

**ANEXO I – TERMO DE REFERÊNCIA****1. DO OBJETO**

- 1.1. Modernização da solução Informatica utilizada atualmente pela CAIXA, contemplando a subscrição do IDMC - *Intelligent Data Management Cloud* do fabricante Informatica na modalidade SaaS (*Software as a Service*) em nuvem, os serviços de implantação, sustentação e atualização tecnológica, os serviço de suporte técnico especializado local (*on site*) e suporte à produção local (*on site*), serviços de suporte técnico especializado (TAM) e o serviço de transferência de conhecimento, conforme termos e condições estabelecidas neste documento e seus anexos, pelo período de 24 meses.

**2. DESCRIÇÃO E VOLUMETRIA DA SOLUÇÃO**

- 2.1. A solução deverá ser fornecida para o ambiente da CAIXA, seguindo o detalhamento a seguir:

OBJETO	DESCRIÇÃO DOS SERVIÇOS	MÉTRICA	QUANTIDADE
Modernização da Solução da Informatica utilizada pela CAIXA, na modalidade Subscrição SaaS e Serviços	Subscrição do IDMC - <i>Intelligent Data Management Cloud</i>	<b>Ano 1</b> – média de 1.691 IPU's ( <i>Informatica Processing Unit</i> ) por mês	20.292
		<b>Ano 2</b> – franquia de 2.951 IPU's por mês	35.412
	Serviço de implantação, sustentação e atualização tecnológica da solução	Parcela fixa mês	24 meses
	Serviço de suporte técnico especializado local ( <i>on site</i> ) e serviço de suporte à produção local ( <i>on site</i> )	HSTs (Horas de Serviço Técnico)	3.840 HSTs
	Serviço de transferência de conhecimento	TUs ( <i>Training Units</i> )	880 (sob demanda)
	Suporte técnico especializado (TAM)	8h por dia, 5 dias na semana	24 meses

- 2.2. A previsão de consumo de IPU's está descrita na rampa de adoção do ANEXO I-B - FORMA DE EXECUÇÃO.
- 2.3. Terminologias utilizadas neste contrato:

- 2.3.1. Entenda-se como **CONTRATADA**, a entidade jurídica com a qual a CAIXA estabelece o contrato que envolve a disponibilização da solução, devendo ser esta uma empresa parceira ou canal de venda autorizado do FABRICANTE no nível platinum.
- 2.3.2. Entenda-se como **FABRICANTE**, a entidade jurídica responsável pelo projeto, a arquitetura e a implantação da solução, com a qual a CONTRATADA estabelece relação de prestação de serviços.
- 2.3.3. Entenda-se como **SOLUÇÃO** toda a infraestrutura composta de software e serviços, construída pelo FABRICANTE e fornecida pela CONTRATADA.
- 2.3.4. Entenda-se como **SUBSCRIÇÃO** o termo que compreende a licença de uso por um determinado período, que no caso será de 24 (vinte e quatro) meses, abrangendo os serviços de suporte técnico, mediante a abertura de chamados e a atualização tecnológica ou de versões da solução.
- 2.3.5. Entenda-se como **ATIVOS DO INFORMATICA POWERCENTER** todos os componentes e recursos da ferramenta necessários para a execução das rotinas de ETL na solução atual *on-premise*. Entre esses ativos incluem-se, mas não se limitam a: *mappings, sessions, workflows, sources, targets*, conexões, entre outros elementos que compõem o processo de integração.

### **3. ESPECIFICAÇÃO TÉCNICA**

- 3.1. Os requisitos técnicos da solução estão detalhados no ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.

### **4. SERVIÇOS DE IMPLANTAÇÃO E SUPORTE**

- 4.1. Trata-se de serviços de suporte técnico, com vistas à reparação de eventuais falhas ou inconsistências detectadas na solução e em seus componentes, inclusive dúvidas associadas às suas configurações e às parametrizações, de forma a garantir o pleno, correto e seguro funcionamento da solução com o ambiente CAIXA, seja local (*on-premise*) ou nuvem (*cloud*).
- 4.2. Os requisitos dos serviços técnicos especializados estão detalhados no ANEXO I-B - FORMA DE EXECUÇÃO e modelo de avaliação da migração no ANEXO I – XI.

### **5. SERVIÇO TÉCNICO ESPECIALIZADO – HST (SOB DEMANDA)**

- 5.1. O serviço técnico especializado local (*on site*) e serviço de suporte à produção local (*on site*) visa garantir o cumprimento de necessidades pontuais e técnicas, especialmente relacionadas à evolução dos sistemas legados de forma a planejar a execução da migração com ajustes de performance e correção de falhas.
- 5.2. De forma a atender as necessidades pontuais é necessário contar com recursos técnicos especializados sob demanda, capazes de executar atividades críticas sem comprometer prazos e qualidade.

- 5.3. Os requisitos do suporte técnico especializado estão detalhados no ANEXO I-B - FORMA DE EXECUÇÃO.

**6. TRANSFERÊNCIA DE CONHECIMENTO (SOB DEMANDA)**

- 6.1. A transferência de conhecimento consiste em tornar os colaboradores CAIXA aptos a compreenderem todas as alternativas de uso de cada funcionalidade existente na solução, bem como usá-las de maneira adequada, além de promover o conhecimento para gerar e avaliar relatórios e prestar suporte aos clientes no uso da referida solução.
- 6.2. Os requisitos da transferência de conhecimento estão detalhados no ANEXO I-B - FORMA DE EXECUÇÃO e modelo avaliação de treinamentos ANEXO I-X - AVALIAÇÃO DE TREINAMENTO.

**7. LÍDER TÉCNICO (TAM)**

- 7.1. A solução atual da INFORMATICA encontra-se em processo de descontinuidade pelo fabricante. Para assegurar a migração para a plataforma IDMC - *Intelligent Data Management Cloud* se faz necessária a atuação de forma contínua e estratégica de um profissional dedicado à CAIXA, garantindo governança, boas práticas e evolução da implantação.
- 7.2. As condições para o suporte técnico (TAM) estão descritas no ANEXO I-B- FORMA DE EXECUÇÃO.

**8. DIREITO DE USO DE SUBSCRIÇÃO DE SOFTWARE**

- 8.1. Direito de uso de subscrição de *Software as a Service* (SAS) é o contrato pelo qual o proprietário de um determinado software, ou seja, seu FABRICANTE, concede a outrem o direito de usá-lo por tempo determinado de forma não exclusiva.

**9. QUALIFICAÇÃO TÉCNICA**

- 9.1. Os requisitos de qualificação técnica estão descritos no ANEXO I-E - QUALIFICAÇÃO TÉCNICA.

**10. DA VIGÊNCIA DO CONTRATO**

- 10.1. O prazo de vigência contratual será de 24 (vinte e quatro) meses contados a partir da sua assinatura, podendo ser prorrogado, a critério da CAIXA, por sucessivos períodos nos limites definidos na Lei 13.303/2016.
- 10.2. O prazo de 24 (vinte e quatro) meses se justifica, por se tratar de serviços de suporte e migração.

**11. DA FORMA DE PAGAMENTO**

- 11.1. A CAIXA, após a execução dos serviços e o exato cumprimento das obrigações assumidas, efetuará o pagamento à CONTRATADA, de acordo com as condições estabelecidas no ANEXO I-B - FORMA DE EXECUÇÃO.

**12. PROPOSTA COMERCIAL**

- 12.1. O modelo de proposta comercial que deve ser enviado está disponível no ANEXO I-C - PROPOSTA COMERCIAL.

**13. REQUISITOS DE SEGURANÇA**

- 13.1. São os requisitos de atendimento obrigatórios pelo FABRICANTE do serviço em nuvem e pela CONTRATADA, devendo cada um observar o seu papel.
- 13.2. O detalhamento dos requisitos de segurança está disponível nos ANEXO I-D - SEGURANÇA EM NUVEM e ANEXO I-F - CLÁUSULAS DE REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES.

**ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS****1. CARACTERÍSTICAS GERAIS**

- 1.1. A CONTRATADA deverá fornecer, em modelo de subscrição, os produtos e serviços da plataforma de nuvem IDMC - *Informatica Intelligent Data Management Cloud*, disponibilizada como *Software as a Service* (SaaS).
- 1.2. O modelo de comercialização da solução IDMC, não prevê a possibilidade de contratação de serviços específicos.
- 1.2.1. Neste contexto, o contrato deverá permitir o consumo de todos os serviços disponíveis no IDMC, bem como o acesso a novas funcionalidades e serviços incorporados durante sua vigência.
- 1.3. O contrato deverá permitir o consumo de recursos disponíveis no *marketplace* da plataforma de integração de dados.
- 1.4. Todas as funcionalidades, *plug-ins* e extensões deverão estar integralmente disponíveis e licenciados para uso.
- 1.5. Considerando possíveis restrições de exportação de metadados, a solução deverá disponibilizar a base completa de dados e metadados em formato aberto e interoperável, permitindo sua migração para solução semelhante.
- 1.5.1. As informações são integralmente de propriedade da CAIXA, e a troca de plataforma poderá ocorrer a qualquer momento, a critério da CAIXA.
- 1.6. A solução deverá permitir a criação de ambientes *multitenancy* totalmente isolados, ficando a critério da CAIXA sua utilização.
- 1.6.1. Ainda assim, deverá possibilitar gestão centralizada e geração de relatórios consolidados contemplando todos os *tenants* criados.
- 1.7. Caso a CONTRATADA ou o provedor de computação em nuvem seja subsidiária brasileira de empresa estrangeira, deverá ser firmado acordo de confidencialidade entre a *holding* e a subsidiária nacional, garantindo que todas as informações da CAIXA sejam tratadas como confidenciais, sem compartilhamento com empresas do mesmo grupo econômico e sem uso para fins distintos dos contratados.

**2. REQUISITOS TÉCNICOS**

- 2.1. ALTA DISPONIBILIDADE:
  - 2.1.1. A solução deverá operar de forma ininterrupta 24x7, ou seja, 24 (vinte e quatro) horas ao dia e 7 (sete) dias por semana.
  - 2.1.2. Considerando que a CAIXA proverá os requisitos de rede, banco de dados e infraestrutura necessários à integração entre seu ambiente e a plataforma Informatica em nuvem, a solução deverá garantir disponibilidade mensal mínima de 99,0% (noventa e nove por cento).
  - 2.1.3. A solução deverá prever mecanismos de verificação do uso da capacidade contratada e emissão de alertas ao atingir limites definidos em função do orçamento disponível.
- 2.2. PROTOCOLOS E INTEROPERABILIDADE:

- 2.2.1. A autenticação de usuários deverá integrar-se à solução de gestão de acessos da CAIXA, utilizando os protocolos *OpenID Connect (OAuth 2.0)* ou *SAML 2.0*.
- 2.3. A solução deverá integrar-se a ferramenta antivírus para verificação dos arquivos recebidos, sem impacto no desempenho necessário ao cumprimento dos parâmetros de qualidade estabelecidos.
- 2.4. LEGAIS:
  - 2.4.1. A solução deverá estar aderente à LGPD (Lei nº 13.709/2018) e às demais legislações vigentes.
  - 2.4.2. Deverá estar alinhada ao disposto na Resolução CMN nº 4.893/2021, no que complementa a IN 05/GSI/PR.
  - 2.4.3. Deverá observar a Instrução Normativa GSI/PR nº 05 e a IN GSI/PR nº 08/2025, relativas ao uso de computação em nuvem em órgãos públicos.
- 2.5. IDIOMA:
  - 2.6. A solução deverá fornecer suas interfaces e relatórios em português do Brasil ou inglês dos Estados Unidos da América.
- 2.7. DOCUMENTAÇÃO:
  - 2.7.1. A CONTRATADA deverá disponibilizar documentação completa dos serviços, seus contextos de uso e formas de acesso.
  - 2.7.2. Deverá fornecer guia prático, preferencialmente com tour guiado e vídeos, em português do Brasil ou inglês dos Estados Unidos da América.
  - 2.7.3. Materiais de transferência de conhecimento deverão estar disponíveis em português do Brasil ou inglês dos Estados Unidos da América.
- 2.8. HISTÓRICO:
  - 2.8.1. A plataforma deverá registrar o histórico de todas as ações executadas pelos usuários, permitindo trilha de auditoria.
- 2.9. COMPATIBILIDADE E MIGRAÇÃO:
  - 2.10. A solução deverá identificar ativos existentes no *Informatica PowerCenter* e permitir sua migração automática, bem como o reaproveitamento de artefatos e lógicas.
  - 2.11. Deverá viabilizar migração direta (*lift-and-shift*), mantendo estrutura e configurações originais, de forma a permitir a reutilização das soluções construídas e em operação da CAIXA em versões anteriores.
  - 2.12. A solução deverá oferecer mecanismos de migração automatizada, com garantia de integridade e mínima intervenção manual, além de permitir gerenciamento unificado de ambientes locais e em nuvem.
  - 2.13. Deverá permitir, por meio de interface unificada, o gerenciamento centralizado de ambientes locais (*on-premise*) e nuvem (*cloud*), com atualizações e correções automáticas.
  - 2.14. Deverá possuir compatibilidade com ambientes *PowerCenter*, permitindo executar e gerenciar rotinas ETL - *Extract, Transform and Load* atualmente desenvolvidas e processadas no *Informatica PowerCenter*.
  - 2.15. Deverá possibilitar a execução, via plataforma de nuvem, sem a necessidade de modernização ou adaptação, garantindo a compatibilidade funcional e continuidade

dos negócios apoiados pelas rotinas atualmente suportadas pela ferramenta, com manutenção de suporte do fornecedor e do fabricante.

- 2.15.1. Fonte: INFORMATICA. *Getting Started with Cloud Data Integration for PowerCenter*. Disponível em: <<https://docs.informatica.com/integration-cloud/cloud-data-integration-for-powercenter/current-version/getting-started-with-cloud-data-integration-for-powercenter.html>>. Acesso em: 05 dez. 2025.

### **3. REQUISITOS FUNCIONAIS**

- 3.1. A solução deverá permitir a integração de dados multinuvem (*multicloud*) e local (*on-premise*).
- 3.2. Deverá conectar e integrar dados provenientes de múltiplas fontes, incluindo nuvens públicas, privadas e sistemas *on-premise*.
- 3.3. Deverá disponibilizar mecanismos de monitoramento da infraestrutura, dos ativos em execução e do consumo financeiro, garantindo visibilidade e controle operacional.
- 3.4. Deverá permitir administração centralizada e geração de relatórios personalizados.
- 3.5. O acesso via web deverá ser compatível com Google Chrome 137.0 ou superior e Microsoft Edge 142.0 ou superior.
- 3.6. Deverá permitir integração, por meio de API (*Application Programming Interface*) abertas, com ferramentas externas.
- 3.7. Deverá disponibilizar conectores nativos para bancos de dados, plataformas *Big Data*, serviços de nuvem e aplicações corporativas, incluindo SQL Server, DB2/zOS, IDMS, Oracle, Sybase, PostgreSQL, Spark, Google BigQuery, Salesforce, ServiceNow, Databricks, Bigquery, dentre outros.
- 3.8. Deverá permitir testes rápidos para identificar anomalias e validar dados.
- 3.9. A solução deverá apoiar desenvolvimento *low-code*, com configuração visual e uso de componentes e transformações pré-definidas (filtros, *joins*, *lookups*, ordenações etc.).

