendo a relação dos profissionais responsáveis, o escopo, produtos entregues e os prazos para finalização do serviço, observando o prazo máximo estabelecido pela CONTRATANTE.
- 5.1.10. O plano deverá conter, no mínimo, as seguintes informações:
- Descrição detalhada da demanda.
 - Solução proposta pela CONTRATADA para implementação da demanda.
 - Orçamento detalhado dos serviços da CONTRATADA que serão usados para atendimento à demanda.
 - Prazo para entrega da demanda em perfeita operação, testada e documentada, conforme padrões de documentação da Caixa.
 - Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.
- 5.1.11. O plano será submetido à análise da CONTRATANTE e os trabalhos terão início após a aprovação do plano pela CONTRATANTE.
- 5.1.12. A CONTRATADA deverá finalizar o serviço no prazo acordado e o não cumprimento ensejará a aplicação das penalidades previstas no contrato.
- 5.1.13. O atendimento será considerado concluído somente após a homologação da CONTRATANTE, momento em que será atestado seu correto funcionamento e atendimento completo ao chamado.
- 5.1.14. As demandas entregues com baixa qualidade ou defeito que se apresente até 72 horas após implantação serão devolvidas para ajuste e terão prazo de entrega reaberto até a implementação final com o nível de qualidade e requisitos aceitos pela CONTRATANTE.
- 5.1.15. Caberá à CONTRATANTE abonar atrasos não imputáveis a CONTRATADA nas situações em que houver pendências por parte da CONTRATANTE de definições ou insumos necessários ao atendimento da demanda, desde que comprovada a impossibilidade da CONTRATADA em prosseguir com qualquer uma das fases da demanda em voga.
- 5.1.16. Serão considerados para fins de abono somente os casos comunicados formalmente à CONTRATANTE e de forma imediata sempre que identificados pela CONTRATADA, em que a CONTRATANTE, de igual modo, deverá dar aceite formal a situação exposta e renegociar o prazo de atendimento, se assim for devido, mediante justificativa apresentada.

- 5.1.17. Não serão aceitas pela CONTRATANTE como justificativa para abono de atraso e/ou renegociação de prazo, impeditivos que a CONTRATADA apresente como falta de insumo, definições de escopo, especificações que já sejam de conhecimento prévio da CONTRATADA pela execução das atividades de serviço, operação e sustentação, sob sua responsabilidade.

6. TRANSIÇÃO FINAL DO CONTRATO

- 6.1. A transferência de todo conhecimento adquirido ou desenvolvido bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados deverão ser disponibilizados por meio de um Plano de Transição, endereçando todas as atividades necessárias para a completa transição.
- 6.2. A CONTRATADA deverá assegurar portabilidade dos dados e que as informações da CAIXA estejam disponíveis para transição, em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar a transição contratual.
- 6.3. O Plano de Transição deverá ser entregue pela CONTRATADA no prazo de 6 (seis) meses antes do término da vigência do CONTRATO, ou a qualquer tempo, por solicitação da CAIXA, com antecedência mínima de 30 (trinta) dias.
- 6.4. O plano deverá identificar todos os compromissos, projetos, papéis, responsabilidades, artefatos, tarefas, a data início e prazo da transição, bem como todos os envolvidos com a transição, e ter a aprovação formal da CAIXA.
- 6.5. Será de inteira responsabilidade da CONTRATADA a execução do Plano de Transição, bem como a garantia do repasse bem-sucedido de todas as informações necessárias para a continuidade dos serviços pela CAIXA ou empresa por ela designada.
- 6.5.1.1. Todos os dados, configurações e parametrizações construídas ao longo do contrato deverão ser objeto da Transição Final do contrato, sendo passíveis de migração entre fornecedores, devendo, ainda, a CONTRATADA disponibilizar equipe para providenciar junto à CAIXA e eventual novo fornecedor, plano e operação assistida na efetiva migração.
- 6.6. Durante o tempo requerido para desenvolver e executar o Plano de Transição, a CONTRATADA deve responsabilizar-se pelo esforço que necessite dedicar à tarefa de completar a transição, sem custo adicional para a CAIXA.
- 6.7. Todo conhecimento adquirido ou desenvolvido bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados deverão ser disponibilizados à CAIXA ou empresa por ela designada durante a execução do Plano de Transição.

7. FORMA DE PAGAMENTO

- 7.1. A CAIXA, após a aceitação dos serviços e verificação do cumprimento de todas as cláusulas contratuais, efetuará o pagamento à CONTRATADA, mensalmente, no 12º (décimo segundo) dia útil do mês subsequente ao da efetiva prestação dos serviços, mediante crédito em conta corrente mantida pela CONTRATADA, obrigatoriamente, em agência da CAIXA.

MODELO DE CONTRATAÇÃO				
GRUPO	DESCRIÇÃO	QTDE	PREÇO UNITÁRIO	PREÇO TOTAL
GRUPO 1	Ativação da Solução de Controle de Enquadramento dos Fundos de Investimento e Carteiras – Configuração e Integrações iniciais (setup)	1	R\$ XXX	R\$ XXX
	Sustentação (valor fixo mensal)	Até 21 parcelas	R\$ XXX	R\$ XXX
GRUPO 2	Serviços de Customização (sob demanda)	5788 Horas	R\$ XXX	R\$ XXX
	Transferência de conhecimento (sob demanda)	2 Turmas	R\$ XXX	R\$ XXX
VALOR GLOBAL DA CONTRATAÇÃO				R\$ XXX

- 7.2. A ativação da Solução (Setup) de Controle de Enquadramento dos Fundos de Investimento e Carteiras será remunerada, em parcela única, somente após a conclusão da Etapa 2 - Execução do plano de ativação da Solução
- 7.3. Pelo serviço de Sustentação da Solução de Controle de Enquadramento dos Fundos de Investimento e Carteiras, o pagamento será feito mensalmente, em até 21 parcelas mensais, que se iniciarão no mês seguinte ao término do setup da solução (etapa 2).
- 7.3.1. A eventual prorrogação da Etapa 2 implicará na redução proporcional do número de parcelas fixas mensais a serem remuneradas à CONTRATADA, mantendo-se inalterado o valor de cada parcela mensal.
- 7.1. Os serviços de Customização e Transferência de Conhecimento (GRUPO 2) terão o seu pagamento efetuado após o aceite de implantação em produção do serviço desenvolvido. Este volume é estimado sob demanda, ou seja, turmas e horas não utilizadas não serão remuneradas.
- 7.2. Não será permitida a cobrança:
- Retroativa de valores referentes aos serviços de suporte técnico e de atualização de versões;
 - De valores relativos a serviço de correção de erros, inclusive retroativos;
 - De taxa específica para o restabelecimento dos serviços agregados.
- 7.3. Nenhuma regra, condição ou referência externa ao contrato será considerada para regular a sua execução, valendo, para tanto, os estritos termos transcritos no contrato e seus anexos, inclusive neste instrumento
- 8. NÍVEL DE SERVIÇO**
- 8.1. Os níveis de serviços são critérios objetivos e mensuráveis estabelecidos, com a finalidade de aferir e avaliar diversos fatores relacionados com os serviços contratados.
- 8.2. Para mensurar esses fatores serão utilizados indicadores de desempenho relacionados com a natureza e característica dos serviços contratados, para os quais foram estabelecidas metas quantificáveis a serem cumpridos pela CONTRATADA.

- 8.3. A frequência de aferição e avaliação dos níveis de serviços será mensal, devendo a CONTRATADA elaborar relatório gerencial, constando os indicadores/metast de níveis de serviços alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual.
- 8.4. Para a execução do contrato, será implementado método de trabalho baseado no conceito de delegação de responsabilidade.
- 8.5. Esse conceito define a CAIXA como responsável pela gestão do CONTRATO e pelo ateste da aderência aos padrões de qualidade exigidos dos produtos e serviços entregues, e a CONTRATADA como responsável pela execução operacional dos serviços e gestão dos recursos humanos e físicos necessários para o atendimento dos chamados e seus respectivos Nível de Serviço.
- 8.6. O Nível de Serviço representa o desempenho dos serviços de monitoração com base em indicadores que tem por finalidade gerar informações objetivas dos serviços desempenhados pela CONTRATADA.
- 8.7. Pelo não cumprimento dos níveis de serviços contratados, atraso de prestação de serviços, inexecução, por culpa imputada à CONTRATADA, ou pela execução de forma incorreta, serão aplicados descontos e/ou multas sobre o valor mensal contratado, sem prejuízo de outras cominações cabíveis.

8.8. Indicador de Desempenho

- 8.8.1. Os indicadores de desempenho constam do ANEXO I-C - Níveis de Serviço, Indicadores e Penalidades.

9. TRANSFERÊNCIA DE CONHECIMENTO (sob demanda)

- 9.1. A Transferência de Conhecimento se constitui em obrigação contratual da CONTRATADA.
- 9.2. A execução da Transferência de Conhecimento pela CONTRATADA não implicará em qualquer ônus adicional para a CAIXA.
- 9.3. A transferência de conhecimento consiste em fornecer todos os subsídios para que a CAIXA obtenha os conhecimentos necessários ao perfeito entendimento da Solução contratada quanto a sua operacionalização e parametrização.
- 9.3.1. A CONTRATADA deverá encaminhar à CAIXA uma proposta preliminar de transferência de conhecimento, em até 10 dias corridos a partir da solicitação da CAIXA, sugerindo conteúdo programático, datas, infraestrutura necessária e carga horária para prévia avaliação, facultando-se à CAIXA solicitar a reformulação da proposta e sugerir inclusões, exclusões e/ou alterações em seu conteúdo.
- 9.3.2. A CAIXA poderá, a seu critério, alterar o cronograma previsto para a transferência de conhecimento, citado nos subitens anteriores, de forma a adequá-lo à disponibilidade dos usuários que trabalharão diretamente com a Solução.
- 9.3.3. A CONTRATADA terá até 15 (quinze) dias corridos, a partir da solicitação da CAIXA, para iniciar cada transferência de conhecimento.
- 9.3.4. Os custos referentes ao deslocamento do profissional técnico, se necessário, incluindo passagens, hospedagem e alimentação, e todo material utilizado, serão de responsabilidade da CONTRATADA, sem ônus adicionais para a CAIXA.

