

## ANEXO I - N

### **SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS**

1. De acordo com o Guia CAIXA de Diretrizes Gerais de Segurança da Informação e Privacidade, o tipo de contratação pretendida deve ter Grau de Criticidade ALTO.
- 1.1. A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (<https://www.caixa.gov.br/Downloads/caixa-governanca/politica-seguranca-informacao.pdf>), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto do contrato.
- 1.2. A CONTRATADA deve proteger as informações corporativas da CAIXA e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.
- 1.3. A CONTRATADA deve garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações obtidas durante a prestação dos serviços ou em função deles e somente as utilizem no âmbito dos serviços contratados.
- 1.4. A CONTRATADA deve garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social.
- 1.5. A CONTRATADA deve garantir que as práticas de segurança da informação por ela executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento.
- 1.6. A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.
- 1.7. A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação.
- 1.8. A CONTRATADA fica ciente de que deve guardar o mais completo e absoluto SIGILO em relação às informações e dados que tiver conhecimento em razão do serviço a ser prestado, observadas as solicitações de órgãos de regulação, fiscalização, supervisão e de controle, bem como as determinações judiciais que deverão ser comunicadas imediatamente, pois ambas somente poderão ser atendidas mediante prévia autorização da área jurídica da CONTRATANTE.

- 1.9. A CONTRATADA fica ciente que, por força da lei, é responsável civil e criminalmente pela divulgação indevida, descuidada ou incorreta utilização das informações corporativas da CAIXA e de seus clientes, sem prejuízo da responsabilidade por perdas e danos a que derem causa e das cominações contratuais impostas.
- 1.10. A CONTRATADA deve comunicar imediatamente à CONTRATANTE qualquer descumprimento às cláusulas acima, principalmente para os casos em que ficar comprovado o comprometimento de informação corporativa da CAIXA ou sob sua responsabilidade.

**CLÁUSULAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO – GRAU DE CRITICIDADE MÉDIO, que também se aplicam ao Grau de Criticidade ALTO:**

- 1.11. A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, anexo (o MO19607 deverá ser anexado).
- 1.12. A CONTRATADA deve enviar, anualmente, à CONTRATANTE a versão vigente do(s) Termo(s) de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, a ser disponibilizado pela área gestora do contrato, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).
- 1.13. A CONTRATADA deve realizar ou contratar, treinamento para seus dirigentes, empregados e colaboradores, visando a sensibilização e conscientização em relação à segurança da informação e privacidade de dados, abordando no mínimo 80% do seguinte conteúdo:

Grau de Criticidade em SI Alto ou Máximo			
Domínio Temático	Conteúdo	Carga Anual	Horária
Política de Segurança da Informação	- Conhecimento da política de segurança da informação da empresa e da Política de Segurança e Informação da CAIXA	8 horas	
Tratamento da Informação	- Uso seguro de informações corporativas a que tiver acesso; - Adoção da política de “mesa limpa”, “tela limpa” e “impressora limpa”; - Descarte seguro de informação.		
Reporte de Incidentes	- Formas de reporte de incidentes de segurança da informação na empresa e na CAIXA		
Privacy by Design e Secure by Design	- Metodologia e princípios		
Fundamentos para Segurança Digital	- Conceitos básicos de segurança digital; - Uso da Internet		
Segurança de Dispositivos Digitais Pessoais	- Proteção e privacidade em dispositivos digitais pessoais; - Conhecendo, configurando e usando o dispositivo; - Mantendo o dispositivo;		

- 1.13.1. O treinamento referido no item 1.13 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual.
- 1.14. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.13.
- 1.15. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do período, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA.
- 1.16. A CONTRATADA deve se adequar às normas e a legislação vigente inerentes à Segurança da Informação relacionadas às atividades da CONTRATANTE, enquanto empresa pública e instituição financeira.
- 1.17. A CONTRATANTE poderá exercer o direito de exigir alterações nos controles de segurança da CONTRATADA, à medida que os ambientes externos e internos se modifiquem.
- 1.18. A CONTRATADA deve solicitar formalmente autorização para subcontratação de serviços, cabendo a CONTRATANTE autorizar ou não.
- 1.19. Em caso de concretização de subcontratação de serviços, previamente autorizada pela CONTRATANTE, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.
- 1.20. A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores: a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, treinados em SI, conforme item 1.13 no último ano dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base; b) Quantidade de empregados que assinaram o Termo de Responsabilidade de Segurança da Informação, dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE até o último dia útil do mês subsequente ao ano base.
- 1.21. O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente instrumento contratual, implicará em:
  - a) Multa de até 1% do valor global do contrato de acordo com a gravidade;
  - b) Rescisão contratual em caso de impacto grave que gere prejuízos financeiros e/ou de imagem para a CAIXA.
- 1.22. Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a comunicar imediatamente à CAIXA e providenciar a solução tempestivamente, conforme Plano de Continuidade operacional.
- 1.23. Quaisquer materiais ou documentos com informações confidenciais que tenham sido fornecidos à CONTRATADA pela CONTRATANTE serão devolvidos, acompanhados de todas as cópias, em até 5 (cinco) dias, a