### **4. REQUISITOS NAO FUNCIONAIS**

- 4.1. A solução deverá ser escalável, permitindo ajustes dinâmicos e rápidos de infraestrutura, sem perda de desempenho e com otimização de custos.
- 4.2. É permitido uso de módulos, *plug-ins* e extensões, desde que nativamente integrados e aderentes às exigências de segurança.
- 4.3. Deverá garantir escalabilidade para futuras expansões, aquisição de novas ferramentas e aumento de projetos.
- 4.4. A solução deverá possuir alta capacidade de processamento, na ordem de *petabytes*.

### **5. SEGURANÇA**

- 5.1. A solução deve atender aos requisitos especificados nos documentos ANEXO I-D - SEGURANÇA EM NUVEM e ANEXO I-F - REQUISITOS DE SEGURANÇA PARA FORNECEDORES – SERVIÇOS EM NUVEM.

- 5.2. Deverá manter logs e trilhas de auditoria contendo, no mínimo: data, hora, usuário, artefato e tipo de modificação.
- 5.3. Deverá permitir geração de relatórios de auditoria.
- 5.4. Deverá permitir a configuração de perfis e autorizações por função ou grupo, garantindo segregação de acesso.
- 5.5. Deverá suportar autenticação por senha, SSO, certificado, *token* e MFA, incluindo restrições por IP confiável.
- 5.6. As credenciais deverão ser armazenadas de forma criptografada.
- 5.7. A solução deverá suportar criptografia em trânsito e em repouso.
- 5.8. Administradores deverão poder definir políticas de força e rotação de senhas.
- 5.9. Deverá oferecer suporte a provedores *SAML 2.0* e autenticação *OAuth 2.0* de curta duração.
- 5.10. Não deverá permitir alteração do *user ID* após a criação do usuário.
- 5.11. Todos os dados persistidos deverão utilizar criptografia AES-256 ou equivalente, permitindo rotação anual de chave e uso de chaves fornecidas pelo cliente.
- 5.12. A solução deverá aplicar patches de segurança de forma automática, sem interromper o funcionamento.
- 5.13. Deverá suportar armazenamento seguro de credenciais (ex.: *Secret Manager* ou *Vault externo*).
- 5.14. Deverá suportar conexões via *link* privado com nuvens públicas, impedindo exposição do tráfego à internet.

**6. RECURSOS DISPONÍVEIS NA SOLUÇÃO**

RECURSO	DESCRIÇÃO
Portal de Documentação do IDMC	Portal central com toda a documentação oficial do <i>Informatica</i> IDMC, incluindo guias de recursos, notas de versão, tutoriais passo a passo, requisitos técnicos por serviço (CDI, CAI, DQ, MDM), catálogos de conectores, instruções de instalação e operação do <i>Secure Agent</i> , exemplos de implementação e links para conhecimento e <i>white papers</i> .  <a href="https://docs.informatica.com/integration-cloud/cloud-data-integration/current-version/introduction/informatica-resources/informatica-documentation.html">https://docs.informatica.com/integration-cloud/cloud-data-integration/current-version/introduction/informatica-resources/informatica-documentation.html</a>
Cloud Data Integration (CDI)	Serviço de integração de dados em nuvem que permite desenhar e executar pipelines com transformações avançadas, conectores nativos para bancos de dados e aplicações SaaS, suporte a carga incremental, agendamento e orquestração, monitoramento e reproprocessamento, promoção entre ambientes (dev/test/prod) e integração com governança/linhagem.  <a href="https://docs.informatica.com/integration-cloud/data-ingestion-and-replication/current-version.html">https://docs.informatica.com/integration-cloud/data-ingestion-and-replication/current-version.html</a>

API & Application Integration (CAI)	<p>Camada para criar e expor APIs REST, orquestrar serviços e integrações em tempo real, suportar eventos e filas, autenticação (<i>OAuth/Key</i>), definição de contratos, políticas de <i>rate limiting</i>, rastreamento de chamadas e logs, além de integração com componentes de dados do IDMC.</p> <p> <a href="https://docs.informatica.com/ipaas/api-center.html">https://docs.informatica.com/ipaas/api-center.html</a>  <a href="https://docs.informatica.com/ipaas/api-manager.html">https://docs.informatica.com/ipaas/api-manager.html</a>  <a href="https://docs.informatica.com/ipaas/api-portal.html">https://docs.informatica.com/ipaas/api-portal.html</a>  <a href="https://docs.informatica.com/ipaas/application-integration.html">https://docs.informatica.com/ipaas/application-integration.html</a>  <a href="https://docs.informatica.com/ipaas/recipes.html">https://docs.informatica.com/ipaas/recipes.html</a> </p>
Data Quality e Governança	<p>Conjunto de capacidades para perfilamento de dados, definição e execução de regras de qualidade (validação, padronização, enriquecimento), medição de métricas, tratamento de exceções e suporte à linhagem e metadados para rastreabilidade ponta a ponta das origens, transformações e destinos.</p> <p> <a href="https://docs.informatica.com/data-governance-and-quality-cloud/data-quality/current-version.html">https://docs.informatica.com/data-governance-and-quality-cloud/data-quality/current-version.html</a>  <a href="https://docs.informatica.com/data-governance-and-quality-cloud/data-governance-and-catalog.html">https://docs.informatica.com/data-governance-and-quality-cloud/data-governance-and-catalog.html</a> </p>
MDM (SaaS)	<p>Master Data Management como serviço, fornecendo modelagem de entidades e relacionamentos, regras de correspondência, “deduplicação” e mesclagem, políticas de governança, publicação e consumo via serviços e integração com CDI/CAI para alimentar e distribuir dados mestres confiáveis.</p> <p> <a href="https://docs.informatica.com/master-data-management-cloud/reference-360-saas/current-version/reference-360.html">https://docs.informatica.com/master-data-management-cloud/reference-360-saas/current-version/reference-360.html</a> </p>
Conectores e Secure Agent	<p>Catálogo de conectores certificados para fontes de dados (bancos, data warehouses, SaaS), com requisitos de versão e driver, e o componente <i>Secure Agent</i> para mover dados de forma segura entre <i>on-premises</i> e cloud, suportando configuração de rede, <i>proxy</i>, alta disponibilidade, balanceamento de cargas e políticas de atualização.</p> <p> <a href="https://success.informatica.com/success-accelerators/overview-of-idmc-architecture.html">https://success.informatica.com/success-accelerators/overview-of-idmc-architecture.html</a>  <a href="https://docs.informatica.com/integration-cloud/data-ingestion-and-replication/current-version/connectors-and-connections.html">https://docs.informatica.com/integration-cloud/data-ingestion-and-replication/current-version/connectors-and-connections.html</a> </p>
Segurança / Compliance	<p>Diretrizes de segurança baseadas em responsabilidade compartilhada: identidade e acesso (RBAC, sub-organizações, SSO/SAML), criptografia em trânsito (TLS) e em repouso, gestão de chaves, segurança de metadados e persistência, conformidade com SOC1/2/3, HIPAA (quando aplicável) e alinhamento a NIST/ISO.</p> <p> <a href="https://trust.informatica.com/content/dam/informatica-trust/generic/2024_idmc_security_architecture_whitepaper.pdf">https://trust.informatica.com/content/dam/informatica-trust/generic/2024_idmc_security_architecture_whitepaper.pdf</a> </p>
CDI-PC (Cloud Data Integration – PowerCenter)	<p>Serviço que oferece compatibilidade com objetos do <i>PowerCenter</i>, permitindo migração, execução e gerenciamento de workflows e mappings legados no ambiente IDMC: permite migrar, executar e gerenciar workflows e mappings legados diretamente no IDMC, preservando lógica de sessões, parâmetros e transformações. Inclui ferramentas de importação de repositórios, execução em nuvem via <i>Secure Agent</i>, monitoramento, auditoria e integração com CDI/CAI e governança. Recurso permite execução de rotinas no legado <i>PowerCenter</i>, assim como acelerar a migração de ETL <i>on-premises</i> para cloud sem reescrita completa, reduzindo custo e tempo.</p>

	<a href="https://docs.informatica.com/integration-cloud/cloud-data-integration-powercenter/current-version.html">https://docs.informatica.com/integration-cloud/cloud-data-integration-powercenter/current-version.html</a>
Padrões & Melhores Práticas	<p>Documento com diretrizes para design e desenvolvimento, otimização de performance, configuração de agentes e ambientes, administração e troubleshooting, além de recomendações que acompanham novos recursos e versões do IDMC.</p> <p><a href="https://knowledge.informatica.com/s/article/IDMC-Best-Practices-and-Standard?type=external">https://knowledge.informatica.com/s/article/IDMC-Best-Practices-and-Standard?type=external</a></p>

**ANEXO I-B – FORMA DE EXECUÇÃO E SERVIÇOS AGREGADOS**

1. **SERVIÇOS DE SUPORTE TÉCNICO COM ATUALIZAÇÃO E MANUTENÇÃO TECNOLÓGICA**
- 1.1. Os serviços de suporte técnico têm por objetivo garantir a disponibilidade operacional da Solução.
- 1.2. O suporte técnico será prestado pela CONTRATADA em regime 24x7, ou seja 24 (vinte e quatro) horas ao dia e 7 (sete) dias por semana, incluindo feriados oficiais ou não, mediante a abertura de requisição (chamado) da CAIXA, nas condições e prazos estabelecidos neste edital.
- 1.3. Para o processo de modernização da plataforma haverá um time de especialistas dedicados à CAIXA e, após a migração da plataforma, os processos serão migrados com o apoio técnico da CONTRATADA.
- 1.4. O Suporte Técnico consiste na correção de falhas ou inconsistências detectadas de forma a garantir o pleno, correto e seguro funcionamento da Solução e de seus módulos ou componentes em produção, inclusive nas suas “implementações”, “customizações” e “parametrizações”, assim como na prestação de informações necessárias ao esclarecimento de dúvidas sobre o funcionamento da plataforma, afiançando sua perfeita operacionalização.
- 1.5. O Suporte Técnico compreende, ainda, a configuração dos componentes da Solução para o funcionamento integrado aos sistemas internos da CAIXA e a melhor utilização e maximização da plataforma nos ambientes *on-premise* e *cloud*, além de garantir:
  - 1.5.1. O acompanhamento do andamento (*status*) do chamado para a prestação de manutenção e suporte técnico, utilizando o GSC. A contratada terá o prazo de 180 (cento e oitenta) dias para implementar a solução para integração dos chamados, assim que solicitado pela CAIXA.
  - 1.5.2. A pesquisa em base de conhecimento com soluções para problemas conhecidos, incluindo alertas de produtos, comunicações de ciclo de vida (*end-of-life*) de produtos, instruções passo-a-passo de instalação de produtos, artigos técnicos, documentação de produtos e disponibilização de *patches*, como também informações relativas aos “*bugs*” documentados dos *softwares* que compõe a Solução.
- 1.6. Os serviços de suporte técnico com atualização e manutenção tecnológica abrangem, também, a prestação dos serviços adiante descritos:
  - 1.6.1. Manter a CAIXA sempre informada de todas as versões e atualizações disponibilizadas para uso, assim como das alterações, correções e vulnerabilidades dos componentes da solução.
  - 1.6.2. Atualização e fornecimento para a CAIXA de todas as novas versões, “*features*” e “*releases*” dos componentes da Solução que forem disponibilizadas durante a vigência do contrato, assim como o fornecimento de manuais e boletins técnicos com informações que assegurem a sua correta utilização.
  - 1.6.3. As novas versões e atualizações estáveis, correções (*patches*) e vulnerabilidades dos *softwares* que surgirem durante a vigência do contrato deverão ser repassadas

à CAIXA, na figura da GESTI - Gerência Nacional de Suporte de TI o prazo máximo de 5 (cinco) dias corridos a partir do seu lançamento e deverão ser disponibilizadas, pela Internet, acompanhadas de manuais ou boletins informativos das funcionalidades implementadas e procedimentos de instalação.

- 1.6.4. Para os produtos em nuvem, as atualizações serão oferecidas à CAIXA de maneira automática ou, quando cabível, lhe será oferecida a opção de determinar a melhor data para atualização do *software*, obedecendo janelas pré-estabelecidas. Todas as notificações são passadas por correio eletrônico aos contatos cadastrados.
- 1.6.5. Caso a CAIXA necessite haverá convocação de reuniões presenciais em Brasília durante a vigência do contrato para discussões dos problemas verificados no período e diagnósticos das Soluções adotadas, assim como para análise das opções de melhorias possíveis no ambiente CAIXA, visando a utilização máxima dos recursos disponíveis.

## **2. LÍDER TÉCNICO (TAM)**

- 2.1. Disponibilizar um profissional do fabricante por 08 (oito) horas por dia e 5 (cinco) dias semana, para desempenhar a função de líder técnico, para realizar as seguintes atividades:

Principais atividades:

- I. Ter visibilidade técnica das principais situações da CAIXA e garantir com o time interno as atividades necessárias para garantir disponibilidade do ambiente.
- II. Apoiar nas atividades de *health check* do ambiente da CAIXA, de forma a garantir as implementações das correções de *software* solicitadas.
- III. Atuar com o time técnico do cliente, garantindo entendimento das atividades do suporte e apoiar no plano de execução das atividades participando de todas as reuniões presenciais e remotas solicitadas pela CAIXA.
- IV. Apresentar plano de melhorias no que tange as atualizações de *software* existente no ambiente. Análise e recomendações de updates e patches críticos para garantir maior disponibilidade.
- V. Apoio técnico especializado na modernização e pós-migração da plataforma PowerCenter para IDMC.
- VI. Onboarding técnico e operacional da equipe da CAIXA, incluindo alinhamento de padrões e boas práticas.
- VII. Transferência de conhecimento técnico, com entrega de documentação e sessões práticas.
- VIII. Acompanhamento técnico dos chamados via GSC e realizar a confecção do relatório mensal de atendimento.
- IX. Execução de serviços conforme padrões acordados, com foco em qualidade e conformidade contratual.

## **3. SERVIÇO DE TRANSFERÊNCIA DE CONHECIMENTO**

- 3.1. A INFORMATICA disponibiliza uma plataforma de microaprendizagem chamada ([Success Portal](#)), que oferece treinamentos gratuitos e uma experiência a digital personalizada.