- 9.3.5. O ambiente e a logística necessária para transferência de conhecimento deverão ser providenciados pela CAIXA.
- 9.3.6. Ao final da transferência de conhecimento os empregados CAIXA deverão estar aptos a compreender todas as alternativas de uso de cada funcionalidade existente na Solução Tecnológica e usá-las de maneira adequada, além do conhecimento para gerar e avaliar relatórios e prestar suporte aos clientes no uso da referida Solução Tecnológica.
- 9.3.7. A transferência de conhecimento se dará de acordo com as datas e prazos estabelecidos pela CAIXA em 02 (duas) turmas.
- 9.3.8. As turmas serão montadas pela CAIXA contendo, no mínimo, 15 (quinze) participantes por turma.
- 9.3.9. Cada turma deverá cumprir um mínimo de 24 (vinte) horas de transferência de conhecimento.
- 9.3.10. As transferências de conhecimento poderão ocorrer via ensino à distância – EaD e serão operacionalizadas em plataforma indicada pela CAIXA, sem ônus adicionais para a CONTRATANTE.
- 9.4. Conteúdo programático
- 9.4.1. Deverão ser contemplados conteúdos programáticos diferenciados de transferência de conhecimento, para atendimento aos seguintes perfis de usuários abaixo especificados:
- a. Usuários finais da Solução
- Gestores de negócio
 - Auditoria interna
- 9.4.2. Usuários finais da solução:
- 9.4.2.1. Compreendem os usuários de negócio, gestores de risco e técnicos em gerenciamento de risco e técnicos de atendimento, os quais possuem perfis técnico gerencial. Estes usuários deverão ser capacitados para obter no mínimo os conhecimentos, habilidades e capacitação para utilização plena, geração de cálculos, produção de relatórios, utilização de ambiente de testes e parametrização da Solução.
- 9.4.3. Conteúdo mínimo a ser contemplado nas transferências de conhecimento:
- 9.4.4. Transferência de conhecimento #1
- 9.4.4.1. Terá o objetivo de capacitar as equipes CAIXA para o conhecimento da Solução Tecnológica, no tocante às suas funcionalidades, execução dos relatórios, parametrizações, criação de condições de conferência do e necessidades expostas pela área gestora do Negócio, na CAXA.
- 9.4.4.2. Público-alvo: Usuários finais da Solução
- Máximo de 15 pessoas
Número de turmas: 02
Local: Dependências da CAIXA ou remoto.
- 9.4.4.3. Todo material didático referente à transferência de conhecimento deverá ser fornecido em língua portuguesa do Brasil.

- 9.4.4.4. Dentre os itens de pauta/conteúdo programático, deverão constar exercícios de fixação a serem realizados pelos participantes, de modo a assegurar a efetiva habilitação do empregado para operação da solução.
- 9.4.4.5. Também é dever da CONTRATADA a elaboração de certificados de participação nas turmas de transferência de conhecimento realizadas, identificando os empregados participantes, o conteúdo abordado e a carga horária da respectiva transferência de conhecimento.
- 9.4.4.6. As transferências de conhecimento deverão ter como foco principal a demonstração prática das funcionalidades da Solução e o esclarecimento de eventuais dúvidas, sendo que, ao final das respectivas reuniões, haverá uma avaliação realizada junto aos participantes para atestar a qualidade e foco na demonstração prática das funcionalidades.
- 9.4.4.7. Ao final dos repasses de conhecimento, a CONTRATADA deverá encaminhar à CAIXA a relação de frequência e a avaliação dos participantes, para a realização do ateste.
- 9.4.4.8. Cada serviço de transferência de conhecimento será atestado pela CAIXA por meio de avaliação que demonstre a qualidade da transferência realizada e o conhecimento absorvido pelos participantes com referência às funcionalidades técnicas e de execução da Solução, conforme os seguintes critérios:
- Capacidade de esclarecimento de dúvidas do instrutor;
 - Didática de ensino/capacidade de transmissão de conteúdo;
 - Materiais e recursos utilizados;
 - Administração do tempo e adequação do conteúdo;
 - Demonstração de conhecimento da Solução;
 - Capacidade de realização das atividades propostas;
 - Funcionalidades técnicas e operacionais absorvidas.
- 9.4.4.9. As notas médias da transferência de conhecimento, atribuídas à CONTRATADA, não poderão ser inferiores a 7, em uma escala de 1 a 10.
- 9.4.4.10. Caso as notas médias sejam inferiores a 7, a CONTRATADA se obriga a repetir a transferência de conhecimento em pauta, sem ônus adicional para a CAIXA.
- 9.4.4.11. A CONTRATADA deverá zelar e assegurar a transferência de todo conhecimento adquirido ou produzido, relativamente a serviços em andamento ou finalizados, para as equipes da CAIXA e/ou para aquelas por ela designadas.
- 9.4.4.12. O descumprimento da obrigação da Transferência de Conhecimento incorrerá a CONTRATADA em multa em seu desfavor.
- 9.4.4.13. A CONTRATADA deverá fornecer a documentação da Solução compatível, incluindo manual de utilização da solução, que deverá conter passo a passo detalhado para utilização de todas as funcionalidades disponibilizadas na ferramenta.
- 9.4.4.13.1. Os documentos deverão ser compatíveis com ao menos o software ADOBE READER 9.0, ou superior (formato "PDF") e entregues em até 10 (dez) dias corridos a partir da solicitação da CAIXA ou da conclusão da fase de Ativação da Solução (setup).
- 9.4.4.14. O material deverá ser entregue em formato digital e em português (brasileiro)

- 9.4.4.15. O manual deverá ser atualizado, a pedido da CAIXA, por motivo de adequação necessária da utilização operacional da solução por parte dos usuários da CAIXA ou por motivo de atualização da Solução.
- 9.4.4.16. As atualizações dos manuais solicitados pela CAIXA deverão ser realizadas pela CONTRATADA em prazo máximo de 2 (dois) dias úteis.
- 9.4.4.17. Na impossibilidade de leitura dos arquivos no ambiente CAIXA, a CONTRATADA disponibilizará novos arquivos em até 24 (vinte e quatro) horas corridas também em formato digital.
- 9.4.4.18. A CONTRATADA fica obrigada, sempre que a CAIXA requerer, a prestar esclarecimentos sobre questões relativas à documentação pertinente à prestação dos serviços sem custos adicionais para a CAIXA.
- 9.4.4.19. A CONTRATADA deverá manter toda a documentação gerada atualizada durante toda a vigência do contrato.
- 9.4.4.20. Toda a documentação gerada pela CONTRATADA deverá ser disponibilizada para a CAIXA e passará a ser de sua propriedade.

10. HORÁRIO DA PRESTAÇÃO DOS SERVIÇOS

- 10.1. A prestação dos serviços se dará em regimes de “8x5” (8 horas por dia, 5 dias por semana, de segunda à sexta) a fim de garantir a disponibilidade e continuidade no atendimento e serviços escopo dessa contratação, conforme disposto no quadro:

Serviços	Regime de atendimento
Solução de Controle de Enquadramento dos Fundos de Investimento e Carteiras (software)	Implantação 8x5 Sustentação do serviço 8x5
Serviços de Customização	Implantação 8x5 Sustentação do serviço 8x5
Transferência de Conhecimento	8x5

11. INFORMAÇÕES COMPLEMENTARES

- 11.1. As demandas relacionadas à validação interna das premissas e metodologia da Solução poderão ser solicitadas a qualquer tempo pela CAIXA, sem limite quanto ao número de requisições ou horas necessárias, devendo ser atendidas no prazo de até 2 (dois) dias úteis, durante toda a vigência do contrato, sempre que houver necessidade de melhor entendimento ou nos casos em que houver atualizações, sem qualquer ônus adicional à CAIXA.

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

- 1.1. A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.
- 1.2. A Contratada deve manter rígido controle de acesso de seus colaboradores baseado nas informações de contratação, dispensa e controle de ausências (férias, licenças, atestados, admissão, demissão etc.) impedindo o acesso ao ambiente computacional, local ou remoto, quando o colaborador não estiver em pleno exercício de suas atividades.
- 1.3. A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 1.4. A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.
- 1.5. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 1.6. Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.
- 1.7. As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 1.8. Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 1.9. A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 1.10. A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 1.11. A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.
- 1.12. Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.
- 1.13. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 1.14. A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 1.15. A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.

- 1.16. A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.
- 1.17. A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 1.18. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 1.19. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.
- 1.20. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.
- 1.21. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 1.22. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.
- 1.23. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:
- O tipo de evento (inclusão, alteração, exclusão, consulta);
 - O autor do evento;
 - A data e hora do evento;
 - O endereço lógico do equipamento de origem do tipo do evento.
- 1.24. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 1.25. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.
- 1.26. Devem ser observadas as boas práticas de segregação e diferenciação entre ambientes de não produção e produtivo, estabelecendo-se acessos pertinentes para cada etapa do ciclo de desenvolvimento/manutenção e alinhado com o princípio do privilégio mínimo.
- 1.27. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 1.28. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.