partir da formalização de solicitação de devolução das informações confidenciais pela CONTRATANTE.

- 1.24. No encerramento/extinção do contrato a CONTRATADA se compromete a:
- a) entregar a versão mais atualizada de todos os artefatos, componentes e demais produtos por ele produzidos durante a vigência do contrato;
  - b) executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CONTRATANTE ou a quem ela indicar, observada a regulamentação vigente;
  - c) devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.

#### **CLÁUSULAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO – GRAU DE CRITICIDADE ALTO**

- 1.25. A CONTRATADA é responsável por realizar o tratamento das informações da CAIXA e as sob sua responsabilidade, observando sua classificação de sigilo, bem como as demais regras internas da CAIXA estipuladas na versão vigente do manual normativo OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.
- 1.26. A CONTRATADA, durante a execução dos serviços contratados, deve adotar a mesma classificação da informação adotada pela CONTRATANTE, observar e cumprir as regras internas da CONTRATANTE quanto ao tratamento de informações sensíveis e confidenciais da CAIXA, previstas no OR016 – Tratamento da Informação, a ser disponibilizado pela área gestora do contrato.
- 1.27. A CONTRATADA é responsável pelas informações que obtiver, em razão de acesso aos recursos computacionais da CAIXA e se compromete a tomar conhecimento e cumprir as regras de uso aceitável e não aceitável da informação.
- 1.28. O treinamento de segurança da informação e proteção de dados referido no item 1.13 será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de forma presencial ou virtual, com carga horária mínima anual de 08 horas.
- 1.29. A CONTRATADA deve apresentar anualmente, até o último dia útil do mês subsequente ao término do ano base, a documentação comprobatória de cumprimento do treinamento referido no item 1.13 e, caso estabelecido pela CONTRATANTE.
- 1.30. A CONTRATADA deve emitir relatório, anualmente, até o último dia útil do mês subsequente ao término do ano base, relacionados aos seus riscos de segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CONTRATANTE.
- 1.31. Os relatórios referidos no item anterior devem proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.
- 1.32. A CONTRATADA garantirá que a CONTRATANTE, ou a auditoria independente indicada pela CONTRATANTE, ou os órgãos de regulação/fiscalização das atividades de atuação da CAIXA tenham acesso

físico e lógico ao seu ambiente e às informações relacionadas ao objeto do contrato, para realizar verificações relativas aos padrões de segurança da informação.

- 1.33. A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.
- 1.34. A CONTRATADA deve reportar imediatamente à CONTRATANTE os incidentes de segurança da informação identificados em seu ambiente ou operação e em toda sua cadeia produtiva.
- 1.35. A CONTRATADA deve enviar à CONTRATANTE, em até 05 dias úteis da detecção da ocorrência, relatório detalhado sobre o incidente de segurança da informação identificado, seus impactos, medidas corretivas implantadas e a implantar.
- 1.36. A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores e dos demais a seguir:
  - a) Quantidade de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, que obtiveram nota mínima de aprovação no treinamento relacionado a Segurança da Informação mencionado no item 2.3 / Quantidade total de empregados e colaboradores, que atuam na prestação de serviço objeto do contrato, em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
  - b) Quantidade de relatórios, referidos no item 3.6, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
  - c) Quantidade de relatórios, referidos no item 1.11, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido anualmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base.
- 1.37. A CONTRATADA deve garantir a continuidade do processamento das informações críticas de negócios, no caso de contratação de bem ou serviço de suporte às atividades críticas da CAIXA.
- 1.38. A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos.
- 1.39. A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.