- 3.2. Como Suporte Premium é oferecida uma Biblioteca de Aprendizagem alinhada às datas de início e término dos Serviços de Suporte contratados ([Pesquisa da Biblioteca de Aprendizagem Premium Success](#)).
- 3.3. Também é possível acessar o INFORMATICA *MarterPass Education*, que inclui todos os eventos e cursos públicos oficiais da Informatica Education. Durante a vigência do contrato, o usuário tem direito a participar de qualquer aula pública em qualquer lugar do mundo, além de acessar cursos no formato *OnDemand* ou *eLearning* durante a vigência do contrato ([Universidade de Informática | Treinamento on-line da Informatica](#)).
- 3.4. Também estão disponíveis treinamentos sob demanda utilizando os TUs (*Training Units*), acessíveis por meio do catálogo de cursos da INFORMATICA, em formato de grupos privados. As aulas contarão com acesso ao ambiente e materiais didáticos desenvolvidos pela INFORMATICA.

### IDMC Training

Exemplos de cursos públicos / sessões virtuais com Instrutor e auto treinamento (On Demand).  
Laboratórios "hands on" e certificações

Treinamentos com INSTRUTOR	Treinamentos ON DEMAND	CERTIFICAÇÕES
<ul style="list-style-type: none"> <li>•Cloud Data Integration for Developers</li> <li>•Cloud Data Integration for Developers, Advanced</li> <li>•IDMC: Administration Fundamentals</li> <li>•Cloud Application Integration Services for Developers</li> <li>•Cloud Data Quality</li> <li>•Cloud Integration Hub Services</li> <li>•Cloud Reference 360: Manage Reference Data</li> <li>•Cloud Data Marketplace</li> <li>•Informatica Cloud B2B Gateway: Foundations</li> <li>•Cloud Data Governance and Catalog for Consumers</li> <li>•Cloud Data Governance and Catalog: Administration</li> <li>•Cloud Data Governance and Catalog: Data Stewardship &amp; Curation</li> <li>•Customer 360 SaaS for Business Users</li> <li>•Customer 360 SaaS: Manage Customer Data</li> <li>•Supplier 360 SaaS: Manage Supplier Data</li> <li>•Supplier 360 SaaS for Business Users</li> <li>•Product 360 SaaS: Manage Product Data</li> <li>•Product 360 SaaS for Business Users</li> <li>•Informatica Intelligent Data Management Cloud Overview</li> <li>•MDM SaaS: Manage Multidomain Data</li> <li>•Customer 360 SaaS for Developers</li> <li>•Product 360 SaaS for Developers</li> <li>•Supplier 360 SaaS for Developers</li> </ul>	<ul style="list-style-type: none"> <li>•Cloud Data Integration for Developers</li> <li>•Cloud Data Integration for Developers, Advanced</li> <li>•IDMC: Administration Fundamentals</li> <li>•Cloud Application Integration Services for Developers</li> <li>•Cloud Data Quality</li> <li>•Cloud Integration Hub Services</li> <li>•Cloud Data Governance Catalog for Consumers</li> <li>•Cloud Data Governance and Catalog: Curation and Discovery</li> <li>•Informatica Cloud B2B Gateway: Foundations</li> <li>•Cloud Data Marketplace</li> <li>•Customer 360 SaaS for Business Users</li> <li>•Informatica Cloud Platform Overview</li> <li>•IDMC: Advanced Serverless Environment</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Data Integration for Developers, Professional Certification</li> <li>• Cloud Data Quality, Professional Certification</li> <li>• Customer 360 SaaS R40 Developer, Professional Certification</li> <li>• Product 360 SaaS R40 Developer, Professional Certification</li> <li>• Supplier 360 SaaS R40 Developer, Professional Certification</li> </ul>

<sup>i</sup>Sessões e Certificados INFORMATICA

- 3.4.1. Após apresentação da necessidade da CAIXA para realização do treinamento, a contratada tem o prazo de 5 (cinco) dias úteis para encaminhar o Plano de Transferência de Conhecimento, detalhando o conteúdo, o cronograma, local de realização e quantidade de TUs que serão dedicadas e o formato (remoto ou presencial). O gestor operacional do contrato, poderá solicitar a reformulação da proposta, sugerir inclusões, exclusões.
- 3.4.2. O treinamento ministrado por um instrutor dedicado exclusivamente à demanda da CAIXA poderá atender até 12 (doze) participantes. Se a modalidade escolhida for presencial nas instalações da CAIXA, serão disponibilizadas 45 (quarenta e cinco) TUs por dia de treinamento. Para treinamentos no formato remoto, serão disponibilizadas 40 (quarenta) TUs por dia.
- 3.4.3. Caso a proposta não seja aprovada pela CAIXA, a CONTRATADA terá o prazo de 3 (três) dias para apresentar proposta ajustada conforme apontado pela CAIXA.
- 3.4.4. No último dia de treinamento a CONTRATADA solicitará aos participantes avaliação do repasse realizado.

- 3.4.5. Ao final dos repasses de conhecimento, a CONTRATADA deverá encaminhar à CAIXA a relação de frequência e a avaliação dos participantes e posteriormente a fatura.
- 3.4.6. A CAIXA emitirá em até 10 (dez) dias úteis após final da realização das atividades de transferência de conhecimento o ateste conforme solicitação da CONTRATADA.
- 3.4.7. Todos os documentos utilizados para a transferência de conhecimento devem ser disponibilizados em idioma português do Brasil.
- 3.4.8. Ao final de cada evento, os participantes com o mínimo de 80% (oitenta por cento) de presença deverão receber certificados de participação.
- 3.5. Caso o curso não atinja a avaliação mínima, geral e em suas subcategorias, como de nível satisfatório, a contratada deverá tomar providências de realização de nova transferência de conhecimento dentro de um prazo de até 45 (quarenta e cinco) dias.

#### **4. SERVIÇO TÉCNICO ESPECIALIZADO – HST (SOB DEMANDA)**

- 4.1. A contratação de um suporte especializado sob demanda visa assegurar uma migração segura e eficiente para a plataforma IDMC, contemplando a diversidade de sistemas que utilizam processos ETL. Esse serviço será executado por especialistas do fabricante, capazes de promover a modernização necessária e apoiar a evolução dos sistemas existentes, garantindo continuidade operacional e mitigação de riscos.
- 4.1.1. Atividades previstas para utilização das HST com Especialistas:
- Conversão de ativos e workflows para IDMC, garantindo compatibilidade e integridade dos processos especialmente para os sistemas legados.
  - Ajustes em sistemas legados com bancos de dados desatualizados; assegurando integração adequada e evolução.
  - Planejamento e execução da migração, com definição de estratégia e cronograma, elaboração da arquitetura de projeto de integração de dados
  - Instalação e configurações de agentes para comunicação entre ambientes *on-premise* e cloud.
  - Orientações sobre compatibilidade de versões, prevenindo falhas e garantindo aderência às melhores práticas;
  - Construção de novos mapas com plano de adoção das tecnológicas nas versões mais recentes.
  - Gerenciamento com equipes do fabricante, para alinhamento técnico e resolução de demandas complexas.
  - Suporte e Resolução de incidentes críticos, garantindo rápida recuperação e continuidade dos serviços.
  - Análise e correção de problemas relacionados à integração de sistemas, como foco em estabilidade e performance.
  - Atuação conjunta com TAM para governança técnica, acompanhamento estratégico e mitigação de riscos.
  - Consultoria/mentoria para a apresentação de boas práticas e diagnósticos dos perfis CAIXA com a utilização dos componentes de *softwares*.
- 4.1.2. A CONTRATADA terá o prazo de 72 (setenta e duas) horas para prestar o serviço a partir do acionamento da CAIXA.

- 4.1.3. A CONTRATADA deverá apresentar relatório técnico informando o serviço a ser realizado, técnicos especialistas envolvidos e números de horas trabalhadas no prazo de até 24 (vinte e quatro) horas do início do atendimento.
- 4.1.4. Os artefatos produzidos e disponibilizados pela CONTRATADA no atendimento dos serviços serão validados por equipe CAIXA visando a verificação da conformidade com padrões normativos, técnicos e metodológicos.
- 4.1.4.1. Caso não sejam atendidos os itens supracitados, os serviços já realizados pela CONTRATADA não surgirão efeitos junto à pagadora.
- 4.1.5. Após a execução dos serviços, a CONTRATADA deverá apresentar relatório técnico contemplando o número de horas efetivamente trabalhadas e o ateste do técnico da CAIXA responsável pelo acompanhamento dos serviços.
- 4.1.5.1. O relatório atestado subsidiará a CAIXA para aprovação dos serviços e efetivação do pagamento. As horas de suporte técnico especializado serão pagas sob demanda e a critério da CAIXA somente após a execução do serviço devidamente atestado.
- 5. **ATIVACÃO DA SOLUÇÃO – SERVIÇOS DE MIGRAÇÃO E IMPLANTAÇÃO DO IDMC**
- 5.1. A CONTRATADA deverá propor uma estratégia de ativação e migração para a arquitetura IDMC (*Intelligent Data Management Cloud*), em até 10 (dez) dias úteis a partir de solicitação formal da CAIXA.
- 5.2. Após aprovação da CAIXA em relação à estratégia proposta, a CONTRATADA deverá elaborar e apresentar, em até 15 (quinze) dias úteis, um plano de trabalho que será utilizado durante todo o processo de ativação e migração.
- 5.3. A migração ocorrerá conforme cronograma previamente acordado entre a CAIXA e a CONTRATADA, não ultrapassando o prazo máximo de 6 (seis) meses contados a partir da aprovação do plano de trabalho.
- 5.4. O serviço de ativação e migração consiste nas seguintes etapas:
  - 5.4.1. Estratégia para a integração com a nuvem (*cloudficação*).
  - 5.4.2. Estratégia de migração para os mapas mais prioritários a serem migrados para a nova arquitetura.
  - 5.4.3. Estratégia de migração para os mapas remanescentes.
  - 5.4.4. Definição de modelo de funcionamento, de forma concomitante, das soluções legada (Informatica Power Center) e nova (IDMC).
- 5.5. Durante o tempo em que as soluções estiverem coexistindo no ambiente da CAIXA, devem ser tomadas todas as medidas para que ocorra o menor impacto possível quanto ao desempenho das soluções em relação aos serviços que as utilizam.
- 5.6. Todos os recursos necessários para realizar a migração dos mapas da solução em uso na CAIXA para a nova solução, objeto desta especificação, deverão ser entregues à CAIXA pela CONTRATADA, sem nenhum ônus adicional.
- 5.7. Entende-se por recursos para migração as seguintes ações: alocação presencial ou remota de especialistas do fabricante durante todo o período de migração e o fornecimento dos *softwares* e serviços necessários à execução do processo de migração.

- 5.8. A alocação dos especialistas do fabricante durante o período de migração deverá ser previamente acordada com a CAIXA.
- 5.9. Possíveis entregas de *softwares* ou serviços adicionais para viabilizar a migração, deverão ser comunicadas previamente à CAIXA, de forma que haja reserva de recursos físicos e computacionais suficientes para instalação destes recursos.
- 5.10. A CAIXA poderá acionar a CONTRATADA para apoiar a migração de dados durante toda a vigência do contrato.
- 5.11. Após a migração e ativação da solução, a contratada deverá encaminhar o ateste dos serviços executados, juntamente com a solicitação de avaliação da nova plataforma à área técnica. Esta realizará a validade e ateste dos serviços prestados.

## **6. RAMPA DE ADOÇÃO**

- 6.1. Devido à necessidade de evolução prévia dos diversos ambientes atuais da CAIXA, o consumo dos IPU's contratados se dará, conforme a previsão abaixo, nos primeiros 6 (seis) meses de contrato:

MÊS DE CONTRATO	01	02	03	04	05	06
CONSUMO PREVISTO DE IPU's	0	0	0	369	738	1.476

- 6.2. Nos meses subsequentes, o consumo mensal previsto será de 2.951 (duas mil novecentas e cinquenta e uma) IPU's até o término do contrato.
- 6.3. Não haverá cobrança adicional, nos casos em que o consumo exceder o previsto de IPU's, conforme abaixo:
- 6.3.1. Em até 25% (vinte e cinco por cento) por 2 (dois) meses consecutivos.
- 6.3.2. Em até 25% (vinte e cinco por cento) por 3 (três) meses em um período de 5 (cinco) meses.
- 6.3.3. Em 100% (cem por cento) em qualquer 1 (um) mês.

## **7. OBRIGAÇÕES DA CONTRATADA**

- 7.1. São obrigações da CONTRATADA, além daquelas previstas nos demais anexos que compõem essa demanda:
- 7.1.1. Cumprir com as disposições constantes deste contrato e em seus anexos, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de qualquer condição aqui estabelecida.
- 7.1.2. Fornecer à CAIXA os nomes, endereços, telefones e endereço eletrônico (e-mail) do responsável pelo suporte.
- 7.1.3. Prestar os esclarecimentos que forem solicitados pela CAIXA e atender a eventuais solicitações e reclamações.
- 7.1.4. Recrutar os técnicos em seu nome e sob sua responsabilidade, sem qualquer solidariedade da CAIXA, cabendo-lhe efetuar todos os pagamentos, inclusive os relativos aos encargos previstos na legislação trabalhista, previdenciária e fiscal, bem como de seguros e quaisquer outros decorrentes de sua condição de empregadora assumindo todas as despesas relativas a pessoal e quaisquer outras oriundas, derivadas ou conexas com o contrato, ficando ainda, para todos os efeitos

legais, declarados pela CONTRATADA a inexistência de qualquer vínculo empregatício entre seus empregados e prepostos e a CAIXA.

- 7.1.5. Disseminar periodicamente ao seu corpo funcional, as orientações passadas pela CAIXA de seus Procedimentos e Padrões internos.
- 7.2. Executar os serviços de acordo com os Procedimentos e Padrões definidos de comum acordo, no início das atividades.
- 7.3. Diligenciar, no sentido de que os seus técnicos, ou de empresas subcontratadas, portem obrigatoriamente, a respectiva identidade funcional, quando do atendimento à CAIXA, apresentando-se, preferencialmente à Gerência da unidade antes do início do atendimento.
- 7.3.1. Encaminhar periodicamente e sempre que ocorrer exclusão ou inclusão de técnicos para atendimento a CAIXA, expediente às unidades de tecnologia da CAIXA, informando os nomes dos técnicos que estão autorizados a executar os serviços contratados.
- 7.4. Manter, sob as penas da lei, o mais completo e absoluto sigilo e não fazer uso sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais dos materiais da CAIXA de que porventura venha a ter conhecimento, acesso ou que lhe venham a ser confiados, sejam relacionados ou não com o fornecimento objeto do contrato, no desempenho de suas atividades relativas a este contrato, sob pena de ressarcir à CAIXA todo e qualquer prejuízo diretamente causado pela divulgação ou uso indevido da informação.
- 7.5. Verificar, durante as visitas para atendimento de chamados, os *softwares*, recomendando à CAIXA qualquer ação corretiva necessária.
- 7.6. Fiscalizar o cumprimento do objeto deste contrato, cabendo-lhe integralmente os ônus decorrentes, fiscalização essa que se dará independentemente da que será exercida pela CAIXA.
- 7.7. Pagar todos os impostos e taxas devidos sobre os serviços objeto deste contrato, bem como as contribuições à previdência social, encargos trabalhistas, prêmios de seguro e acidentes de trabalho, emolumentos, quaisquer insumos e outras despesas diretas e indiretas que se façam necessárias à execução dos serviços contratados.
- 7.7.1. Tomar todas as providências e realizar as obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrências da espécie, forem vítimas os seus empregados, no desempenho dos serviços ou em conexão com eles, ainda que verificados nas dependências da CAIXA.
- 7.7.2. Prestar todo o suporte técnico necessário à solução de problemas no *software*, inclusive, comparecimento com pontualidade em horário previamente agendado quando em atendimento conjunto com terceiros indicados pela CAIXA no intuito de detectar as causas dos problemas e solucioná-los.
- 7.8. Fazer constar nas faturas apresentadas o número do processo e o mês de competência a que se refere o documento.
- 7.8.1. Dar ciência à CAIXA, imediatamente e por escrito, de qualquer anormalidade que verificar quando da execução do contrato.
- 7.8.2. Dispor-se a toda e qualquer fiscalização da CAIXA, no tocante à prestação do serviço, assim como ao cumprimento das obrigações previstas neste Contrato e em seus anexos.