- 1.29. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos na seção 2.7.
- 1.30. A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

2. SEGURANÇA DE PLATAFORMAS

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

automatizado, com base em múltiplos fatores de autenticação. Em caso de dispositivos Apple solicita-se também o cadastro do ABM – Apple Bussines Manager - de forma a garantir as configurações de MDM sem a intervenção dos usuários finais.

2.12. Os dados armazenados em dispositivos móveis devem ser criptografados pela solução de MDM e a Contratada deve ter a capacidade de fazer exclusão remota (wiping) em dispositivos móveis corporativos.

2.13. Caso a Contratada permita BYOD ou o uso de dispositivos móveis particulares em atividades laborais, ela deve estabelecer uma separação lógica dos dados organizacionais dos dados pessoais do seu funcionário, de modo a limitar a capacidade de propagação dos dados organizacionais e facilitar a exclusão remota desses dados.

3. SEGURANÇA DE REDES

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

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

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

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

3.5. Caso o firewall esteja em ambiente de um Provedor de Serviços em Nuvem, este garantirá a adequação do ambiente aos itens descritos e manterá as certificações solicitadas pela CAIXA, como descrito no item 4.

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

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

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

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

3.10. As soluções de firewall, IPS e anti-DDoS utilizadas pela Contratada serão validadas pela CAIXA a partir de documentações do fabricante ou certificações. No caso em que a Contratada sustentar a rede através de um Provedor de Serviços em Nuvem serão aceitas as certificações descritas no item 4 como garantia de conformidade de segurança no ambiente.

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

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

3.13. Excepcionalmente, quando a versão 1.3 do TLS não for suportada, deve ser usada a versão 1.2.

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

4. GESTÃO DE VULNERABILIDADES

- 4.1. A Contratada deve adotar o princípio de security by design para garantir que as aplicações de TI por ela desenvolvidas sejam seguras desde a concepção, assim como deve adotar as melhores práticas de mercado de análise de código automatizada, utilizando como referência os padrões do OWASP.
- 4.2. A Contratada deve possuir um processo de Gestão Contínua de Vulnerabilidades, sem custo adicional para a CAIXA, observando prazos para remediação em normativo específico estabelecido pela CAIXA, conforme a criticidade da falha encontrada.
- 4.3. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.
- 4.4. A Contratada deve realizar testes independentes de intrusão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA, seguindo frameworks de melhores práticas aplicáveis a testes dessa natureza.
- 4.5. Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados à CAIXA sempre que solicitado.

5. GESTÃO DE INCIDENTES DE SEGURANÇA

- 5.1. A Contratada deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.
- 5.2. O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.
- 5.3. A Contratada deve comunicar os incidentes detectados à CAIXA dentro do prazo acordado, conforme termos do SLA definido em contrato.
- 5.4. A Contratada deve ter um processo de notificação de incidentes **24x7**.
- 5.5. No caminho inverso, se a CAIXA detectar um incidente de segurança, a Contratada será notificada e deverá cooperar totalmente para resolver o incidente de segurança, fornecendo todas as informações relacionadas que possam levar a solução do incidente em questão (também **24x7**).
- 5.6. 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.

- 5.7. A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.
- 5.8. A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.
- 5.9. A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.
- 5.10. 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.

6. AUDITORIA CONTÍNUA

- 6.1. A Contratada deve apresentar à CAIXA, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.
- 6.2. A Contratada deve informar imediatamente à CAIXA sobre qualquer auditoria regulatória, sua finalidade e como ela se relaciona com os serviços prestados à CAIXA.
- 6.3. 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.
- 6.4. A Contratada deve fornecer os subsídios necessários para que a CAIXA implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.

7. CONTROLES CRIPTOGRÁFICOS

- 7.1. Os requisitos apresentados nesta seção devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá comprovar por relatório de auditoria (Due Dilligence Remoto) que o armazenamento/processamento dos dados ocorre somente em ambiente de nuvem e o Provedor deve atender, além dos requisitos a seguir, as regras descritas no item 3.3 deste Guia.
- 7.2. A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.
- 7.3. A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.
- 7.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.

- 7.5. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 7.6. A Contratada deve fazer a geração e a renovação de certificados digitais expostos na Internet junto a autoridades certificadoras reconhecidas internacionalmente, cujas raízes de cadeias utilizadas na emissão dos certificados digitais façam parte do repositório de cadeias confiáveis dos principais navegadores e versões de sistemas operacionais, como: iOS 7 e superiores; Android 4 e superiores; Microsoft Edge 12 e superiores; Mozilla Firefox 45 e superiores; Google Chrome 49 e superiores; Apple Safari 8 e superiores; Linux Ubuntu 14 e superiores; Linux Mint 15 e superiores; MAC OS X 10.10 e superiores; e Windows 7 e superiores.
- 7.7. A Autoridade Certificadora deve possuir o selo Web Trust dentro do prazo de validade e a certificação Web Trust deve estar de acordo com, no mínimo, os Princípios e Critérios para Autoridades Certificadoras – versão 2.2.1, disponível em <https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/WT100aWebTrust-for-CA-221-110120-FinalAODA.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6FD> para todas as raízes de cadeias utilizadas na emissão dos certificados digitais.
- 7.8. Após a instalação desses certificados, todas as URLs publicadas deverão obter nota “A” nos testes realizados pela ferramenta Qualys SSL Labs (<https://www.ssllabs.com/ssltest>).
- 7.9. As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 7.10. Caso haja a necessidade do compartilhamento de chaves simétricas entre a CAIXA e a Contratada, essas chaves devem ser geradas pela CAIXA e levadas para o ambiente da Contratada, onde devem ser armazenadas por meio de soluções FIPS 140-2 nível 3, sem possibilidade de exportação das chaves. Nesse caso, a Contratada deve prover meios que permitam a inserção das chaves da CAIXA no seu ambiente de forma segura, sem a necessidade de manipulação de chaves em um único componente em texto-claro.
- 7.11. A Contratada deve permitir a criptografia de dados em repouso, considerando volumes (por exemplo: a criptografia de um disco inteiro) e estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).
- 7.12. A Contratada deve prover a criptografia de dados em repouso utilizando, no mínimo, algoritmo AES com chaves de 128 bits.
- 7.13. A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.
- 7.14. A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.
- 7.15. A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.
- 7.16. A Contratada deve permitir a auditoria da segurança de chaves criptográficas.
- 7.17. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3, ou, quando não for suportado, 1.2.
- 7.18. A Contratada deve possuir a capacidade de configuração das cifras criptográficas e das versões de TLS utilizadas pela CAIXA, suportando, no mínimo, TLS 1.2 e as cifras a seguir:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- 7.19. Os parâmetros TLS Renegotiation e TLS Resumption devem estar desabilitados.
- 7.20. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão mTLS, por exemplo – a Contratada deve fazer todas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.
- 7.21. O certificado de cliente só deve ser aceito se o método X509_verify_cert retornar OK para todas as validações previstas.

8. ENCERRAMENTO DO CONTRATO

- 8.1. Os requisitos apresentados nesta seção devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá comprovar por relatório de auditoria (Due Dilligence Remoto) que o armazenamento ocorre somente em ambiente de nuvem.
- 8.2. A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.
- 8.3. A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.
- 8.4. A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer os padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.
- 8.5. Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

9. GLOSSÁRIO

- 9.1. AICPA (American Institute of Certified Public Accountants) - Instituto Americano de Contadores Públicos Certificados - É a associação profissional nacional dos contadores dos Estados Unidos, com mais de 330.000 membros, incluindo contadores com atuação em negócios, indústria, governo e educação, estudantes e associados estrangeiros.
- 9.2. Atividades críticas - atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo (Adaptado da portaria PR/GSI nº 93, de 26 de setembro de 2019).

- 9.3. BYOD (Bring Your Own Device) – política que prevê a utilização de recursos do próprio empregado para realização das atividades laborais.
- 9.4. CASB (Cloud Access Security Broker) – Agente de segurança em nuvem que monitora as atividades e aplica políticas de segurança.
- 9.5. Dados estratégicos – dados que subsidiam a tomada de decisão, planos estratégicos, planejamentos, diretrizes, análise de riscos, oportunidades e ambições da CAIXA, podendo estar relacionados a processos e/ou produtos estratégicos/prioritários para a empresa. A perda, modificação ou divulgação não autorizada desses dados pode afetar a competitividade e a governança corporativa da CAIXA.
- 9.6. Fornecedor – pessoa física ou jurídica contratada para fornecer bens ou serviços para a CAIXA, o qual se encontra integrado à cadeia produtiva da empresa.
- 9.7. FIPS (Federal Information Processing Standards) – padrões desenvolvidos pelo NIST para uso em sistemas de computador por agências do governo americano não-militares e contratantes do governo.
- 9.8. Gestor de TI – empregado com atribuições gerenciais designado pela Unidade Executora para coordenar e comandar a utilização e execução no tocante aos aspectos técnicos do contrato, conforme TE165.
- 9.9. Hardening - é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.
- 9.10. HSM (Hardware Security Module) – equipamento para o armazenamento seguro de chaves criptográficas.
- 9.11. Informação Corporativa - informação não pública que possui valor para o negócio da CAIXA e sua perda, modificação ou divulgação não autorizada pode gerar impactos para a CAIXA.
- 9.12. Informação Pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem abrangendo clientes ou empregados da CAIXA.
- 9.13. Key Vault – Estrutura segura de armazenamento para chaves criptográficas e certificados.
- 9.14. LGPD – Lei Geral de Proteção de Dados, no 13.709 de 14 de agosto de 2018.
- 9.15. MAM (Mobile Application Management) – Solução que permite controlar os dados de negócios nos dispositivos pessoais dos usuários.
- 9.16. MDM (Mobile Device Management) – Solução que permite configurar políticas de proteção de dados em seus dispositivos móveis. Quando um dispositivo está sob o gerenciamento de dispositivo móvel, é possível controlar todo o dispositivo, apagar dados dele e redefini-lo para as configurações de fábrica.
- 9.17. NAC (Network Access Control) – Tecnologia que viabiliza a implementação de políticas para controlar o acesso à rede corporativa. Tais políticas podem ser baseadas em autenticação do dispositivo, configuração do endpoint (postura) ou identidade do usuário.
- 9.18. NIST (National Institute of Standards and Technology) – Instituto de padrões de tecnologia do governo dos Estados Unidos da América.