- 7.8.3. Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento objeto deste contrato, inclusive considerados os casos de greve ou paralisação de qualquer natureza.
- 7.8.4. Responder por todo e qualquer dano que causar à CAIXA ou a terceiros, ainda que culposos, praticado por seus prepostos, empregados ou mandatário, não excluindo ou reduzindo essa responsabilidade à fiscalização ou acompanhamento pela CAIXA.
- 7.8.5. Estruturar-se de modo compatível e prover os recursos necessários ao fornecimento objeto deste contrato, conforme especificado neste instrumento.
- 7.8.6. Diligenciar para que os seus empregados tratem com urbanidade o pessoal da CAIXA, clientes, visitantes e demais contratados.
  - 7.8.6.1. Não permitir que seus empregados executem serviços além dos previstos no objeto deste contrato.
- 7.9. Indenizar todos os custos financeiros que porventura venham a ser suportados pela CAIXA por força de sentença judicial que reconheça a existência de vínculo empregatício entre a CAIXA e os empregados da CONTRATADA.
- 7.10. Até que ocorra a integração da ferramenta para abertura dos chamados, em caso de indisponibilidade da ferramenta da CAIXA, ou em casos em que a CAIXA julgar pertinente, outras formas de abertura, consulta e tratamento dos chamados poderão ser utilizadas.
  - 7.10.1. Nesses casos, poderão ser efetuados chamados por telefone, Internet, correio eletrônico, central de atendimento da CONTRATADA, com atendimento em português, que atende à Unidade Operacional da CAIXA solicitante do serviço.
- 7.11. A CONTRATADA deverá iniciar o atendimento ao chamado da CAIXA para prestar os serviços de suporte técnico, nos prazos estabelecidos neste documento, a serem contabilizados de forma corrida a partir da abertura do chamado.
- 7.12. O termo, forma corrida, indica que a contagem de tempo se dará de maneira contínua sem interrupções, exceto aquelas que sejam provocadas pela CAIXA.
- 7.13. A solução operacional ao problema técnico deverá ser concluída nos prazos estabelecidos neste documento.
  - 7.13.1. Entende-se como solução operacional, a disponibilidade da solução, porém de forma paliativa ou temporária.
- 7.14. A qualidade dos serviços será aferida na forma estabelecida no Cálculo do Nível de Serviço deste termo de referência.
- 7.15. A CONTRATADA compromete-se a realizar a conclusão dos chamados no instante da resolução definitiva do serviço de atendimento, sendo que esta conclusão deverá ser executada diretamente pelo técnico ou pela Central de Atendimento da CONTRATADA, mediante interface com o Sistema de Atendimento da CAIXA.
- 7.16. A CONTRATADA deverá disponibilizar acesso às informações relativas a problemas (*bugs*) documentados pelo fabricante e à documentação referente aos produtos e componentes especificados neste documento.
  - 7.16.1. Disponibilizar acesso à documentação, por meio da internet, sem custos adicionais.

- 7.17. A CONTRATADA deverá analisar e recomendar a aplicação de updates, fixes, alertas de segurança e patches críticos, garantindo maior disponibilidade dos produtos.
- 7.18. A CONTRATADA disponibilizará um Líder Técnico que terá a responsabilidade pela qualidade do serviço prestado, pelo acompanhamento dos chamados, pela emissão e entrega do relatório mensal de atividades executadas e participação nas reuniões de mudanças e em reuniões executivas.
- 7.19. Todos os termos constantes deste item deverão ser obedecidos durante toda a vigência do contrato.
- 7.20. A Critério da CAIXA, os chamados poderão ser abertos, acompanhados e fechados por equipe própria ou terceirizada.

**8. FORNECIMENTO DE RELATÓRIO CONSOLIDADO DOS CHAMADOS**

- 8.1. A CONTRATADA deverá fornecer, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico, formato planilha e em português, relatório detalhado sobre as atividades prestadas contendo dados gerenciais e estatísticos pertinentes à gestão dos serviços relativos ao mês anterior, incluindo obrigatoriamente os campos e informações abaixo.
- 8.2. A CONTRATADA deverá fornecer, mensalmente, até o 5º (quinto) dia útil do mês subsequente à prestação do serviço, em meio eletrônico, formato planilha e em português, relatório detalhado sobre as atividades prestadas contendo dados gerenciais e estatísticos pertinentes à gestão dos serviços relativos ao mês anterior, incluindo obrigatoriamente os campos e informações abaixo.
- 8.2.1. Para cada chamado aberto no mês de referência:
- Data/hora da abertura do chamado técnico;
  - Identificação do *software* relacionado;
  - Identificação da localidade e da unidade da CAIXA responsável pela abertura e acompanhamento de cada chamado;
  - Severidade do chamado;
  - Número de identificação do chamado;
  - Descrição da situação da falha ou dúvidas relacionadas;
  - Data/hora do início do atendimento;
  - Data/hora da conclusão da solução operacional;
  - Detalhamento do tempo em que o chamado ficou aguardando ações da CAIXA para o seu andamento (tempo de responsabilidade da CAIXA);
  - Descrição da solução implantada.
- 8.2.2. Consolidado de chamados em tratamento no mês e que não foram solucionados:
- Data/hora da abertura do chamado;
  - Identificação do software relacionado;
  - Identificação da localidade e da unidade da CAIXA responsável pela abertura e acompanhamento de cada chamado;
  - Nome do empregado da CAIXA responsável pela abertura do chamado e acompanhamento de cada chamado;
  - Severidade do chamado;
  - Número de identificação do chamado;
  - Descrição da situação da falha ou dúvidas relacionadas;
  - Data/hora do início do atendimento.

8.2.3. Consolidado dos chamados que não atenderam os prazos estabelecidos neste termo com as devidas justificativas para o descumprimento dos prazos contratados:

- Data e hora da abertura do chamado técnico;
- Identificação do software relacionado;
- Identificação da localidade e da unidade da CAIXA responsável pela abertura e acompanhamento de cada chamado;
- Severidade do chamado;
- Número de identificação do chamado;
- Descrição da situação da falha ou dúvidas relacionadas;
- Data/hora do início do atendimento;
- Data/hora da conclusão da solução operacional;
- Tempo de atraso do chamado;
- Detalhamento do tempo em que o chamado ficou aguardando ações da CAIXA para o seu andamento (tempo de responsabilidade da CAIXA);
- Descrição da solução implantada;
- Explicação ou justificativa para o descumprimento do prazo contratado.

8.2.4. Tais relatórios são obrigações contratuais sujeitas às sanções previstas no item correspondente deste documento (Cálculo do Nível de Serviço), os quais deverão ser entregues nas mesmas localidades em que o serviço for prestado, indicadas no corpo deste documento.

## **9. CONSIDERAÇÕES GERAIS**

9.1. A prestação de serviços de suporte deverá ser efetuada pela CONTRATADA ou pelo FABRICANTE da solução.

9.2. O acesso dos técnicos da contratada ou do fabricante dos produtos licenciados aos ambientes da CAIXA somente será admitido com prévia autorização e com observância aos padrões de segurança vigentes.

9.3. O acesso às informações do ambiente computacional, objeto do serviço ora contratado, por intermédio de relatórios, *logs*, diagramas ou configurações e por meio de telefone ou eletronicamente, só será permitido quando cabível, com autorização expressa da CAIXA.

9.4. Todo serviço de suporte técnico deverá ser executado somente mediante prévia autorização da CAIXA, com informações claras dos procedimentos que serão adotados ou executados, nos horários estabelecidos pela CAIXA.

9.4.1. As exceções serão pontualmente tratadas pela CAIXA.

9.5. O acesso às informações do ambiente computacional da CAIXA, a partir das instalações da CONTRATADA só será efetuado quando for possível restringir tal acesso apenas ao recurso objeto da contratação e em situações expressamente autorizada pela CAIXA, obedecendo aos padrões em vigência na CAIXA.

9.6. Para realização dos serviços especificados neste anexo, a CONTRATADA poderá utilizar ferramentas (*software* aplicativo) de sua propriedade, desde que autorizado pela CAIXA e destinado a facilitar a execução dos serviços e diagnósticos de problemas, sem ônus adicionais para a CAIXA.

9.7. Despesas relativas a eventuais deslocamentos de pessoal técnico, que se fizerem necessárias para a correção de problemas técnicos e adequações ou ajustes de configurações, são de exclusiva responsabilidade da CONTRATADA.

## **10. ATENDIMENTO**

- 10.1. A CONTRATADA deverá obrigatoriamente na abertura do chamado utilizar o número do chamado gerado pelo sistema de atendimento CAIXA BMC/ITSM.
- 10.1.1. Caso não seja possível a abertura de chamado pelo sistema de atendimento CAIXA, a abertura de chamado poderá ocorrer pelos canais de atendimento da contratada, gerando um número de atendimento provisório.
- 10.1.2. No retorno do sistema de atendimento CAIXA, deverá ser gerado um novo número para o chamado que será substituído pelo número provisório gerado anteriormente.
- 10.2. A CONTRATADA deverá disponibilizar central de atendimento única que possua capacidade de recebimento e emissão automática de chamados (*trouble-tickets*), para possibilitar comunicação com a ferramenta de gestão de serviços da CAIXA (GSC – BMC/ITSM), de modo a permitir a implementação de sistemática de troca de mensagens eletrônicas Webservices, protocoladas entre a CAIXA e a CONTRATADA e entre CONTRATADA e a CAIXA para abertura, fechamento e atualização da situação do chamado.
- 10.2.1. Cabe à CONTRATADA prover a comunicação da sua central de atendimento com a da CAIXA, de modo que a abertura do chamado e seu respectivo fechamento sejam gerenciados pela ferramenta de gestão de serviços da CAIXA, sem ônus adicionais, cabendo ainda, à CONTRATADA, os custos dessa conexão.
- 10.2.2. A abertura dos chamados, como regra, dar-se-á pela integração de ferramentas eletrônicas.
- 10.3. A CONTRATADA deverá disponibilizar central de atendimento para abertura e registro dos chamados técnicos em regime de funcionamento de 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, todos os dias do ano.
- 10.4. Em situação de contingência e, ou até a entrega da integração das ferramentas eletrônicas, deverá ser previsto central de atendimento da CONTRATADA, a disponibilização de número telefônico, mensagens eletrônicas de e-mail ou página de abertura de chamado na Internet.
- 10.4.1. A CONTRATADA deverá informar, em até 05 (cinco) dias úteis, após a assinatura do contrato, pelo menos uma CAIXA postal para acionamento e recebimento de mensagem eletrônica e um número de telefone para contingenciamento em caso de indisponibilidade da Central de Atendimento.
- 10.5. A CONTRATADA deverá iniciar o atendimento ao chamado da CAIXA para prestar os serviços de suporte técnico, nos prazos estabelecidos neste documento, a serem contabilizados de forma corrida a partir da abertura do chamado.
- 10.6. O termo, forma corrida, indica que a contagem de tempo se dará de maneira contínua sem interrupções, exceto aquelas que sejam provocadas pela CAIXA.
- 10.7. A qualidade dos serviços será aferida na forma estabelecida no item correspondente deste documento (Cálculo do Nível de Serviço).
- 10.8. A CONTRATADA deverá disponibilizar acesso à documentação do fabricante, com:
  - 10.8.1. Acesso às informações relativas a problemas (*bugs*) documentados pelo fabricante.
  - 10.8.2. Disponibilizar acesso à documentação, por meio da internet, sem custos adicionais.
- 11. **PRAZOS DE ATENDIMENTO E RESOLUÇÃO DOS CHAMADOS**
- 11.1. Descrição da Severidade dos chamados:

SEVERIDADE	DESCRIÇÃO
1 – Crítica	O <i>Software</i> não está operante e não é possível nenhuma solução de contorno viável. Problema no <i>Software</i> que gera <b>indisponibilidade</b> em sistemas ou serviços produtivos que dependem desse produto.
2 – Alta	Problema no <i>Software</i> que gera impacto em <b>determinados</b> sistemas ou serviços produtivo que dependem desse produto.
3 – Média	Problema contornável que <b>não</b> gera qualquer impacto aos sistemas ou serviços produtivos que dependem desses ativos.
4 – Baixa	Esclarecimento de dúvidas ou consultas técnicas sobre o produto.

## 12. CÁLCULO DO NÍVEL DE SERVIÇO (SLA)

- 12.1. O Nível de Serviço é um indicativo de qualidade da prestação do serviço.
- 12.2. A qualidade da prestação de serviços será apurada por meio de Indicadores, cuja finalidade é garantir o atendimento aos chamados, bem como a sua priorização.
- 12.3. Os descontos serão cumulativos para cada dia, hora ou fração de atraso de cada chamado fechado no mês de referência de acordo com sua severidade e deverão ser concedidos na fatura do mês seguinte ao período de apuração.
- 12.4. Para o último mês de vigência do contrato a apuração deverá ser antecipada de maneira que os descontos sejam contemplados na última fatura do contrato.

INDICADORES DE NÍVEL DE SERVIÇO				
INDICADOR	DESCRIÇÃO	SEVERIDADE	META	PENALIDADE
<b>Tempo Máximo de Início de Atendimento</b>	Tempo entre a abertura do chamado no GSC e o início do atendimento	Severidade 1	<30 min	0,3% (zero vírgula três por cento) de desconto sobre o valor da fatura mensal, por cada hora de atraso de cada chamado ou fração de hora.
		Severidade 2	<1 hora	
		Severidade 3	<2 horas	
		Severidade 4	<4horas	
<b>Tempo Máximo de Solução Operacional</b>	Tempo para restabelecimento funcional da solução após incidente / esclarecimento de dúvida	Severidade 1	<12 horas	0,4% (zero vírgula quatro por cento) de desconto sobre o valor da fatura mensal, por cada hora de atraso de cada chamado ou fração de hora.
		Severidade 2	<24 horas	
		Severidade 3	<36 horas	
		Severidade 4	<72 horas	

<b>Entrega dos Relatórios Mensais</b>	Relatórios de chamados e atividades entregues até o 5º dia útil do mês subsequente à prestação do serviço	<b>100% (cem por cento)</b>	0,1% (zero vírgula um por cento) de desconto sobre o valor da fatura mensal, por cada dia de atraso.
<b>Execução de Treinamentos</b>	Realização dos treinamentos solicitados dentro do prazo acordado e com avaliação igual ou acima de BOM pelos participantes	<b>100% (cem por cento) de acordo com a demanda CAIXA</b>	0,05% (zero vírgula zero cinco por cento) de desconto sobre o valor da fatura do treinamento, por cada dia de atraso.  Retenção de 50% (cinquenta por cento) do valor caso os participantes avaliem abaixo de BOM
<b>Observação:</b> A meta de severidade é incluída apenas pela equipe CAIXA na abertura do chamado no GSC, qualquer alteração realizada posteriormente deve ser desconsiderada para medir os serviços prestados.			