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

ANEXO I-C**NÍVEIS DE SERVIÇO, INDICADORES E PENALIDADES****1 NÍVEL DE SERVIÇO**

- 1.1 Os níveis de serviços são critérios objetivos e mensuráveis estabelecidos, com a finalidade de aferir e avaliar diversos fatores relacionados com os serviços contratados.
- 1.2 Para mensurar esses fatores serão utilizados indicadores de desempenho relacionados com a natureza e característica dos serviços contratados, para os quais foram estabelecidas metas quantificáveis a serem cumpridos pela CONTRATADA.
- 1.3 A frequência de aferição e avaliação dos níveis de serviços será mensal, devendo a CONTRATADA elaborar relatório gerencial, constando os indicadores/metadados de níveis de serviços alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual.
- 1.4 Para a execução do contrato, será implementado método de trabalho baseado no conceito de delegação de responsabilidade.
- 1.5 Esse conceito define a CONTRATANTE como responsável pela gestão do CONTRATO e pelo ateste da aderência aos padrões de qualidade exigidos dos produtos e serviços entregues, e a CONTRATADA como responsável pela execução operacional dos serviços e gestão dos recursos humanos e físicos necessários para o atendimento dos chamados e seus respectivos Nível de Serviço.
- 1.6 O Nível de Serviço representa o desempenho dos serviços de monitoração com base em indicadores que tem por finalidade gerar informações objetivas dos serviços desempenhados pela CONTRATADA.
- 1.7 Pelo não cumprimento dos níveis de serviços contratados, atraso de prestação de serviços, inexecução, por culpa imputada à CONTRATADA, ou pela execução de forma incorreta, serão aplicados descontos e/ou multas sobre o valor mensal contratado, sem prejuízo de outras cominações cabíveis.

1.8 Indicador de Qualidade Do Serviço

1.8.1 **Propósito:** Identificar a qualidade do serviço prestado.

1.8.2 **Meta:** Mínimo de 98,0%

1.8.3 **Métrica:**

IQS: Indicador de qualidade do serviço

ID: Índice de disponibilidade

IA: Índice de chamados de suporte funcional da ferramenta atendidos no prazo

IR: Índice de chamados de suporte funcional da ferramenta sem reabertura

IC: Índice de comunicação de incidentes à CONTRATANTE

IE: Índice de relatórios entregues no prazo

IP: Índice de demandas entregues no prazo

$$IQS = (5 \times ID + 2 \times IA + 1 \times IR + 0,5 \times IC + 0,5 \times IE + 2 \times IP) / 11$$

- 1.8.4 O valor do pagamento mensal correspondente aos **Serviços para o Ambiente Tecnológico em Nuvem e Serviços de Sustentação** será ajustado conforme tabela a seguir, de forma tal que o valor aferido será multiplicado pelo respectivo fator de ajuste, gerando o valor devido para pagamento à CONTRATADA:

Fator de Nível de Serviço	
IQS (%)	Fator de Ajuste
Igual ou superior a 98,0	1,0
97,9 a 88,0	0,9
87,9 a 78,0	0,8
77,9 a 68,0	0,7
67,9 a 58,0	0,6
57,9 a 48,0	0,5
47,9 a 38,0	0,4
Inferior a 38,0	0,3

1.8.5 Métricas de Aferição da Qualidade Do Serviço

1.8.5.1 Disponibilidade

1.8.5.1.1 **Propósito:** Aferir a disponibilidade dos serviços.

1.8.5.1.2 **Meta:** Mínimo de 99,9% de disponibilidade

1.8.5.1.3 **Métrica:**

ID: Índice de disponibilidade

TTI: Quantidade de minutos de indisponibilidade da Solução no período de referência

TM: Quantidade de minutos no período de referência

$$ID = \left(1 - \frac{TTI}{TM}\right) \times 100$$

1.8.5.1.4 Os períodos de indisponibilidade serão contabilizados a partir do registro do incidente nas ferramentas de monitoração da própria CONTRATADA ou a partir do momento da abertura do chamado técnico pela CONTRATANTE.

1.8.5.1.5 Será considerado no cálculo de disponibilidade a soma dos tempos de indisponibilidades totais e parciais do serviço, a partir do primeiro minuto do período de referência até último minuto deste, salvo interrupções para manutenção previamente planejadas e autorizadas, devendo ser informadas à CONTRATANTE.

1.8.5.2 Chamados atendidos no prazo

1.8.5.2.1 **Propósito:** Garantir o cumprimento dos prazos de atendimento de suporte funcional da ferramenta.

1.8.5.2.2 **Meta:** Mínimo de 95% dos chamados de suporte funcional da ferramenta atendidos no prazo

1.8.5.2.3 Métrica:

IA: Índice de chamados de suporte funcional da ferramenta atendidos no prazo

CCP: Quantidade de chamados de suporte funcional da ferramenta concluídos no prazo no período de referência

CC: Quantidade de chamados de suporte funcional da ferramenta concluídos no período de referência.

$$IA = \frac{CCP}{CC} \times 100$$

1.8.5.2.4 O atendimento deverá ser realizado conforme os prazos dispostos a seguir:

Tipo do chamado	Criticidade	Período de atendimento	Tempo máximo para início do atendimento	Tempo máximo de solução paliativa	Tempo máximo de solução definitiva
Suporte funcional da ferramenta	Severidade 1	Dias úteis das 09h00 às 17h00	30 min	2 horas	12 horas
	Solução está parada ou fora de funcionamento e não há meios de contornar a falha. Número significativo de usuários foi afetado ou impacto operacional significativo foi causado.				
	Severidade 2	Dias úteis das 09h00 às 17h00	40 min	3 horas	24 horas
	Solução está apresentando falhas de funcionamento, sem causar interrupção do serviço, mas afetando significativamente seu desempenho. Impacto crítico aos usuários.				
	Severidade 3		02 horas	6 horas	36 horas

	Solução está parada ou fora de funcionamento. O problema pode ser contornado. Impactos operacionais moderados a pequenos. Impacto moderado aos usuários.	Dias úteis das 09h00 às 17h00			
	Severidade 4	Dias úteis das 09h00 às 17h00	02 horas	6 horas	6 horas
	Consultas técnicas e dúvidas				

1.8.5.3 Reabertura de chamados

1.8.5.3.1 **Propósito:** Garantir efetividade dos atendimentos de suporte funcional da ferramenta.

1.8.5.3.2 **Meta:** Mínimo de 95% dos chamados de suporte funcional da ferramenta sem reabertura.

1.8.5.3.3 **Métrica:**

IR: Índice de chamados de suporte funcional da ferramenta sem reabertura

CSR: Quantidade de chamados de suporte funcional da ferramenta reabertos no período de referência

CC: Quantidade de chamados de suporte funcional da ferramenta concluídos no período de referência.

$$IR = \left(1 - \frac{CSR}{CC}\right) \times 100$$

1.8.5.4 Comunicação de incidentes

1.8.5.4.1 **Propósito:** Garantir tempestividade na comunicação dos incidentes com Severidade 1 ou Severidade 2.

1.8.5.4.2 **Meta:** Mínimo de 90% dos incidentes com Severidade 1 ou Severidade 2 comunicados à CONTRATANTE em até 10 minutos.

1.8.5.4.3 **Métrica:**

IC: Índice de comunicação de incidentes à CONTRATANTE

ICP: Quantidade de incidentes com Severidade 1 ou Severidade 2 comunicados à CONTRATANTE em até 10 minutos, no período de referência

IP: Quantidade de incidentes com Severidade 1 ou Severidade 2 identificados no período de referência

$$IC = \frac{ICP}{IP} \times 100$$

- 1.8.5.4.4 Em até 10 minutos após sua identificação, a CONTRATADA deverá comunicar à CONTRATANTE todo incidente com Severidade 1 ou Severidade 2 identificados pela CONTRATADA, parceiros ou usuários Solução.
- 1.8.5.4.5 A comunicação inicial deverá ser realizada ainda que não se tenha o diagnóstico da situação e visão completa dos impactos.
- 1.8.5.4.6 Após a primeira comunicação à CONTRATANTE, a CONTRATADA deverá manter rotina de comunicação a cada 30 minutos, informando o diagnóstico do incidente e ações em andamento, até a resolução.
- 1.8.5.4.7 A comunicação se dará por telefone, WhatsApp, ou qualquer outra forma de comunicação instantânea, devendo posteriormente a CONTRATADA formalizar relatório complementar sobre a ocorrência.

1.8.5.5 **Entrega de relatórios no prazo**

1.8.5.5.1 **Propósito:** Garantir tempestividade e efetividade nas análises realizadas pela equipe da CONTRATANTE, tanto para aspectos gerenciais, financeiros, técnicos e de qualidade.

1.8.5.5.2 **Meta:** 95% dos relatórios entregues no prazo.

1.8.5.5.3 **Métrica:**

IE: Índice de relatórios entregues no prazo

REP: Quantidade de relatórios entregues no prazo no período de referência

RE: Quantidade de relatórios entregues no período de referência

$$IE = \frac{REP}{RE} \times 100$$

- 1.8.5.5.4 A CONTRATADA deverá disponibilizar os relatórios gerenciais, financeiros, técnicos e de qualidade requeridos pela CONTRATANTE.
- 1.8.5.5.5 O formato, periodicidade e data de entrega dos relatórios serão acordados previamente entre CONTRATANTE e CONTRATADA.
- 1.8.5.5.6 Relatórios entregues fora do prazo ou não aceitos pela CONTRATANTE penalizarão o indicador.
- 1.8.5.5.7 Caso necessário, a CONTRATANTE poderá solicitar que os relatórios sejam entregues e apresentados pela CONTRATADA em reunião previamente agendada.

1.8.5.6 **Entrega de demandas no prazo**

1.8.5.6.1 **Propósito:** Garantir que as entregas de demandas de Serviço Técnico Especializado sejam entregues no prazo estabelecido.

1.8.5.6.2 **Meta:** Mínimo de 95% das demandas entregues no prazo.

1.8.5.6.3 **Métrica:**

IDE: Índice de demandas de Serviço Técnico Especializado entregues no prazo

DEP: Quantidade de demandas de Serviço Técnico Especializado entregues no prazo no período de referência

DE: Quantidade de demandas de Serviço Técnico Especializado entregues no período de referência

$$IP = \frac{DEP}{DE} \times 100$$

- 1.1 A CONTRATADA não poderá ser responsabilizada pelo não atendimento do nível de severidade estabelecido, quando o acionamento for originado por falha, interrupção ou qualquer outra ocorrência nos serviços prestados pelas concessionárias de serviços de telecomunicações ou energia elétrica, indisponibilidade de dados, inconsistência de dados e informações geradas pela CAIXA, infraestrutura e capacidade de ambiente de tecnologia CAIXA ou de terceiros, inclusive o tempo necessário à restauração do ambiente após o restabelecimento das condições de operação, não se caracterizando nesses casos a indisponibilidade dos serviços ou inadimplemento da CONTRATADA.
- 1.2 Considera-se um problema plenamente solucionado quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva, ou seja, quando não se tratar de uma resolução paliativa.
- 1.3 Toda e qualquer intervenção no ambiente produtivo que venha a impactar a disponibilidade da solução deve ser executada somente mediante comunicação prévia a CAIXA, a partir de informações claras dos procedimentos que serão adotados/executados pela CONTRATADA
- 1.4 Ao final de cada atendimento e resolução de chamado, o técnico da CONTRATADA realizará, em conjunto com empregados da CAIXA, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.
- 1.5 Ao término dos testes e do atendimento (fechamento do chamado), a CONTRATADA deverá registrar, detalhadamente, na ferramenta de abertura do chamado da CAIXA, as causas do problema e a resolução adotada.
- 1.6 Nos casos em que o atendimento não se mostrar satisfatório, a CAIXA fará reabertura do chamado, mantendo-se as condições e prazos do primeiro acionamento.
- 1.7 A CONTRATADA emitirá relatório, sempre que solicitado pela CAIXA, em papel e em arquivo eletrônico editável, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados abertos e fechados no período, incluindo:
- Quantidade de ocorrências (chamados) registradas no período; Número do chamado registrado na ferramenta e nível de severidade, inclusive aqueles com reabertura;
 - Data e hora de abertura;
 - Data e hora de início e conclusão do atendimento;
 - Identificação da localidade, unidade e técnico da CAIXA que registrou o chamado;
 - Identificação do técnico da CONTRATADA que atendeu ao chamado aberto;
 - Descrição do problema;
 - Severidade de cada chamado;
 - Descrição da resolução;

- Informações sobre eventuais escalações dos problemas;
- Consolidado dos chamados que não atenderam aos prazos estabelecidos, com as devidas justificativas para o descumprimento dos prazos contratados;
- Total de chamados no mês e o total acumulado até a apresentação do relatório.

1.8 Revisão do ANMS

1.8.1 A critério da CAIXA, o presente Nível Mínimo de Serviço (NMS) poderá ser revisto, com periodicidade mínima de 6 (seis) meses.

1.9 Das Sanções Administrativas

1.9.1 Pela inexecução total ou parcial do objeto deste contrato e/ou pelo atraso injustificado na sua execução, garantida a prévia defesa, a CONTRATADA ficará sujeita às seguintes sanções, sem prejuízo das demais cominações aplicáveis:

- Multa;
- Suspensão temporária de participação em licitação e contratação com a CAIXA, pelo prazo de até 2 (dois) anos;

1.9.2 A multa será aplicada nas situações, condições e percentuais indicados a seguir:

a) Será cobrada MULTA pelo descumprimento injustificado das obrigações detalhadas na Cláusula Segunda - Das Obrigações da Contratada, nas situações e formas abaixo:

Item	Descumprimento	Sanção
I	Não observar as obrigações de natureza operacional , previstas no contrato.	Multa de 0,5 % (por cento) sobre o valor total do contrato .
II	Não observar as obrigações de natureza técnica , previstas no contrato.	Multa de 0,4 % (por cento) sobre o valor total do contrato .
III	Não observar as obrigações de natureza administrativa , previstas no contrato.	Multa de 0,3 % (por cento) sobre o valor total do contrato .

1.9.3 Pelo descumprimento dos prazos estabelecidos/acordados para o Serviço de **Ativação da Solução** (SETUP), a CONTRATADA estará sujeita a multa de 0,2% (por cento) do valor total do Serviço, para cada dia até o 30º (trigésimo) dia de atraso.

1.9.3.1 A partir da 31º (trigésimo primeiro) dia, persistindo o atraso, a multa será de 0,4% (por cento), sobre o valor total do contrato, por cada dia subsequente, ou seja, por quantos dias persistirem a não entrega da demanda.

1.9.4 Pelo descumprimento dos prazos estabelecidos para o Serviço de **Sustentação**, conforme definido no Termo de Referência, a CONTRATADA estará sujeita à multa de 0,2% (por cento) sobre o valor total do contrato, para cada dia de atraso até o 30º (trigésimo) dia de atraso.

- 1.9.4.1 A partir do 31º dia, persistindo o atraso, a multa será de 0,4% (por cento) sobre o valor total do contrato, por cada dia subsequente, ou seja, por quantos dias persistirem a não entrega da demanda.
- 1.9.5 Pelo descumprimento dos prazos estabelecidos/acordados para o **Serviço de Customização (sob demanda)**, conforme definido no Termo de Referência, a CONTRATADA estará sujeita à multa de 0,2% (por cento) sobre o valor total do contrato, para cada dia de atraso até o 30º (trigésimo) dia de atraso.
- 1.9.5.1 A partir do 31º dia, persistindo o atraso, a multa será de 0,4% (por cento) sobre o valor total do contrato, por cada dia subsequente, ou seja, por quantos dias persistirem a não entrega da demanda.
- 1.9.6 Pelo descumprimento dos prazos estabelecidos para o Serviço de **Transferência de Conhecimento (sob demanda)**, conforme definido no Termo de Referência, a CONTRATADA estará sujeita à multa de 0,2% (por cento) sobre o valor total do contrato, para cada dia de atraso até o 30º (trigésimo) dia de atraso.
- 1.9.6.1 A partir do 31º dia, persistindo o atraso, a multa será de 0,4% (por cento) sobre o valor total do contrato, por cada dia subsequente, ou seja, por quantos dias persistirem a não entrega da demanda.
- 1.9.7 Pelo descumprimento dos prazos estabelecidos para a Transição Contratual, conforme definido no Termo de Referência, a CONTRATADA estará sujeita à multa de 0,2% (por cento) sobre o valor total do contrato, para cada dia de atraso até o 30º (trigésimo) dia de atraso.
- 1.9.7.1 A partir do 31º dia, persistindo o atraso, a multa será de 0,5% (por cento) sobre o valor total do contrato, por cada dia subsequente, ou seja, por quantos dias persistirem a não entrega da demanda.
- 1.9.8 Pelo descumprimento de quaisquer dos requisitos de segurança e privacidade, a CONTRATADA estará sujeita à multa de 0,5% (meio por cento) sobre o valor Global do contrato.
- 1.9.9 A MULTA por inexecução contratual poderá ser cobrada nas seguintes situações:
- Interrupção da execução do contrato, sem prévia autorização da CAIXA, sendo a multa de 10% (dez por cento), calculada sobre o valor do faturamento do mês da ocorrência.
 - O total inadimplemento de nível de serviço contratado por culpa exclusiva da CONTRATADA em prazo superior a 30 dias de atraso implicará na aplicação de multa compensatória equivalente a 10% do valor do serviço em questão, sem detrimento da cobrança de ressarcimento suplementar caso o prejuízo causado seja superior ao valor da multa.
- 1.9.10 As multas estarão limitadas a 10% (dez por cento) do valor total do contrato.
- 1.9.11 As multas serão descontadas da garantia do valor do documento fiscal e, se não for suficiente, será cobrada diretamente da CONTRATADA judicialmente.