<b>INDICADORES DE NÍVEL DE SERVIÇO PARA MIGRAÇÃO (ON-PREMISE PARA CLOUD)</b>			
<b>INDICADOR</b>	<b>DESCRIÇÃO</b>	<b>META</b>	<b>PENALIDADE</b>
<b>Entrega da Estratégia de Migração</b>	Documento com abordagem técnica e cronograma	Até 10 dias corridos após solicitação CAIXA	0,1% (zero vírgula um por cento) de desconto sobre o valor da ordem de serviço, por cada dia de atraso
<b>Entrega do Plano de Trabalho</b>	Plano detalhado com fases, recursos e riscos	Até 15 (quinze) dias úteis após aprovação da estratégia.	0,15% (zero vírgula quinze por cento) de desconto sobre o valor da ordem de serviço, por cada dia de atraso

<b>Execução da Migração</b>	Conclusão da migração de todo o escopo acordado	Até 12 (doze) meses após o início da execução	0,2% (zero vírgula zero dois por cento) de desconto sobre o valor da ordem de serviço, por cada dia de atraso
<b>Disponibilidade e durante e convivência</b>	Garantia de operação simultânea dos ambientes	Meta: > 99% (noventa e nove por cento) $**DISPONIBILIDADE = \left(1 - \frac{TTI}{TM}\right) \times 100$ TTI: Tempo Total de Interrupção do Serviço; TM: Total de Minutos no Mês;	0,02% (zero vírgula zero dois por cento) de desconto, caso não seja garantida a disponibilidade e acordada, no valor global do contrato.
<b>Satisfação do usuário final com o uso da nova Plataforma</b>  <b>CSAT (Customer Satisfaction Score)</b>	Avaliação dos usuários após a migração e/ou uso da nova plataforma	*Meta > 80% (oitenta por cento) $CSAT(\%) = \left( \frac{N^{\circ} \text{ de respostas positivas ao questionário}}{N^{\circ} \text{ total de respostas}} \right) \times 100$	Plano de ação corretiva obrigatório se a média for inferior a 80% (oitenta por cento) e 0,1% (zero vírgula um) de desconto sobre o valor da fatura mensal até a próxima avaliação satisfatória.
<b>Observação:</b> *Serão consideradas positivas as respostas correspondentes aos dois últimos níveis de cada pergunta do questionário Anexo XI. Para o cálculo de SLA o tempo sob responsabilidade da CAIXA, deve ser desconsiderado como tempo em atraso.			

- 12.5. Para todos os chamados classificados com severidades 1, 2 e 3, quando pendentes de solução operacional por mais tempo do que o estipulado neste documento, além do tempo de resolução, será aplicada uma multa de 0,5% (zero vírgula cinco) ao dia sobre o valor da fatura mensal, contada em dobro a partir do 5º (quinto) dia de atraso, podendo motivar a rescisão contratual após o 10º (décimo) dia de atraso.

- 12.6. Para todos os chamados classificados com Nível 4, dentro do mesmo mês, quando pendentes de resposta por mais de 96 (noventa e seis) horas além do tempo de resolução, será aplicada uma multa de 0,1% (zero vírgula um) ao dia sobre o valor da fatura mensal.

**13. LOCAL DE EXECUÇÃO E PRESTAÇÃO DE SUPORTE**

- 13.1. O atendimento ao chamado da CAIXA para prestação do serviço de suporte e, ou manutenção corretiva para reparação de eventuais falhas no software, configuração e parametrização que apresentarem defeito, será efetuado nas localidades abaixo relacionadas, nos prazos estabelecidos para cada indicador e com apresentação de laudo técnico para os casos que assim requererem:

UNIDADE	ENDEREÇO	CIDADE
CEPIP/CEMOT	SEPN 512, Cj. C – Lotes 09/10 Ed. José Alencar	Brasília/DF
CESOA/CESOB	SAUS Quadra 3 LT 3/4 12 Andar – Ala Norte	Brasília/DF
RESOA/RJ RESOB/RJ	Av Marrecas, 20 - Torre 3 - 13/14 Andar	Rio de Janeiro/RJ
REPIP/RJ	Av Marrecas, 20 - Torre 3 - 5 Andar	Rio de Janeiro/RJ
REPIP/SP	Av Dr. Martin Luther king, 762. Jd. Santo Antoninho	Osasco/SP
RESOA/SP RESOB/SP	Av Guido Caloi, 1000 Bl 9 2 Andar, Jardim São Luis	São Paulo/SP
CESTI	SEPN 512, Cj. C – Lotes 09/10 Ed. José Alencar	Brasília/DF
	SIG Quadra 01, Lote 685/805	Brasília/DF
	Datacenter CAIXA - Parque Capital Digital	Brasília/DF

- 13.2. Em situação de contingência, ou configurando-se qualquer ocorrência pontual que se apresentem, os serviços poderão ser prestados em outro local, nas cidades de Brasília, Rio de Janeiro ou São Paulo, a pedido da CAIXA, e, em caso de alteração definitiva de local de prestação dos serviços, a CONTRATADA será comunicada antecipadamente.

**14. DEMAIS OBRIGAÇÕES DA CONTRATADA**

- 14.1. Caberá à CONTRATADA dimensionar corretamente suas equipes, de forma a cobrir todos os turnos de trabalho, de acordo com o volume de demandas e atendimentos, mantendo a qualidade e os níveis de serviços exigidos, bem como os clientes, usuários e parceiros assistidos sob todos os aspectos.
- 14.2. Para execução dos serviços, a CONTRATADA deverá disponibilizar equipe técnica plenamente capacitada para executar as atividades dentro dos prazos previstos.
- 14.3. Todo o conhecimento adquirido ou desenvolvido, bem como toda informação produzida e utilizada para a execução dos serviços contratados, deverá ser

disponibilizado pela CONTRATADA à CAIXA ou empresa por ela designada durante a execução do contrato.

- 14.4. Todos os custos referentes ao fornecimento da solução e à prestação dos serviços contratados serão de responsabilidade exclusiva da CONTRATADA.
- 14.5. A CONTRATADA deverá participar, sempre que solicitado pela CAIXA, de pesquisa para avaliação do desempenho da execução contratual.
- 14.5.1. A pesquisa poderá abordar qualidade dos serviços, qualificação dos profissionais, aspectos de negociação, definição de cumprimento das ações de melhoria, satisfação geral e outros aspectos relevantes relativos ao contrato.
- 14.5.2. A CONTRATADA receberá informação do conceito obtido e, conforme ponderação, ficará obrigada a apresentar Plano de Melhoria, que deverá ser homologado pela CAIXA, propondo melhorias objetivas com prazos determinados, visando elevar os conceitos a níveis aceitáveis.
- 14.6. A CONTRATADA deve estar disponível para reuniões, durante a vigência do contrato, sempre que a CAIXA requisitar.
- 14.7. Considerando que o objeto contratual contempla uma solução de mercado, durante o período de vigência do contrato, a CONTRATADA deverá implementar todas as atualizações e melhorias de versão da ferramenta, ainda que elas não tenham sido propostas ou sugeridas pela CAIXA.

**15. RESPONSÁVEL PELO ACOMPANHAMENTO DO CONTRATO**

- 15.1. Unidades gestoras e seus endereços:
  - 15.1.1. GESTI – GN SUPORTE TI  
Endereço: SETOR SAUS QUADRA 3 BLOCO E 8º ANDAR  
Bairro: ASA SUL  
Brasília/DF  
CEP: 70.070-030
  - 15.1.2. CESTI – CN Suporte de TI  
Endereço: SEPN 512, Cj. C – Lotes 09/10 Ed. José Alencar  
Bairro: ASA NORTE  
Brasília/DF  
CEP 70.760-500
  - 15.1.3. CEGTI - CN Governança de TI  
Endereço: Quadra SEPN512 CJT C Lote 9/10 4º Andar  
Bairro: Asa Norte Brasília/DF  
CEP 70760-500

**16. TI VERDE**

- 16.1. Ao prestar os serviços, a CONTRATADA deverá, sempre que possível, priorizar a aquisição e utilização de insumos, produtos e serviços com adicionalidades socioambientais, tais como: reciclados, recicláveis, ecoeficientes, biodegradáveis, baixa intensidade de utilização de recursos naturais, emissão de gases de efeito estufa e exigir comprovação de origem ambientalmente regular dos recursos naturais utilizados.
- 16.2. O manejo e o transporte de peças deverão pautar a utilização de embalagens sustentáveis e recicláveis.

- 16.3. A CONTRATADA é responsável pelo recolhimento e descarte direcionado à reciclagem das embalagens e, quando autorizadas pela CAIXA, das peças substituídas, em conformidade com a Lei 12.305/2010 (Política Nacional de Resíduos Sólidos).

**17. PLANO DE GESTÃO E FISCALIZAÇÃO**

- 17.1. A Contratada fica obrigada a participar de pesquisa de 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 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.

- 17.2. Quando necessário, a CESTI - Centralizadora Nacional de Suporte de TI realizará, durante a vigência da garantia, a análise de desempenho quanto à entrega e qualidade dos serviços prestados.

- 17.2.1. Caberá à centralizadora elaborar e estruturar os itens de avaliação e metodologia de apuração, apresentando o resultado do desempenho nas seguintes categorias:

- Péssimo;
- Ruim;
- Mediano;
- Bom;
- Excelente.

- 17.3. 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 igual a “mediano” ou categoria inferior.

- 17.4. A CESTI elaborará em conjunto com a CONTRATADA um plano de melhoria para as categorias com baixa avaliação, devendo ser entregue no prazo de até 15 dias úteis, com aplicação imediata das medidas voltadas às correções necessárias.

- 17.5. 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.

- 17.6. 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.

- 17.7. A CESTI realizará nova pesquisa após 30 (trinta) dias corridos de início da aplicação do plano de melhorias.

- 17.8. O não atendimento deste item e subitens configura descumprimento de obrigação contratual, com aplicação de multa de 0,5% (zero vírgula cinco por cento) sobre o valor global do contrato.

**18. INFORMAÇÕES PARA ELABORAÇÃO DA MINUTA CONTRATUAL**

- 18.1. OBRIGAÇÕES DA CONTRATADA:

- 18.1.1. Responsabilizar-se por eventuais prejuízos decorrentes do descumprimento de qualquer condição estabelecida, obrigando-se a indenizar a CAIXA, mesmo em caso de ausência ou omissão de fiscalização de sua parte. A responsabilização estender-se-á aos danos causados a terceiros.
- 18.1.2. Recrutar e contratar mão-de-obra especializada, em seu nome e sob sua responsabilidade, sem qualquer solidariedade da CAIXA, cabendo-lhe efetuar todos os pagamentos, inclusive os relativos aos encargos previstos na legislação trabalhista, previdenciária e fiscal, bem como de seguros e quaisquer outros decorrentes da sua condição de empregadora, assumindo, ainda, com relação ao contingente alocado, total responsabilidade pela coordenação e supervisão dos encargos administrativos, tais como: controle, fiscalização e orientação técnica, controle de frequência, ausências permitidas, licenças autorizadas, férias, punições, admissões, demissões, transferências e promoções.
- 18.1.3. Adotar o Padrão Tecnológico CAIXA, promovendo todas as ações necessárias para torná-la adequada com este padrão, podendo ser revisto e atualizado a critério da CAIXA.
- 18.1.4. Participar de reuniões técnicas ou gerenciais de Ponto de Controle, presenciais ou remotas, a critério da CAIXA, prestando esclarecimentos às equipes CAIXA sobre questões relativas à documentação, adequações e integrações solicitadas.
- 18.1.5. Manter seu corpo técnico atualizado em relação às tecnologias, normas e metodologias adotadas pela CAIXA, capacitando às suas expensas os profissionais envolvidos na execução dos serviços.
- 18.1.6. Os profissionais alocados para a prestação do serviço deverão apresentar a qualificação técnica conforme natureza do serviço.
- 18.1.7. Prestar apoio técnico à sua equipe, durante toda execução dos serviços, garantindo a qualificação necessária dos profissionais alocados, respeitando os perfis e qualificações definidos no contrato e anexos.
- 18.1.8. Atuar em todas as fases/etapas dos serviços para os quais foi CONTRATADA, avaliando o seu desenvolvimento e promovendo ações que assegurem os resultados esperados pela CAIXA.
- 18.1.9. Garantir a conformidade dos produtos construídos em relação aos requisitos funcionais, ou quaisquer outros requisitos, normas, padrões ou processos fornecidos pela CAIXA.
- 18.1.10. Manter a CAIXA sempre informada de todas as versões e atualizações disponibilizadas para uso, assim como das alterações, correções e vulnerabilidades dos *softwares*, obedecendo aos prazos estabelecidos.
- 18.1.11. Entregar o serviço sempre conferido e testado, juntamente com as evidências dos testes realizados, cumprindo rigorosamente o cronograma previsto, responsabilizando-se pela imediata correção dos erros verificados, sem ônus para a CAIXA.
- 18.1.12. Realizar, durante o período de vigência, sem ônus para a CAIXA, toda correção decorrente dos erros ou falhas que tenha cometido na execução dos serviços ou decorrentes de integração e adequação sistêmica, independente da data em que a solução tenha sido implantada em produção.
- 18.1.13. Estruturar-se de modo compatível e prover toda a infraestrutura necessária ao fornecimento do objeto deste contrato, com a qualidade e rigor exigidos.

**19. VIGÊNCIA CONTRATUAL**

- 19.1. A vigência deste contrato será de 24 (vinte e quatro) meses, contados a partir de sua assinatura, podendo ser prorrogado observando os termos e limites da Lei 13.303/2016.

**20. FORMA DE PAGAMENTO**

- 20.1. A CAIXA, após o aceite de entrega dos serviços e verificação do exato cumprimento de todas as cláusulas contratuais, efetuará o pagamento no 12º (décimo segundo) dia útil do mês subsequente, após entrega da nota fiscal e da fatura, que deverão ser apresentadas à CAIXA até o 5º (quinto) dia útil do mês subsequente à prestação dos serviços.
- 20.2. As notas fiscais e faturas deverão ser entregues à CEGTI – CN GOVERNANÇA DE TI, localizada no endereço QUADRA SEPN 512 CJ C LOTE 9/10, 4º ANDAR, ASA NORTE, BRASÍLIA/DF, CEP 70760-500, e-mail [cegti04@CAIXA.gov.br](mailto:cegti04@CAIXA.gov.br).
- 20.3. O pagamento será realizado mediante crédito em conta corrente mantida pela CONTRATADA em agência da CAIXA.
- 20.4. A data de pagamento será prorrogada na mesma proporção de eventual atraso ocorrido na entrega da nota fiscal/fatura, cabendo à CONTRATADA emitir a correspondente nota fiscal/fatura em conformidade com a legislação aplicável e regulamentações dos órgãos competentes.
- 20.5. Os pagamentos se darão:

DESCRIÇÃO DO SERVIÇO	FORMA DE PAGAMENTO	ATESTES PARA OS SERVIÇOS PRESTADOS
Subscrição do IDMC - <i>Intelligent Data Management Cloud</i>	Pagamentos mensais, com parcelas fixas, definidas para cada ano de contrato	Após a migração acordada, efetivo uso da nova solução, entrega do relatório pela contratada e o ateste dos serviços prestados.
Serviço de implantação, sustentação e atualização tecnológica da solução	Pagamentos mensais com parcelas fixas	Após a entrega do relatório pela contratada e o ateste dos serviços prestados pelas Unidades Técnicas por meio do Relatório de chamados (via GSC).
Serviço de suporte técnico especializado local ( <i>on site</i> ) e serviço de suporte à produção local ( <i>on site</i> )	Pagamento sob-demanda de HST (Horas de Serviço Técnico)	Após a entrega do Relatório pela contratada e o ateste dos serviços prestados pelas Unidades Técnicas.
Suporte técnico especializado (TAM)	Pagamentos mensais com parcelas fixas	Após a entrega do Relatório pela contratada e o ateste dos serviços prestados pelas Unidades Técnicas.
Serviço de transferência de conhecimento	Pagamento sob-demanda de TUs ( <i>Training Units</i> )	Após Relatório Técnico do Serviço emitido pela contratada e assinado pela área demandante (Informações, Detalhamento, e Avaliação igual ou acima de BOM realizada pelos Participantes) – ANEXO X.

**21. SANÇÕES**

- 21.1. Pelo não cumprimento das obrigações assumidas, garantida a previa defesa em processo regular, a CONTRATADA sujeitar-se-á às seguintes sanções, sem prejuízo das demais cominações aplicáveis:
- a) Multa;
  - b) Suspensão temporária de participar em licitação e impedimento de contratar com a CAIXA, pelo prazo de até 2 (dois) anos quando utilizada as modalidades Pregão Eletrônico, Licitação CAIXA, Dispensa e Inexigibilidade.
- 21.2. Parágrafo Primeiro - Pelo descumprimento dos prazos estabelecidos no Anexo FORMA DE EXECUÇÃO, a CONTRATADA sujeitar-se-á a multa equivalente a:
- I. 0,01% (zero vírgula zero um por cento) do valor global do contrato, por dia de atraso, na disponibilização de novas versões e atualizações dos produtos;
  - II. 0,03% (zero vírgula zero um por cento) do valor global do contrato, por dia de atraso na integração dos sistemas de atendimento da CONTRATADA com o da CAIXA.
- 21.3. As multas serão descontadas da fatura, do valor da garantia contratual, cobradas diretamente da CONTRATADA ou judicialmente.
- 21.4. Se a multa for de valor superior ao valor da garantia apresentada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CAIXA ou ainda, quando for o caso, cobrada judicialmente.
- 21.5. A penalidade de declaração de suspensão temporária de licitar e contratar com a CAIXA pelo prazo de até 02 (dois) anos poderá ser aplicada em casos de reincidências em descumprimento de prazo contratual, descumprimento parcial ou total de obrigação contratual ou, ainda, em caso de rescisão contratual, mesmo que desses fatos não resulte prejuízo à CAIXA.
- 21.6. A falta de quaisquer dos materiais cujo fornecimento e manutenção incumbe à CONTRATADA, não poderá ser alegada como motivo de força maior para o atraso, má execução ou inexecução do fornecimento objeto deste contrato e não a eximirá das penalidades a que está sujeita pelo não cumprimento dos prazos e demais condições estabelecidas.
- 21.7. As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, desde que as penalidades de multas não ultrapassem 10% (dez por cento) do valor total do contrato.
- 21.8. Constituem motivo de rescisão do contrato:
- 21.8.1. O descumprimento total ou parcial, pela CONTRATADA, de cláusulas contratuais, especificações, projetos ou prazos;
  - 21.8.2. A transferência total ou parcial do contrato;
  - 21.8.3. O cometimento reiterado de faltas ou falhas na prestação dos serviços;
  - 21.8.4. A lentidão no seu cumprimento, levando a CAIXA a presumir a não execução da prestação dos serviços contratados.
- 21.9. Caso a CAIXA não se utilize da prerrogativa de rescindir o contrato a seu exclusivo critério, poderá suspender a sua execução, suspendendo o pagamento da respectiva fatura, até que a CONTRATADA cumpra integralmente a condição contratual infringida.
- 21.10. O descumprimento das obrigações relacionadas com confidencialidade e segurança de dados, de informações e sistemas, mediante ações ou omissões,

intencionais ou acidentais, que impliquem perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenados, em que trafeguem ou do ambiente em que estejam sendo processados, determinará a responsabilização, na forma da lei, de seus dirigentes e funcionários envolvidos.

---

<sup>i</sup> Sessões e Certificados INFORMATICA

## **ANEXO I-C – 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 hiper escala. A hiper escala 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:
  - 1.3.1. 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.
  - 1.3.2. 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.
  - 1.3.3. 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.
  - 1.3.4. 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.
  - 1.3.5. Serviços medidos por utilização (“*measured service*”): os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos, através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado (por exemplo: armazenamento, processamento, largura de banda, e contas de usuário ativas). A utilização dos recursos pode ser monitorada, controlada e reportada, fornecendo transparência tanto para provedores como para consumidores. Portanto, a precificação, se houver, será balizada pelo uso dos serviços.”
- 1.4. Os requisitos deste capítulo se aplicam às empresas que prestarão serviços em nuvem para a CAIXA, ou que irão manter a estrutura de atendimento para a CAIXA em nuvem pública, incluindo o armazenamento de arquivos corporativos que tenham relação com o trabalho desempenhado na CAIXA. As empresas Contratadas para prestação de serviços em nuvem também devem observar os controles relatados nos demais capítulos deste documento.
- 1.5. Os serviços em nuvem do tipo SaaS poderão ser provenientes tanto do marketplace ou do catálogo de serviços do provedor de nuvem, oriundos de um contrato de Multinuvem e fornecidos pelo provedor; quanto serviços de SaaS contratados a parte e provenientes de contratos específicos com a empresa fornecedora da solução.

**2. GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS**

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

- 2.18. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 2.19. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.
- 2.20. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.
- 2.21. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 2.22. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.
- 2.23. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:
- O tipo de evento (inclusão, alteração, exclusão, consulta);
  - O autor do evento;
  - A data e hora do evento;
  - O endereço lógico do equipamento de origem do tipo do evento.
- 2.24. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 2.25. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.
- 2.26. Devem ser observadas as boas práticas de segregação e diferenciação entre ambientes de não produção e produtivo, estabelecendo-se acessos pertinentes para cada etapa do ciclo de desenvolvimento/manutenção e alinhado com o princípio do privilégio mínimo.
- 2.27. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 2.28. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.
- 2.29. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos na seção 2.4.
- 2.30. A Contratada deverá prover os recursos necessários para que os seus funcionários acessem remotamente o ambiente da CAIXA, se for o caso. Nesse caso, é responsabilidade da Contratada prover certificados digitais ou outros tokens de acesso conforme definido pela CAIXA, sem ônus adicionais para a CAIXA.

### **3. CONTROLES CRIPTOGRÁFICOS**

- 3.1. Os requisitos apresentados nesta seção devem ser obedecidos pela Contratada ou, caso os dados estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor. Neste último caso, a Contratada deverá

comprovar por relatório de auditoria (*Due Dilligence* Remoto) que o armazenamento/processamento dos dados ocorre somente em ambiente de nuvem e o Provedor deve atender, além dos requisitos a seguir, as regras descritas no item 6 deste Guia.

- 3.2. A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.
- 3.3. A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.
- 3.4. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 3.5. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 3.6. A Contratada deve fazer a geração e a renovação de certificados digitais expostos na Internet junto a autoridades certificadoras reconhecidas internacionalmente, cujas raízes de cadeias utilizadas na emissão dos certificados digitais façam parte do repositório de cadeias confiáveis dos principais navegadores e versões de sistemas operacionais, como: iOS 7 e superiores; Android 4 e superiores; Microsoft Edge 12 e superiores; Mozilla Firefox 45 e superiores; Google Chrome 49 e superiores; Apple Safari 8 e superiores; Linux Ubuntu 14 e superiores; Linux Mint 15 e superiores; MAC OS X 10.10 e superiores; e Windows 7 e superiores.
- 3.7. A Autoridade Certificadora deve possuir o selo Web Trust dentro do prazo de validade e a certificação Web Trust deve estar de acordo com, no mínimo, os Princípios e Critérios para Autoridades Certificadoras – versão 2.2.1, disponível em <https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/WT100aWebTrust-for-CA-221-110120-finalaoda.pdf?la=en&hash=0FDB6C541E7A61976625B9EAC55474D260A7E6> FD 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. Em atendimento à IN 05 GSI/PR, a disponibilização, execução e armazenamento de serviços de computação em nuvem deverá ser restrita ao território nacional.
- 5.3. 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.
- 5.4. 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.
- 5.5. Esta mesma Contratada deve assegurar que os dados da CAIXA processados e armazenados na Contratada são de propriedade exclusiva da CAIXA.
- 5.6. 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.
- 5.7. A Contratada deve assegurar a confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processadas e/ou armazenadas em nuvem.
- 5.8. 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.
- 5.9. 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.
- 5.10. 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.
- 5.11. 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.
- 5.12. 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:
- 5.13. 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;
- 5.14. 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
------------	----------	-----------	-------------------	----------

<i>Due Diligence Presencial</i>	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 <i>Due Diligence</i> 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
<i>Due Diligence Remoto</i>	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,	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	Disponibilizar relatório de auditoria em nome do Provedor de Nuvem	SEMESTRAL

	confidencialidade e privacidade	serviços de confiança do AICPA		
--	---------------------------------	--------------------------------	--	--

**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 aporem 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-D****CLÁUSULAS DE REQUISITOS DE SEGURANÇA TECNOLÓGICA PARA FORNECEDORES****1. GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS**

- 1.1. A Contratada deve ter uma política de controle de acesso dos seus colaboradores baseada no princípio do menor privilégio, que defina um processo formal de concessão, alteração e revogação de acesso.
- 1.2. A Contratada deve utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 1.3. A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.
- 1.4. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.
- 1.5. Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.
- 1.6. As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 1.7. Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no login.
- 1.8. A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 1.9. A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 1.10. A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.
- 1.11. Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.

[Cecot29@caixa.gov.br](mailto:Cecot29@caixa.gov.br)

- 1.12. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 1.13. A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 1.14. A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.
- 1.15. A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.
- 1.16. A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 1.17. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 1.18. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.
- 1.19. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.
- 1.20. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 1.21. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.
- 1.22. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:
- O tipo de evento (inclusão, alteração, exclusão, consulta);
  - O autor do evento;
  - A data e hora do evento;
  - IP e Porta do equipamento que originou o evento.

- 1.23. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 1.24. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.
- 1.25. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 1.26. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.
- 1.27. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9.
- 1.28. A Contratada 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 ATIVOS**

- 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 utilizar mecanismos de autenticação e autorização utilizando credenciais corporativas.
- 2.3. A Contratada deve dispor de recursos que garantam múltiplos fatores de autenticação do usuário (MFA), a serem utilizados de acordo com a criticidade ou classificação da informação/recurso a ser acessado. Esses múltiplos fatores devem ser implementados, no mínimo, por meio de biometria, OTP ou autorização por notificações de push em celulares.
- 2.4. A Contratada deve dispor de mecanismo de garantia de identidade, o qual deve ser realizado previamente à execução das requisições dos usuários.

- 2.5. Todas as contas de usuário devem ser identificadas por um ID de usuário exclusivo e todas as ações de um ID de usuário devem ser associadas a um único indivíduo ou proprietário registrado.
- 2.6. As contas do usuário devem ser criadas e configuradas pelo administrador de segurança do usuário.
- 2.7. Os controles de acesso em nível de aplicativo devem fazer uso da identidade autenticada do usuário, conforme estabelecido no logon.
- 2.8. A Contratada deve permitir criar e gerenciar perfis e credenciais de segurança para seus usuários.
- 2.9. A Contratada deve permitir que somente os usuários por ela autorizados tenham acesso aos recursos, em conformidade aos respectivos perfis de uso.
- 2.10. A Contratada não deve usar contas padrões, contas genéricas, contas não pessoais ou convidadas, a menos que a CAIXA tenha dado aprovação prévia por escrito para tais contas.
- 2.11. Uma conta não pessoal deve ser atribuída exclusivamente a uma única aplicação ou serviço e não pode ser utilizada para qualquer outra finalidade além daquela para a qual ela foi criada.
- 2.12. A Contratada deve informar os logins de usuário e senhas iniciais por meio de canais separados.
- 2.13. A Contratada deve implementar mecanismo de comunicação ao usuário em caso de alteração ou pedido de recuperação de sua senha.
- 2.14. A Contratada deve revisar os direitos de acesso existentes nos seus ativos pelo menos a cada dois anos. Em caso de dados pessoais, os direitos devem ser revisados pelo menos uma vez por ano.
- 2.15. A Contratada deve revisar as contas não pessoais mantidas em seu ambiente pelo menos duas vezes por ano, independentemente da classificação ou da confidencialidade da informação tratada.
- 2.16. A Contratada deve revisar os acessos privilegiados ao seu ambiente pelo menos a cada três meses.
- 2.17. A Contratada deve gerar e armazenar as evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões acima, e disponibilizá-las para a CAIXA sempre que solicitado.
- 2.18. As contas de acesso privilegiado não devem conter a indicação dos privilégios, a posição do indivíduo ou a organização a que pertence o indivíduo (por exemplo, "administrador" ou "diretor" não pode fazer parte de qualquer nome de utilizador) no logon do usuário.