ANEXO I-D

CATÁLOGO DE SERVIÇOS

1. Serviço de Customização (sob demanda)

- 1.1. A mensuração dos serviços de customização da Solução para controle de enquadramento de fundos de investimento e carteiras será feita por horas, buscando a prestação de serviços por produtos e serviços entregues.
- 1.2. Entende-se por Horas a unidade de medida adotada que corresponde ao esforço para a realização e conclusão das atividades definidas, independentemente da quantidade de recursos alocados, condicionados a pagamento por entrega.
- 1.3. A complexidade estará identificada no quadro do item 3 – “Mensuração de Complexidade”, a partir dessa identificação, estima-se a quantidade de horas técnicas necessárias para a atividade.
- 1.3.1. Para que se defina a quantidade de horas, o serviço deverá inicialmente ser enquadrado conforme as atividades que constam na tabela do item 2 – “Serviços”.
- 1.3.2. Observando que a complexidade da atividade determinará o número de horas, seja simples, média ou complexa onde o critério para a definição da complexidade está descrito, respectivamente para cada tipo de atividade, no quadro do item 3 – “Mensuração de Complexidade”.

2. Serviços

Descrição	Estimativa					
	Complexidade Baixa		Complexidade Média		Complexidade Alta	
	Prazo (Hrs)	Valor (R\$)	Prazo (Hrs)	Valor (R\$)	Prazo (Hrs)	Valor (R\$)
Criar ou configurar jornada de controle de enquadramento de fundos de investimento e carteiras	35		80		141	
Criar ou configurar dashboard/relatórios	31		93		127	
Criar ou configurar integrações com sistemas/aplicativos da CAIXA	60		160		259	
Criar ou configurar integrações com sistemas/aplicativos de Terceiros	63		147		253	
Criar ou configurar políticas de UI/layout	31		60		127	
Criar ou configurar regra de negócio	39		103		138	
Criar ou configurar regras de controle de acesso	25		77		200	

3. Mensuração de Complexidade

Descrição da Atividade	Matriz de Complexidade		
	Baixa	Média	Alta
Criar ou configurar jornada de controle de enquadramento de fundos de investimento e carteiras	Configuração de jornadas nativas da plataforma (por meio de parâmetros)	Configuração de jornadas não nativas já existentes na plataforma (por meio de codificação).	Criação de jornadas não nativas da plataforma (por meio de codificação).
Criar ou configurar integrações com sistemas da CAIXA	Configuração de integração com sistemas da Caixa através de conectores à sistemas de mercado já disponíveis na plataforma.	Criação ou configuração de integração com sistemas da CAIXA através da criação de interfaces ainda não existentes na plataforma (1:1, unidirecional, API Rest, SOAP, troca de arquivos, MQ).	Criação ou configuração de integração com sistemas da CAIXA através da criação de interfaces ainda não existentes na plataforma (1:N, bidirecional, API Rest, SOAP, troca de arquivos, MQ).
Criar ou configurar integrações com sistemas de terceiros	Configuração de integração com sistemas de terceiros através de conectores à sistemas de mercado já disponíveis na plataforma.	Criação ou configuração de integração com sistemas de terceiros através da criação de interfaces ainda não existentes na plataforma (1:1, unidirecional, API Rest, SOAP, troca de arquivos, MQ).	Criação ou configuração de integração com sistemas de terceiros através da criação de interfaces ainda não existentes na plataforma (1:N, bidirecional, API Rest, SOAP, troca de arquivos, MQ).
Criar ou configurar dashboards/relatórios	Criação ou configuração de um relatório utilizando recursos nativos da funcionalidade de <i>reporting</i> em cima de uma estrutura de dados já criada.	Criação ou configuração de um relatório utilizando recursos nativos da funcionalidade de <i>reporting</i> com a necessidade de adequação da estrutura de dados unificando tabelas.	Criação ou configuração de um relatório com funcionalidades que requerem análise temporal dos dados, onde for necessária a criação de indicadores, <i>breakdowns</i> e templates.

Criar ou configurar políticas de UI/layout	Parametrização na localização ou cores de elementos gráficos da interface da aplicação ou padrões de layout.	Criação e ajustes de elementos gráficos da interface da aplicação, scripts ou padrões de layout sem a necessidade de customizar uma nova versão da ferramenta.	Criação e ajustes de elementos gráficos da interface da aplicação, scripts ou padrões de layout através de customização de versão da ferramenta.
Criar ou configurar regra de negócio	Criação ou configuração de regra de negócio utilizando-se condições de gatilho e ações através de parametrizações.	Criação ou configuração de regra de negócio utilizando-se condições de gatilho e ações através de scripts sem a necessidade de customizar uma nova versão da ferramenta.	Criação ou configuração de regra de negócio utilizando-se condições de gatilho e ações através de customização da versão da ferramenta.
Criar ou configurar regras de controle de acesso	Configuração de regras de controle de acesso em componentes já existentes na plataforma.	Criação de regras de controle de acesso em componentes novos criados na plataforma através de parametrização.	Criação de regras de controle de acesso em componentes novos criados na plataforma que necessitem script para que sejam configuradas as condições.

ANEXO I-E
PADRÃO TECNOLÓGICO
1. CONDIÇÕES GERAIS

Plataforma de hardware	Storage	Scale-Out
	Servidores	X86
Plataforma servidora	SISTEMA OPERACIONAL	Red Hat 7.0
		Windows 2016
	SERVIDOR WEB	IIS 7
		APACHE http Server 2.2
		APACHE TOMCAT 7.0
	SERVIDOR DE APLICAÇÕES	JBOSS EAP 6.2
	BANCO DE DADOS	SQL SERVER 2012
		Oracle 10g
	JVM	Versão 1.6.0.13
	SERVIÇO DE AUTENTICAÇÃO E AUTORIZAÇÃO	RedHat Keycloak SSO
Estação de Trabalho	SISTEMA OPERACIONAL	Windows 10
		McAfee Virusscan 10.7
	BROWSER	Microsoft Edge
		Google Chrome 120.0.6099.63
		Firefox 113
	ESCRITÓRIO	Microsoft Office 365
		Adobe Acrobat Reader DC
		Adobe Flash Player 15
		7-Zip 16
		Java 1.8.0.31
Integrações	Forma de integração on-line com os sistemas internos	Web Services (SOAP e REST)
		IBM Websphere MQ (Message Queue)
	Forma de integração on-line com os sistemas externos	Web Services (SOAP e REST)
	Forma de integração batch com os sistemas internos	Transferência de Arquivos
		ETL (Informática PowerCenter)
	Forma de integração batch com os sistemas externos	IBM B2B
Outros	Protocolo de rede	Socket TCP/IP e/ou HTTP e HTTPS
	Ferramenta de modelagem de dados	Power Designer versão 12
	Tipo de pacote para troca de mensagem	JSON
		XML
		Text/Plain
		ISO 8583

Ferramenta de virtualização	Vmware versão 6.0
Ferramenta de gerenciamento de conteúdo (ECM)	IBM FileNet
Ferramenta de ETL	PowerCenter versão 8
Ferramentas de BI	Pentaho Enterprise Premium Edition 7
	SAP BO 4.2
	Oracle BI Foundation 10G
	Power BI Reporting Services e Desktop 2019.
Ferramenta de Gerenciamento de Requisitos	Rational Requisite Composer
Ferramenta de Gerenciamento de Mudanças	ITSM - BMC
Ferramentas de Execução de Testes	Rational Performance Tester
	Rational Functional Tester
Ferramenta de transferência de arquivos	IBM B2B
	IBM Connect:Direct
Ferramenta de Gestão de Testes	Rational Quality Manager
Ferramentas de Gestão de Configuração	Rational Clear Case (ambiente centralizado)
	Subversion (ambiente descentralizado)

ANEXO I-F
PLANO DE CONTINGÊNCIA

1 Plano de Contingência

- 1.1 A CONTRATADA terá prazo de até 90 dias corridos, a contar da assinatura do contrato, para apresentar o seu plano de contingência, a ser aprovado pela CONTRATANTE.
- 1.2 O plano de contingência visa prover os serviços em caso da não disponibilidade do ambiente, conforme abaixo:
- 1.2.1 Nos casos de desastres naturais, acidentes, falhas de equipamentos, falhas de segurança, perda de serviços e ações intencionais, que porventura possam ocorrer prejudicando a continuidade de prestação dos serviços, não causando a paralisação dos serviços prestados à CONTRATANTE.
- 1.2.2 Assegurar, nos casos de greve ou paralisação de seus empregados, a continuação da prestação dos serviços, inclusive no caso de paralisação dos transportes públicos, hipótese em que a CONTRATADA deverá promover, às suas expensas, os meios necessários para que seus empregados cheguem aos seus locais de trabalho.
- 1.3 A CONTRATADA deve possuir ambiente de contingência da solução em nuvem pública, através de redundância do provedor de nuvem atual ou de outro provedor de nuvem pública, para continuidade dos serviços e apresentar, sempre que solicitado pela CONTRATANTE, evidências de que o ambiente de realização dos serviços contingenciados possui o grau de segurança necessário para garantir o sigilo das informações a ela confiadas.
- 1.4 O plano de contingência deverá apresentar a estratégia e o método de trabalho da CONTRATADA para continuidade dos serviços, onde deverá constar, no mínimo, os seguintes tópicos.
- 1.4.1 Identificação dos profissionais da CONTRATADA envolvidos na contingência, seus papéis e responsabilidades;
- 1.4.2 Cronograma identificando as tarefas, recursos e marcos de referência;
- 1.4.3 Estruturas e atividades de gerenciamento da contingência e as regras propostas de relacionamento/atendimento da CONTRATADA.
- 1.5 A CONTRATADA deverá assumir total responsabilidade pela continuidade dos serviços, garantindo que a CONTRATANTE não será prejudicada com qualquer esforço adicional requerido.