- 2.19. A Contratada deve implementar a separação entre a administração do sistema (acesso privilegiado) e as atividades de negócios (acesso não privilegiado), por meio de níveis de acesso separados para atender a segregação entre as funções.
- 2.20. A Contratada deve permitir e fornecer utilitários para o monitoramento de contas privilegiadas.
- 2.21. Cabe à Contratada decidir pelo fornecimento do acesso remoto aos seus colaboradores. Uma vez fornecido, a Contratada deverá prover esse acesso por meio de canais seguros/VPN, utilizando múltiplos fatores de autenticação.
- 2.22. A Contratada deve implementar trilha de auditoria para todo e qualquer acesso realizado aos seus ativos, tornando possível identificar, de forma cronológica e inequívoca, os seguintes registros:
- O tipo de evento (inclusão, alteração, exclusão, consulta);
  - O autor do evento;
  - A data e hora do evento;
  - IP e Porta do equipamento que originou o evento.
- 2.23. A Contratada deve proteger os registros de trilha de auditoria contra adulteração.
- 2.24. A Contratada deve implementar o monitoramento dos acessos privilegiados às bases de dados, que fazem parte do objeto do contrato por meio de solução independente dos bancos de dados em uso.
- 2.25. A monitoração dos acessos privilegiados às bases de dados deve ocorrer em tempo-real e deve ser possível configurar respostas automatizadas para eventos específicos.
- 2.26. A Contratada deve desenvolver políticas e implementar soluções para garantir que o acesso remoto por parte dos seus funcionários – seja utilizando dispositivos da Contratada, seja utilizando dispositivos de propriedade pessoal - seja fornecido de forma segura e adequada. Tais políticas e procedimentos devem definir como a Contratada fornece acesso remoto e quais os controles necessários para oferecer este acesso de forma segura.
- 2.27. A Contratada deve usar métodos de autenticação robustos, baseados em múltiplos fatores de autenticação, para viabilizar o acesso remoto de seus funcionários à sua rede interna e deve empregar criptografia para proteger os dados em trânsito, considerando os requisitos descritos no item 9.
- 2.28. 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. SEGURANÇA DE REDES**

- 3.1. Todo o tráfego de rede associado ao objeto do contrato deve ser mediado por uma solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações).
- 3.2. O conjunto de regras do firewall deve se basear na negação de todos os serviços, exceto aqueles especificamente permitidos.
- 3.3. O processo para instalação e adaptação de regras de firewalls deve ser feito com duplo controle.
- 3.4. A Contratada deve revisar as regras de firewall pelo menos semestralmente, guardando evidências dessas revisões e dos ajustes eventualmente realizados, comunicando à CAIXA sobre a realização desta revisão.
- 3.5. Todos os componentes de gateway de perímetro e sistemas de computadores devem ser monitorados contra tentativas de intrusão, por meio de solução de prevenção e detecção de intrusão (IPS).
- 3.6. O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de intrusão suspeitas ou reais.
- 3.7. A Contratada deve informar imediatamente à CAIXA em caso de tentativa de intrusão real, e informar à CAIXA em relatório mensal sobre as tentativas de intrusão suspeitas.
- 3.8. A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).
- 3.9. As soluções de firewall, IPS e-DDoS utilizadas pela Contratada serão validadas pela CAIXA a partir de documentações do fabricante ou certificações.
- 3.10. A Contratada deve impedir o uso do protocolo Bluetooth para a transferência de dados.
- 3.11. Todas as comunicações e trocas de informações entre a Contratada e a CAIXA devem ser realizadas por meio de conexão protegida, com TLS 1.3 ou superior.
- 3.12. Para os casos aplicáveis, os acessos diretos de diferentes equipamentos ao serviço da Contratada devem ser gerenciados por ferramentas de gerenciamento de dispositivos e/ou aplicativos (MDM/MAM) ou controle de acesso à rede (NAC).

**4. CICLO DE VIDA DE DESENVOLVIMENTO SEGURO**

- 4.1. A Contratada deve adotar o princípio de security by design para garantir que as aplicações de TI por ela desenvolvidas sejam seguras desde a concepção.
- 4.2. A Contratada deve fazer análise de código automatizada com base nas melhores práticas de mercado, utilizando como referência os padrões do OWASP.
- 4.3. A Contratada deve fazer análise de código estática (SAST) e dinâmica (DAST) periodicamente e de forma integrada ao ciclo de desenvolvimento como um todo para a solução Contratada. Essas análises precisam ser executadas pelo menos uma vez por ano ou quando houver uma mudança considerada significativa nas funcionalidades do sistema/aplicação (como a inclusão de uma nova funcionalidade crítica ou manutenção em módulos que tratem informações sensíveis e confidenciais). A bateria de testes deve incluir testes de resistência, injeções de falhas, teste de penetração e teste de vulnerabilidades onde aplicável.
- 4.4. A Contratada deve incluir a análise e a remediação das vulnerabilidades detectadas como parte do ciclo de vida de desenvolvimento de software padrão, sem custo adicional para a CAIXA, dentro de um período razoável e de acordo com a criticidade da falha encontrada.
- 4.5. A Contratada deve estabelecer critérios de escala e prazo para correção das vulnerabilidades e deve definir as alçadas para aceitação de riscos. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.
- 4.6. A Contratada deve submeter suas políticas de desenvolvimento seguro à aprovação da CAIXA.
- 4.7. Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados à CAIXA sempre que solicitado.

**5. GESTÃO DE SERVIÇOS E MUDANÇAS**

- 5.1. A Contratada deve ter um processo de Gestão de Mudanças para garantir a proteção contínua dos ativos de informação e dados, em particular aqueles que fazem parte do escopo do objeto do contrato.
- 5.2. A Contratada deve revisar periodicamente as atividades de gestão de mudanças, incluindo a acurácia da Base de Dados de Gerenciamento de Configuração (Configuration Management Database – CMDB).
- 5.3. A Contratada deve cumprir com os procedimentos de registros de informações relacionadas ao processo de gestão de mudanças, no contexto do contrato, incluindo:

- Referência da mudança
  - Data de implementação
  - Avaliação de impactos
  - Resultados do teste
  - Procedimentos de rollback
  - Alterações de emergência
  - Atualizações relacionadas ao inventário de ativos de informação
  - Armazenamento Seguro de mídia de backup produzidos durante a atualização
  - Atualização dos procedimentos de Documentação e de trabalho
  - Atualizações aos documentos de Plano de Continuidade dos Negócios / Recuperação de Desastres se for o caso;
  - Categorização, priorização e procedimentos de emergência
  - Autorização de mudança
  - Gerenciamento de liberação
  - Link para incidentes / problemas (conforme apropriado).
- 5.4. A Contratada só deve promover os aplicativos e sistemas relacionados ao escopo do objeto do contrato para o ambiente de Produção após a realização com sucesso dos testes predefinidos baseados em caso de uso.
- 5.5. A Contratada deve conduzir uma avaliação de risco e ameaças, contemplando inclusive os testes baseados em casos de uso, quando da implantação de uma mudança.
- 5.6. A Contratada deve realizar uma avaliação de risco:
- Quando o escopo do sistema é expandido para incluir novos ativos de informação com novas funcionalidades;
  - Quando uma nova comunidade de usuários é introduzida; ou
  - Anualmente, por se tratar de risco cibernético, nos termos do art. 8º da Resolução BACEN 4.893/2021.
- 5.7. A Contratada deve disponibilizar os documentos de avaliação de risco à CAIXA sempre que solicitado.
- 6. GESTÃO DE INCIDENTES DE SEGURANÇA**

- 6.1. A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua infraestrutura de servidores e redes.
- 6.2. A Contratada deve realizar testes independentes de penetração/invasão pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para a CAIXA. O escopo dos testes será previamente combinado e aprovado pela CAIXA, dentro dos limites do contrato.
- 6.3. Os testes de penetração/invasão terão como escopo, rede, aplicação web, Application Programming Interface (API), serviços hospedados e; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações do ponto de contato; remediação, por exemplo, como as descobertas serão encaminhadas internamente; dentre outros.
- 6.4. Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções necessárias, serão fornecidos à CAIXA sempre que solicitado.
- 6.5. A Contratada deverá possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.
- 6.6. A contratada poderá utilizar como modelo de referência do processo a norma NIST SP 800-61 Rev. 2.
- 6.7. O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou a CAIXA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CAIXA.
- 6.8. A Contratada deverá ter um processo de notificação de incidentes 24x7.
- 6.9. A Contratada deverá comunicar à CAIXA incidentes que cause impacto na confidencialidade, integridade ou disponibilidade do serviço prestado.
- 6.10. Os incidentes serão comunicados tanto ao gestor do contrato vinculado quanto ao SOC CAIXA, que opera 24x7, por meio do endereço de e-mail: [abuse@caixa.gov.br](mailto:abuse@caixa.gov.br). Esse endereço poderá ser alterado durante a vigência do contrato, e, em caso de alteração, a Contratada será devidamente informada.
- 6.11. A Contratada deverá comunicar à CAIXA, dentro do prazo acordado, todos os incidentes detectados que envolvam os serviços prestados, conforme a classificação abaixo:

Nível de severidade	Descrição do nível de severidade	Prazo Máximo
<b>Severidade 1 (Crítica)</b>	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> <li>-Impacto em ativos ou serviços críticos de TI;</li> <li>-Violação significativa de dados sensíveis;</li> <li>-Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente.</li> </ul> <p><b>Exemplos não exaustivos:</b> ataque de <i>Ransomware</i>, ataque de negação de serviço distribuído – DDoS, vazamento de informações corporativa ou dados pessoais. Dentre outros.</p>	2 horas após o início da ocorrência.
<b>Severidade 2 (Alta)</b>	<p>Eventos cujo contexto principal é a segurança cibernética, tais como:</p> <ul style="list-style-type: none"> <li>-Impacto em ativos ou serviços de TI de alta criticidade;</li> <li>-Detecção de acesso não autorizado e/ou alterações em sistemas de informação;</li> <li>-Infecção persistente por código malicioso;</li> <li>-Intrusão persistente na rede;</li> <li>-Incidentes de segurança cibernética envolvendo dirigentes;</li> <li>-Ameaça significativa à disponibilidade e/ou integridade do ambiente;</li> <li>-Ameaça significativa à imagem da CAIXA.</li> </ul> <p><b>Exemplos não exaustivos:</b> ataques de escalação de privilégio em servidores, ataques do tipo <i>brute force</i> e <i>password spray</i>. Dentre outros</p>	4 horas após o início da ocorrência.

- 6.12. Não será escopo deste comunicado, demais incidentes que aconteçam na infraestrutura cibernética da Contratada que não tenham relação com a CAIXA.
- 6.13. A Contratada deverá fornecer descrição detalhada dos incidentes, incluindo informações suficientes para classificá-los por nível de severidade, conforme a definição dos eventos. As informações sobre incidentes podem ser enriquecidas utilizando o modelo do MITRE ATT&CK®.
- 6.14. A contratada deverá seguir preferencialmente o modelo de comunicação de ISCF – Incidente de Segurança Cibernética em Fornecedor, Anexo IIA, que também contempla situações de incidentes de segurança com dados pessoais.
- 6.15. Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, a CAIXA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.

- 6.16. A Contratada deve documentar os casos de uso que são utilizados para realizar a configuração e o monitoramento de eventos, correlacionando tecnologias para tratar padrões / cenários de ataque comuns e avançados; e disponibilizar os casos de uso à CAIXA sempre que solicitado.
- 6.17. A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.
- 6.18. A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança da CAIXA deve ser considerada, observada a regulamentação em vigor, conforme art. 3º, §4º da Res. BACEN 4.893/2021.
- 6.19. Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência da CAIXA por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética da CAIXA.

## **7. CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES**

- 7.1. A Contratada deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.
- 7.2. O referido plano de continuidade deverá ser informado para a CAIXA como parte das ações de acompanhamento do contrato, e deverá ser atualizado e testado anualmente, ou em qualquer mudança significativa do ambiente.
- 7.3. A atuação, em caráter de contingência, causada por uma eventual indisponibilidade do serviço prestado, considera as seguintes premissas:
- a) Interrupção total ou parcial dos serviços
  - b) Ter infraestrutura alternativa: física e lógica em local distante do ambiente central de produção, com o objetivo de minimizar o risco de perda de ambas as instâncias;
  - c) Manter os serviços essenciais suportados pelo contrato
  - d) Manter a lista de integrantes das equipes e o Plano de Recuperação de Desastres atualizados;
  - e) Ter local seguro para guarda de backups fora do local atingido;
  - f) Assegurar a disponibilidade dos serviços essenciais dentro do tempo previsto para recuperação do serviço, de acordo com o contrato;
  - g) Procedimento documentado e evidenciado de testes das mídias armazenadas *offsite*;
  - h) Cópias de todos os procedimentos abordando backup, restauração e reconstituição de armazenamento de dados.

- 7.4. O plano de continuidade deve possuir os seguintes elementos em sua composição:
- a) Identificação do serviço suportado pelo contrato;
  - b) A forma de conectividade usada e os direitos de acesso;
  - c) A arquitetura do ambiente de produção;
  - d) As interfaces de aplicações e suas dependências;
  - e) O SLA contratado e os limites suportados para interrupção;
  - f) A forma de replicação dos dados com o site alternativo;
  - g) Procedimentos adotados para recuperação de desastres;
  - h) Lista de contatos das equipes responsáveis pelo restabelecimento do serviço, divididos por tipos de atividades executadas;
- 7.5. A obrigatoriedade do plano de continuidade se estende para empresas que sejam subcontratadas pela Contratada.
- 7.6. A Contratada deve considerar, como parte do plano de continuidade, os diferentes ambientes de risco e o grau de mitigação de riscos necessários para proteger a Instituição, caso seja necessário colocar o plano em prática.
- 7.7. A avaliação de riscos e dos processos críticos devem levar em consideração instrumentos específicos, como um BIA – Business Impact Analysis.
- 7.8. A Contratada, visando a continuidade dos negócios, deve implantar uma política de backup, conforme exposto no item 10.

## **8. AUDITORIA CONTÍNUA**

- 8.1. A Contratada deve apresentar à CAIXA, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.
- 8.2. A Contratada deve informar imediatamente à CAIXA sobre qualquer auditoria regulatória, sua finalidade e como ela se relaciona com os serviços prestados à CAIXA.
- 8.3. A Contratada deve informar à CAIXA caso sejam contatados por um órgão regulador e se o propósito desse contato pode estar relacionado com/ou afetar os serviços prestados à CAIXA.
- 8.4. A Contratada deve fornecer os subsídios necessários para que a CAIXA implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.
- 8.5. A Contratada deverá disponibilizar, caso a CAIXA solicite, acesso às instalações da Contratada para realização de processo de *Due Dilligence* Presencial, para verificar o cumprimento dos requisitos de segurança.

- 8.6. Caso a Contratada não tenha certificação SOC Nível 2, ela deverá fazer auditoria externa independente, pelo menos uma vez por ano, em relação ao cumprimento dos requisitos de segurança estabelecidos neste documento, e apresentar os relatórios à CAIXA sempre que solicitado.