ANEXO I-G**SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE****1. GRAU DE CRITICIDADE SEGURANÇA DA INFORMAÇÃO - Máximo**

- 1.1. A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (<https://www.caixa.gov.br/Downloads/caixa-governanca/politica-seguranca-informacao.pdf>), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto do contrato.
- 1.2. A CONTRATADA deve proteger as informações corporativas da CAIXA e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.
- 1.3. A CONTRATADA deve garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações obtidas durante a prestação dos serviços ou em função deles e somente as utilizem no âmbito dos serviços contratados.
- 1.4. A CONTRATADA deve garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social.
- 1.5. A CONTRATADA deve garantir que as práticas de segurança da informação por ela executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento.
- 1.6. A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.
- 1.7. A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação.
- 1.8. A CONTRATADA fica ciente de que deve guardar o mais completo e absoluto SIGILO em relação às informações e dados que tiver conhecimento em razão do serviço a ser prestado, observadas as solicitações de órgãos de regulação, fiscalização, supervisão e de controle, bem como as determinações judiciais que deverão ser comunicadas imediatamente, pois ambas somente poderão ser atendidas mediante prévia autorização da área jurídica da CONTRATANTE.
- 1.9. A CONTRATADA fica ciente que, por força da lei, é responsável civil e criminalmente pela divulgação indevida, descuidada ou incorreta utilização das informações corporativas da CAIXA e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.
- 1.10. A CONTRATADA deve comunicar imediatamente à CONTRATANTE qualquer descumprimento às cláusulas acima, principalmente para os casos em que ficar comprovado o comprometimento de informação corporativa da CAIXA ou sob sua responsabilidade.
- 1.11. A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, anexo.

- 1.12. A CONTRATADA deve enviar, anualmente, à CONTRATANTE a versão vigente do(s) Termo(s) de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, a ser disponibilizado pela área gestora do contrato, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).
- 1.13. A CONTRATADA deve realizar ou contratar, treinamento para seus dirigentes, empregados e colaboradores, visando a sensibilização e conscientização em relação à segurança da informação e privacidade de dados, abordando no mínimo 80% do seguinte conteúdo:
- Política de Segurança da Informação: Conhecimento da política de segurança da informação da empresa e da Política de Segurança e Informação da CAIXA.
 - Tratamento da Informação: Uso seguro de informações corporativas a que tiver acesso; Adoção da política de “mesa limpa”, “tela limpa” e “impressora limpa”; Descarte seguro de informação.
 - Reporte de Incidentes: Formas de reporte de incidentes de segurança da informação na empresa e na CAIXA.
 - *Privacy by Design* e *Secure by Design*: Metodologia e princípios.
 - Fundamentos para Segurança Digital: Conceitos básicos de segurança digital; Uso da Internet.
 - Segurança de Dispositivos Digitais Pessoais: Proteção e privacidade em dispositivos digitais pessoais; Conhecendo, configurando e usando o dispositivo; mantendo o dispositivo; Vulnerabilidades e ameaças.
 - Segurança em Redes: Segurança na Internet; Segurança em redes *wi-fi* públicas; Proteção de redes pessoais; Computação em nuvem.
 - Segurança do Usuário: Autenticação no acesso ao sistema e a serviços; Proteção de contas pessoais; Mídias sociais; Segurança com e-mails; Armazenamento e compartilhamento de dados; Qualidade de vida digital; Segurança de dados do usuário em viagens.
 - Segurança e Comportamento em Mídias Sociais: Netiqueta; construindo seu perfil na Internet; Segurança em mídias sociais; administrando seu rastro digital; Uso saudável de mídias sociais; Fake News; Jogos online.
 - Comunidades Digitais: Educação na Internet; construindo comunidades digitais cidadãos; Empreendedorismo na Internet.
 - Criptografia: Criptografia; Certificação Digital; Assinatura Digital.
 - Direito Digital: Conceitos jurídicos e legislação relacionada à segurança da informação; Direitos autorais; Fraudes; Assédio virtual; Crimes cibernéticos; Crimes na Internet; Hacktivismo.
 - Prevenção à fraude: Engenharia social (formas defensivas contra *Phishing* e *Smishing*).
- 1.14. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.13.

- 1.15. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do período, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA.
- 1.16. A CONTRATADA deve se adequar às normas e a legislação vigente inerentes à Segurança da Informação relacionadas às atividades da CONTRATANTE, enquanto empresa pública e instituição financeira.
- 1.17. A CONTRATANTE poderá exercer o direito de exigir alterações nos controles de segurança da CONTRATADA, à medida que os ambientes externos e internos se modifiquem.
- 1.18. A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores:
- a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, treinados em SI, conforme item 1.13 no último ano dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base;
 - b) Quantidade de empregados que assinaram o Termo de Responsabilidade de Segurança da Informação, previsto no item 1.12, dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base.
- 1.19. O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente instrumento contratual, implicará em:
- a) Multa;
 - b) Suspensão temporária de participação em licitação e contratação com a CONTRATANTE, por prazo não superior a 2 (dois) anos.
- 1.19.1. A multa poderá ser aplicada na hipótese de não atendimento a qualquer requisito de segurança definido no instrumento contratual, sendo a multa de 10% (dez por cento), calculada sobre o valor do faturamento referente ao mês da ocorrência do descumprimento contratual.
- 1.19.2. A CONTRATANTE poderá solicitar a apresentação de Plano de Melhoria à CONTRATADA constatado o não atendimento a qualquer requisito de segurança definido no instrumento contratual.
- 1.19.3. Constatada a execução insatisfatória do Plano de Melhoria, a CONTRATANTE, a seu critério, poderá promover a rescisão antecipada do contrato, ressaltado o seu direito à indenização pelos prejuízos eventualmente constatados e aplicação da penalidade contratual a ela associada.
- 1.20. Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a executar o Plano de Continuidade de Negócios aprovado pela CAIXA.
- 1.21. Quaisquer materiais ou documentos com informações confidenciais que tenham sido fornecidos à CONTRATADA pela CONTRATANTE serão devolvidos, acompanhados de todas as cópias, em até 5 (cinco) dias, a partir da formalização de solicitação de devolução das informações confidenciais pela CONTRATANTE.

- 1.22. No encerramento/extinção do contrato a CONTRATADA se compromete a:
- a) entregar a versão mais atualizada de todos os artefatos, componentes e demais produtos por ele produzidos durante a vigência do contrato;
 - b) executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CONTRATANTE ou a quem ela indicar, observada a regulamentação vigente;
 - c) devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.
- 1.23. A CONTRATADA é responsável por realizar o tratamento das informações da CAIXA e as sob sua responsabilidade, observando sua classificação de sigilo, bem como as demais regras internas da CAIXA estipuladas na versão vigente do manual normativo OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.
- 1.24. A CONTRATADA, durante a execução dos serviços contratados, deve adotar a mesma classificação da informação adotada pela CONTRATANTE, observar e cumprir as regras internas da CONTRATANTE quanto ao tratamento de informações sensíveis e confidenciais da CAIXA, previstas no OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.
- 1.25. A CONTRATADA é responsável pelas informações que obtiver, em razão de acesso aos recursos computacionais da CAIXA e se compromete a tomar conhecimento e cumprir as regras de uso aceitável e não aceitável da informação.
- 1.26. O treinamento de segurança da informação e proteção de dados referido no item 1.13 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 08 horas.
- 1.27. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.26, caso estabelecido pela CONTRATANTE.
- 1.28. A CONTRATADA deve emitir relatório, anualmente, até o último dia útil do mês subsequente ao término do ano base, relacionados aos seus riscos de segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CONTRATANTE.
- 1.29. O relatório referido no item anterior deve proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.
- 1.30. A CONTRATADA garantirá que a CONTRATANTE, ou a auditoria independente indicada pela CONTRATANTE, ou os órgãos de regulação/fiscalização das atividades de atuação da CAIXA tenham acesso físico e lógico ao seu ambiente e às informações relacionadas ao objeto do contrato, para realizar verificações relativas aos padrões de segurança da informação.

- 1.31. A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.
- 1.32. A CONTRATADA deve reportar imediatamente à CONTRATANTE os incidentes de segurança da informação identificados em seu ambiente ou operação e em toda sua cadeia produtiva.
- 1.33. A CONTRATADA deve enviar à CONTRATANTE, em até 05 dias úteis da detecção da ocorrência, relatório detalhado sobre o incidente de segurança da informação identificado, seus impactos, medidas corretivas implantadas e a implantar.
- 1.34. A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores mencionados no item 1.18 e dos demais a seguir:
- a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, que obtiveram nota mínima de aprovação no treinamento relacionado a Segurança da Informação mencionado no item 1.13 / Quantidade total de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
 - b) Quantidade de relatórios, referidos no item 1.28, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
 - c) Quantidade de relatórios, referidos no item 1.33, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base.
- 1.35. A CONTRATADA deve garantir a continuidade do processamento das informações críticas de negócios, no caso de contratação de bem ou serviço de suporte às atividades críticas da CAIXA.
- 1.36. A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos.
- 1.37. A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.
- 1.38. A CONTRATADA deve apresentar, sempre que requerido pela CONTRATANTE, relatórios emitidos por empresas de auditoria especializada independente que tenha realizado trabalho de auditoria em segurança da informação na CONTRATADA e certificações que atestem o nível de confiança nos princípios de segurança da informação.
- 1.39. A CONTRATADA se responsabiliza pelos incidentes de segurança detectados em sua infraestrutura.