## **9. CONTROLES CRIPTOGRÁFICOS**

- 9.1. A Contratada deve implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela CAIXA.
- 9.2. A Contratada deve implementar um processo de gestão de chaves criptográficas que deve considerar todo o ciclo de vida da chave, o qual envolve: geração, armazenamento, distribuição, utilização, recuperação, renovação, exclusão e destruição da chave.
- 9.3. A Contratada deve utilizar algoritmos, tamanhos de chave e prazos de validade de chaves aprovados pelo NIST.
- 9.4. A Contratada deve gerar, controlar e distribuir chaves criptográficas simétricas e assimétricas usando processos e tecnologias de gerenciamento de chaves aprovados pelo NIST.
- 9.5. Caso a Contratada hospede uma página com uma URL e um certificado gerados pela CAIXA, a Contratada deverá armazenar este certificado em dispositivo seguro com bloqueio para exportação da chave.
- 9.6. As chaves criptográficas geradas pela Contratada devem ser utilizadas com a finalidade exclusiva de atender às necessidades do objeto contratado.
- 9.7. A Contratada deve permitir a criptografia de volume (por exemplo: a criptografia de um disco inteiro) e a criptografia de estruturas de dados específicas (por exemplo: arquivos ou registros específicos de uma tabela de banco de dados).
- 9.8. A Contratada deve permitir recursos para trilha de auditoria, permitindo visualizar quem usou determinada chave para acessar um objeto, qual objeto foi acessado, quando ocorreu esse acesso e qual endereço de origem do acesso.
- 9.9. A Contratada deve permitir visualizar ou gerar relatório, a critério da CAIXA, de tentativas malsucedidas de acesso por usuários sem permissão para decifrar os dados.
- 9.10. A Contratada deve permitir que dados criptografados e chaves de criptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.
- 9.11. A Contratada deve permitir a auditoria da segurança de chaves criptográficas.

- 9.12. A Contratada deve possibilitar comunicação criptografada e protegida para a transferência de dados por meio do TLS 1.3 e superior.

## **10. POLÍTICA DE BACKUP**

- 10.1. A Contratada deve possuir e implementar política de backup das informações e dos registros de log associados ao objeto do contrato, em conformidade com os dispositivos legais aplicáveis.
- 10.2. A política de backup deve assegurar a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica e os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha, ou por solicitação da CAIXA.
- 10.3. A Contratada deve prover pelo menos um site de armazenamento alternativo – e geograficamente distinto - como parte de sua política de backup, permitindo o armazenamento e a recuperação da informação sempre que necessário e de acordo com os requisitos definidos na item 7.
- 10.4. A Contratada deve garantir que o site de armazenamento alternativo conta com os mesmos controles de segurança do site de armazenamento primário.

## **11. RELATÓRIOS QUE COMPROVAM O CUMPRIMENTO DOS REQUERIMENTOS MÍNIMOS DE SEGURANÇA.**

- 11.1. Sempre que a CAIXA julgar necessário, poderá realizar Due Diligence presencial ou remota para verificar os requisitos de segurança presente nas cláusulas, são atendidos pela Contratada. O Due Diligence presencial é facultativo e será feito a critério da CAIXA.
- 11.2. Os documentos exigidos devem ter a sua primeira versão entregue antes da assinatura do contrato, que comprovam o cumprimento dos requerimentos de segurança cibernética conforme estabelecido nas cláusulas e devem ser reiterados de acordo com a vigência indicada nos quadros abaixo:

REQUISITOS	OBJETIVO	DESCRIÇÃO	FORMA DE CONTROLE	VIGÊNCIA
------------	----------	-----------	-------------------	----------

Due Diligence Presencial	Sempre que a CAIXA julgar necessário, poderá realizar visitas in-loco às zonas de disponibilidade da Contratada para verificar os requisitos de segurança presente nas cláusulas	A CAIXA, por iniciativa própria, fará due diligence presencial em função de discrepâncias identificadas em relatórios de auditoria entregues ou dúvidas onde apenas a documentação não seja suficiente.	A visita poderá ser realizada por equipe própria da CAIXA ou empresa designada pela CAIXA	SOB DEMANDA
Due Diligence Remoto	Constatar que os processos determinados pela CAIXA estão sendo seguidos, conforme descrito nas cláusulas	Documentos previstos nas cláusulas e demais comprovantes de seus requisitos.  Quando não comprovados por certificação, os itens exigidos nas cláusulas devem ser certificados por empresa de auditoria independente.	Relatórios próprios da empresa para comprovação do atendimento aos itens das cláusulas, desde que ratificados por empresa de auditoria independente  Relatório de empresa de auditoria independente, a ser apresentado pela Contratada	SOB DEMANDA
Certificação SOC 2 – Tipos 1 e 2	Garantir acesso a uma avaliação independente, por meio de relatório de auditoria, sobre o ambiente de controle do provedor, relevante para a segurança, disponibilidade, confidencialidade e privacidade	SOC TYPE 2 Fornece relatórios com descrição do ambiente de controles do provedor e da auditoria externa dos controles que atendem aos princípios e critérios de segurança, disponibilidade e confidencialidade dos serviços de confiança do AICPA	Disponibilizar relatório de auditoria em nome da empresa	ANUAL

## 12. ENCERRAMENTO DO CONTRATO

- 12.1. A Contratada deve garantir que todos os dados - incluindo chaves criptográficas e os backups armazenados e que não sejam mais necessários na execução do Contrato - serão descartados de acordo com os padrões do mercado, de maneira que os requisitos de confidencialidade não sejam violados.
- 12.2. A Contratada deve reter os dados por até 180 dias para a migração para ambiente interno ou outro fornecedor indicado pela CAIXA.
- 12.3. Os dados, após transferência e validação da integridade, devem ser excluídos pelo antigo fornecedor.

[Cecot29@caixa.gov.br](mailto:Cecot29@caixa.gov.br)

12.4. A exclusão dos dados após o término do contrato e o período de retenção de 180 dias deve obedecer aos padrões definidos no NIST SP 800-88 Guidelines for Media Sanitization, com fornecimento de relatório para a CAIXA certificando a conformidade dos processos realizados com a norma indicada.

12.5. Caso a Contratada tenha ativo de informação no fim do ciclo de vida, ou considerado inservível, este ativo deverá ser destruído, com o fornecimento do Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction – CEED), discriminando os ativos reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição.

### **13. NÃO CONFORMIDADE COM REQUISITOS DE SEGURANÇA E CONSEQUÊNCIAS**

13.1. O não cumprimento, pela Contratada, de qualquer um dos seguintes requisitos de segurança, definidos neste instrumento contratual, ensejará a aplicação das penalidades previstas neste contrato e poderá, a critério da Contratante, ensejar a rescisão imediata do contrato, sem prejuízo de outras medidas cabíveis:

- a) Não fornecer evidências de aprovação ou rejeição dos direitos de acesso, resultantes das revisões de acesso realizadas;
- b) Não comunicar a revisão das regras de firewall;
- c) Não comunicar ocorrências de intrusão real;
- d) Não fornecer relatório mensal sobre as tentativas de intrusão;
- e) Não fornecer o planejamento de correção de vulnerabilidades;
- f) Não fornecer os relatórios dos testes SAST e DAST realizados e o planejamento das correções a serem feitas;
- g) Não fornecer os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções;
- h) Não fornecer os relatórios de incidentes conforme SLA;
- i) Não prestar as informações e relatórios solicitados pela CAIXA;
- j) Não fornecer os relatórios de auditoria externa independente;
- k) Não fornecer relatório indicando conformidade com o NIST SP 800-88;
- l) Não atender a convocação da CAIXA para Due Diligence presencial ou remoto;
- m) Não fornecer a documentação solicitada em decorrência do Due Diligence presencial ou remoto, conforme prazo acordado entre as partes;

**Modelo ISCF - Incidente de Segurança Cibernética em Fornecedor****ISCF – Incidente de Segurança Cibernética em Fornecedor**

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

**1. INTRODUÇÃO**

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

**2. ANÁLISE RESUMIDA DA OCORRÊNCIA**

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

**2.1. DETECÇÃO**

<Informar como o evento foi detectado (ex.: Email externo ou interno, SIEM, Teams etc.)>

**2.2. ANÁLISE**

<Informar a classificação do incidente, tática utilizada pelo atacante, POP, playbook utilizado etc.>

**2.3. CONTENÇÃO**

<Informar todas as ações que foram necessárias para conter o incidente (ex: isolamento de máquinas, bloqueio de usuários, bloqueio de IP, takedown de páginas etc.)>

**2.4. ERRADICAÇÃO**

<Caso existam, informar todas as ações que foram necessárias para erradicar as fragilidades que permitiram o incidente (ex.: Atualização de patch, alteração em regras de firewall, alteração em permissionamento de acessos etc.)>

**2.5. RECUPERAÇÃO**

<Caso existam, informar servidores, serviços ou aplicações que foram afetadas e que precisaram ser recuperadas por todas as áreas envolvidas.>

**3. CONCLUSÃO****3.1. ANÁLISE FINAL DE PÓS-INCIDENTE**

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

**4. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS****4.1. FORMULÁRIO ISDP**

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

**4.1.1 COMUNICAÇÃO****4.1.1.1 Tipo de Comunicação**

☐ Completa.

☐ Parcial.

Comentário:

**4.1.1.2 Para comunicação parcial**

☐ Preliminar

☐ Complementar

Comentário:

**4.1.1.3 Critério para comunicação**

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

☐ Não foi identificado riscos relevantes aos titulares

☐ Impacto continua sob avaliação

Comentário:

**4.2 IDENTIFICAÇÃO DO AGENTE DE TRATAMENTO****4.2.1 Responsabilidade no tratamento de dados envolvido**

☐ Controlador.

☐ Operador.

Comentário:

**4.2.2 Comunicação ao Controlador**

☐ Não necessária, o notificante é o Controlador.

☐ O Controlador já foi notificado.

☐ O Controlador não foi notificado.

Comentário:

**4.2.3 Identificação da empresa**

Número do CPF ou CNPJ:

Nome ou Razão Social:

Natureza da Organização (Pública ou Privada):

Endereço:

Cidade:

Estado:

CEP:

E-mail:

Comentário:

4.2.4 *Dados do notificante*

Nome

E-mail

Telefone

4.2.5 *Dados do encarregado*

☐ Mesmos do notificante

Nome

E-mail

Telefone

### **4.3 SOBRE O INCIDENTE DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS**

#### **4.3.1.1 Breve Descrição**

##### **4.3.1.2 Quando o incidente ocorreu**

Data e hora de confirmação

Comentário

##### **4.3.1.3 Quando a organização teve ciência do incidente de segurança**

Data e hora de confirmação

Comentário

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

Comentário

##### **4.3.1.5 Justificativa quando a comunicação não ocorrer de forma imediata**

Comentário

##### **4.3.1.6 Qual a natureza dos dados afetados**

☐ Origem racial ou étnica

☐ Convicção religiosa

☐ Opinião política

☐ Filiação a sindicato

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

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

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

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.

Comentário

##### **4.3.1.7 Qual a quantidade de titulares afetados**

Comentário

##### **4.3.1.8 Qual a categoria dos dados afetados**

☐ Funcionários

☐ Prestadores de serviço

☐ Clientes

☐ Consumidores

☐ Usuários

☐ Pacientes de serviço de saúde

☐ Crianças ou adolescentes

☐ Outros (Comentar)

Comentário

## **5 MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS**

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

Comentário

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

Comentário

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

Comentário

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

Comentário

## **6 RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA**

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

Comentário

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

☐ Sim

☐ Não

Comentário

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

☐ Sim

☐ Não

Comentário

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

Comentário

**ANEXO I-E**  
**AVALIAÇÃO DA CAPACITAÇÃO – REAÇÃO**

Colegas, necessário avaliar a *mentoring* sobre: \_\_\_\_\_

1. Insira sua matrícula (cxxxxxx): \_\_\_\_\_
2. Clareza na definição dos objetivos do curso:
  - ☐ Ruim
  - ☐ Regular
  - ☐ Boa
  - ☐ Muito boa
  - ☐ Ótima
3. Compatibilidade dos objetivos do curso com as suas necessidades de Desenvolvimento:
  - ☐ Ruim
  - ☐ Regular
  - ☐ Boa
  - ☐ Muito boa
  - ☐ Ótima
4. Carga horária programada para as atividades:
  - ☐ Ruim
  - ☐ Regular
  - ☐ Boa
  - ☐ Muito boa
  - ☐ Ótima
5. Ordenação do conteúdo programático e qualidade do material distribuído:
  - ☐ Ruim
  - ☐ Regular
  - ☐ Boa
  - ☐ Muito boa
  - ☐ Ótima
6. Possibilidade de aplicação, em curto prazo, dos conhecimentos adquiridos na execução de suas tarefas no trabalho:
  - ☐ Ruim
  - ☐ Regular
  - ☐ Boa
  - ☐ Muito boa
  - ☐ Ótima
7. Sobre o(a) instrutor(a): Segurança na transmissão dos conteúdos e da exemplificação:

- ☐ Ruim
- ☐ Regular
- ☐ Boa
- ☐ Muito boa
- ☐ Ótima

8. Sobre o(a) instrutor(a): Nível de profundidade com que os temas e assuntos foram abordados:

- ☐ Ruim
- ☐ Regular
- ☐ Boa
- ☐ Muito boa
- ☐ Ótima

9. Sobre (o)a instrutor(a): Disposição para esclarecer dúvidas e respeito às ideias manifestadas pelos participantes acerca dos temas abordados no curso:

- ☐ Ruim
- ☐ Regular
- ☐ Boa
- ☐ Muito boa
- ☐ Ótima

10. Quais foram os pontos fortes desse curso na sua opinião. Caso considere necessário registrar algum comentário, utilize o espaço:

---

---

---

---

---

**ANEXO I-F****AVALIAÇÃO DE USUÁRIOS PÓS-MIGRAÇÃO PARA SAAS****1. Informações Gerais:**

- Nome (opcional): \_\_\_\_\_
- Cargo/Função: \_\_\_\_\_
- Departamento/Área: \_\_\_\_\_

**2. Experiência com o Sistema SaaS:****2.1. Facilidade de acesso ao sistema**

- ( ) Muito difícil
- ( ) Difícil
- ( ) Neutro
- ( ) Fácil
- ( ) Muito fácil

**2.2. Desempenho do sistema (velocidade, estabilidade etc.):**

- ( ) Muito insatisfeito
- ( ) Insatisfeito
- ( ) Neutro
- ( ) Satisfeito
- ( ) Muito satisfeito

**2.3. Interface e usabilidade:**

- ( ) Muito confusa
- ( ) Confusa
- ( ) Neutra
- ( ) Intuitiva
- ( ) Muito intuitiva

**2.4. Funcionalidades atendem às necessidades especificadas?**

- ( ) Não atende
- ( ) Atende parcialmente
- ( ) Atende totalmente
- ( ) Supera as expectativas

**3. Comparação com o Ambiente On-Premise****3.1. Em relação ao sistema anterior, como você avalia o novo modelo SaaS?**

- ( ) Muito pior
- ( ) Pior

[Cecot29@caixa.gov.br](mailto:Cecot29@caixa.gov.br)

- ☐ Igual
- ☐ Melhor
- ☐ Muito melhor

**4. Suporte**

4.1. O suporte técnico foi eficiente durante a transição?

- ☐ Muito ineficiente
- ☐ Ineficiente
- ☐ Neutro
- ☐ Eficiente
- ☐ Muito eficiente