2. PRIVACIDADE

- 2.1. A CONTRATADA deve tomar conhecimento dos termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD e de suas regulamentações, bem como das orientações da ANPD – Autoridade Nacional de Proteção de Dados, reconhecendo sua responsabilidade objetiva e de seus empregados/colaboradores em observar o disposto na LGPD no exercício de

suas atividades no tratamento de dados pessoais de clientes, empregados e colaboradores da CONTRATANTE.

- 2.2. Para fins do contrato, A CONTRATANTE assume o papel de Controladora de dados pessoais e a CONTRATADA assume o papel de operadora de dados pessoais.
- 2.3. Para a execução da finalidade prevista no contrato, a CONTRATANTE colocará à disposição da CONTRATADA:
- a) os dados pessoais envolvidos como nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, endereço de IP (Protocolo da Internet), dentre outros;
 - b) a categoria dos dados, como dados pessoais, dados pessoais sensíveis, dados pessoais de crianças e adolescentes;
 - c) a natureza das operações realizadas, 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.
- 2.4. A CONTRATADA se compromete a tratar os dados pessoais a que tiver acesso em decorrência do contrato, única e exclusivamente para cumprir a finalidade a que se destina seu tratamento, responsabilizando-se por qualquer acesso indevido.
- 2.5. A CONTRATADA deve garantir a confidencialidade no tratamento de dados pessoais, protegendo-os contra acesso, modificação, destruição ou divulgação não autorizada.
- 2.6. A CONTRATADA está autorizada a tratar, em nome da CONTRATANTE, os dados pessoais a que tiver acesso em decorrência do contrato para as finalidades relacionadas ao objeto avençado que justificam o tratamento de dados pessoais.
- 2.7. A CONTRATADA deverá, quando do término das atividades de tratamento de dados pessoais ou ao final do contrato, a critério da CONTRATANTE, eliminar ou devolver todos os dados pessoais, acompanhados de todas as cópias.
- 2.8. A CONTRATADA deve manter, por escrito, o registro das operações de tratamento realizadas em nome da CONTRATANTE.
- 2.9. A CONTRATADA deve colaborar com a CONTRATANTE no cumprimento de sua obrigação de responder às solicitações de exercício dos direitos dos titulares.
- 2.10. A CONTRATADA deve comunicar imediatamente a CONTRATANTE o recebimento de requisição do titular de dados no exercício de seus direitos.
- 2.11. A CONTRATADA garantirá à CONTRATANTE a disponibilização de todas as informações necessárias para que esta consiga demonstrar o cumprimento de suas obrigações nos termos da LGPD, mantendo a documentação disponível para a realização de auditorias e quaisquer inspeções.
- 2.12. A CONTRATADA deve obrigatoriamente adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- 2.13. A CONTRATADA notificará a CONTRATANTE de qualquer violação de dados pessoais imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência ao gestor operacional do contrato. Essa notificação deve ser acompanhada de todos os dados necessários para eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao(s) titular(es) de dados pessoais.
- 2.14. A CONTRATADA auxiliará a CONTRATANTE com as informações necessárias para cumprimento de suas obrigações junto à Autoridade Nacional de Proteção de Dados (ANPD) e quaisquer órgãos reguladores, de fiscalização, de supervisão e de controle, inclusive na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).
- 2.15. A CONTRATADA deverá notificar imediatamente a CONTRATANTE em caso de solicitações judiciais e de órgãos reguladores, de fiscalização, de supervisão e de controle para disponibilização de dados pessoais.
- 2.16. A CONTRATADA deverá observar os requisitos de privacidade desde a concepção em seus produtos, processos, serviços e soluções tecnológicas relacionadas ao tratamento de dados pessoais referentes ao contrato.
- 2.17. A CONTRATADA somente poderá realizar transferência de dados pessoais para terceiros seguindo as instruções da CONTRATANTE ou mediante prévia autorização

ANEXO I-H**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 login.
- 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/WT100aweTrust-for-ca-221-110120-finalaoda.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6FD> 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 Resumption 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 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 Technology) – 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 deles, 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

ANEXO I-I**INFRAESTRUTURA TECNOLÓGICA – Método de conexão com a CAIXA**

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

Os endereços de instalação são:

PRQ TECNOLOGICO CAPITAL DIGITAL LOTE 03 – S/N

Bairro: Granja do Torto

Cidade: Brasília UF: DF

CEP: 70.636-000

Setor de Indústrias Gráficas – SIG Quadra 1 – Lote 685/705

Bairro: SIG

Cidade: Brasília UF: DF

CEP: 70.610-410

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

Os endereços de instalação são:

Equinix SP IBX SP3

Av. Marcos Penteado de Ulhoa Rodrigues, 249

Santana de Parnaíba – SP – CEP: 06543 001

Equinix RJ IBX RJ2

Estrada Adhemar Bebianno, 1380

Del Castilho - RJ - CEP: 21051 070

- 1.3. O circuito WAN de contingência deve ser instalado em localidade e operadora de telecomunicações diferente do circuito principal.
- 1.3.1. Caso a CONTRATADA disponha de duas ou mais localidades de processamento deve-se considerar a contratação de circuitos para todas essas localidades direcionados aos Datacenters da CAIXA.
- 1.3.2. A Caixa poderá alterar seus endereços de conexão, inclusive de cidade e/ou de estado, de acordo com as suas necessidades, o que deverá ser atendido sem ônus para a Caixa.
- 1.4. Características gerais da conexão:

- 1.4.1. O dimensionamento do link de comunicação é de responsabilidade da contratada.
- 1.4.2. A responsabilidade de fornecimento e negociação junto à operadora do roteador CPE na ponta da CONTRATADA é de inteira responsabilidade da CONTRATADA.
- 1.4.3. A operadora deverá fornecer, caso ainda não tenha, concentrador na ponta da CAIXA conforme padrões estabelecidos. Caso a operadora já disponha de infraestrutura e equipamentos nos SITE DA CAIXA, ou pretenda utilizar o FABRIC dos ambientes de Multicloud, esta deverá fazer uso compartilhado destes equipamentos/conexões.
- 1.4.4. A operadora deve adotar arquitetura de compartilhamento de conexões físicas, ou seja, não será autorizado o uso de conexões físicas exclusivas. Este compartilhamento deve ser observado na conexão entre o equipamento da operadora e da Caixa garantindo ativação de diversas conexões lógicas na mesma interface física.
- 1.4.5. Nova conexão física independente poderá ser solicitada pela Caixa no caso de a conexão atender a ambientes internos segregados, tais como ambiente de desenvolvimento ou homologação.
- 1.4.6. A conexão com os equipamentos da Caixa deverá ser feita através de interface ethernet (mínimo gigabitethernet).
- 1.4.7. O endereçamento IP para trânsito WAN e de serviço (range para hosts) serão definidos pela CAIXA.
- 1.4.8. As conexões devem possibilitar a ativação de roteamento dinâmico baseado em BGP (Border Gateway Protocol).
- 1.4.9. Não é permitida a instalação de equipamentos da CONTRATADA no ambiente da Caixa.
- 1.4.9.1. É admitida a instalação de equipamentos de operadora instalados para uso na modalidade compartilhada, exceto nos ambientes de Multicloud.
- 1.4.9.2. Caso a CONTRATADA já disponha de conexão com a Caixa para o mesmo ambiente deste contrato, ela poderá fazer uso desta desde que efetue o upgrade correspondente ao novo serviço e atenda aos padrões definidos nesta especificação.
- 1.5. Permite-se conexão para ambientes de DESENVOLVIMENTO/HOMOLOGAÇÃO por VPN IPSEC, via Internet, conforme abaixo:
 - a) VPN site-to-site via Internet.
 - b) O acesso à Internet da empresa deverá possuir IP Fixo.
 - c) O dimensionamento deste acesso é responsabilidade da Empresa.
 - d) A CONTRATADA deverá dispor de roteador e concentrador VPN sob sua inteira responsabilidade.
 - e) A CAIXA fornecerá as definições de padrões para estabelecimento da VPN, porém não proverá suporte e manutenção na ponta da CONTRATADA.
 - f) Deverá utilizar no mínimo protocolo IPSEC 3DES-SHA1 IKE com 112bits.

ANEXO I-J

INTEGRAÇÕES PREVISTAS NA IMPLANTAÇÃO DA SOLUÇÃO

1. A tabela a seguir lista as integrações que deverão ser realizadas com a CAIXA, cujas interfaces enviam e/ou recebem informações no padrão e periodicidade definidos pela CAIXA.

Sigla	Descrição do Sistema / Entidade	Natureza da Informação	Plataforma	Padrão de Integração
SSO	Servidor de autenticação de clientes da CAIXA (SSO)	Integração com a solução de gestão de acessos da CAIXA	Baixa	OpenID Connect (OAuth 2.0) ou SAML 2.0, Financial-grade API (FAPI)
SISEQ	Sistema de Serviços Qualificados (Custódia Qualificada)	Acesso aos dados referentes aos ativos, fundos de investimentos, clubes de investimentos e carteiras administradas (próprias e de terceiros), além de demais informações necessárias para a execução das regras de enquadramento.	Baixa	API REST, B2B (FTP, SFTP, Connect Direct), Arquivos TXT.

- 1.1 **Observação:** O rol de sistemas ora apresentado poderá ser revisto a qualquer momento durante a execução contratual, com a inclusão, alteração e/ou exclusão de integrações, a critério exclusivo da CAIXA.