#### **1.40. CLÁUSULAS DE PRIVACIDADE DE DADOS**

- 1.40.1. A CONTRATADA deverá emitir concordância com a seguinte cláusula referente à Privacidade dos Dados:

- 1.40.2. A CONTRATADA deve tomar conhecimento dos termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD e de suas regulamentações, bem como das orientações da ANPD – Autoridade Nacional de Proteção de Dados, reconhecendo sua responsabilidade objetiva e de seus empregados/colaboradores em observar o disposto na LGPD no exercício de suas atividades no tratamento de dados pessoais de clientes, empregados e colaboradores da CONTRATANTE.
- 1.40.3. Para fins deste contrato, a CAIXA, doravante denominada de “CONTRATANTE”, assume o papel de Controladora de dados pessoais, e a empresa [identificar a empresa contratada], doravante denominada “CONTRATADA”, assume o papel de operadora de dados pessoais.
- 1.40.4. Para a execução da finalidade prevista no presente contrato, a CONTRATANTE colocará à disposição da CONTRATADA:
- a) os dados pessoais envolvidos [descrever quais dados, como nome, telefone, CPF etc.];
  - b) a categoria dos dados [informar se são dados pessoais, dados pessoais sensíveis, dados pessoais de crianças e adolescentes etc.];
  - c) a natureza das operações realizadas [relacionar o tipo de operação; ex. coleta, armazenamento, eliminação, inclusive a eliminação de arquivos temporários etc.];
- 1.40.5. A CONTRATADA se compromete a tratar os dados pessoais a que tiver acesso em decorrência do presente Contrato, única e exclusivamente para cumprir a finalidade a que se destina seu tratamento, responsabilizando-se por qualquer acesso indevido.
- 1.40.6. A CONTRATADA deve garantir a confidencialidade no tratamento de dados pessoais, protegendo-os contra acesso, modificação, destruição ou divulgação não autorizada.
- 1.40.7. A CONTRATADA está autorizada a tratar, em nome da CONTRATANTE, os dados pessoais a que tiver acesso em decorrência do presente Contrato para as seguintes finalidades [relacionar a(s) finalidade(s) que justifica(m) o tratamento de dados pessoais - ex.: confeccionar cartão de crédito, enviar correspondência em nome da CAIXA etc.].
- 1.40.8. A CONTRATADA deverá, quando do término das atividades de tratamento de dados pessoais ou ao final do contrato, a critério da CONTRATANTE, OPÇÃO 1 [eliminar todos os dados pessoais] ou OPÇÃO 2 [devolver todos os dados pessoais], acompanhados de todas as cópias.
- 1.40.9. A CONTRATADA deve manter, por escrito, o registro das operações de tratamento realizadas em nome da CONTRATANTE.
- 1.40.10. A CONTRATADA deve colaborar com a CONTRATANTE no cumprimento de sua obrigação de responder às solicitações de exercício dos direitos dos titulares.
- 1.40.11. A CONTRATADA deve comunicar imediatamente a CONTRATANTE o recebimento de requisição do titular de dados no exercício de seus direitos.

- 1.40.12. A CONTRATADA garantirá à CONTRATANTE a disponibilização de todas as informações necessárias para que esta consiga demonstrar o cumprimento de suas obrigações nos termos da LGPD, mantendo a documentação disponível para a realização de auditorias e quaisquer inspeções.
- 1.40.13. A CONTRATADA deve obrigatoriamente adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- 1.40.14. A CONTRATADA notificará a CONTRATANTE de qualquer violação de dados pessoais imediatamente após tomar conhecimento, inclusive aplicando medidas de contenção, formalizando a ocorrência ao gestor operacional do contrato. Essa notificação deve ser acompanhada de todos os dados necessários para eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao(s) titular(es) de dados pessoais.
- 1.40.15. A CONTRATADA auxiliará a CONTRATANTE com as informações necessárias para cumprimento de suas obrigações junto à Autoridade Nacional de Proteção de Dados (ANPD) e quaisquer órgãos reguladores, de fiscalização, de supervisão e de controle, inclusive na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).
- 1.40.16. A CONTRATADA deverá notificar imediatamente a CONTRATANTE em caso de solicitações judiciais e de órgãos reguladores, de fiscalização, de supervisão e de controle para disponibilização de dados pessoais.
- 1.40.17. A CONTRATADA deverá solicitar autorização prévia da CONTRATANTE para subcontratação de outra empresa para quaisquer atividades que envolvam o tratamento de dados pessoais relativos ao presente contrato.
- 1.40.18. Em caso de concretização de subcontratação ou de sua rescisão, a CONTRATADA deverá enviar notificação mandatória sobre o fato à CONTRATANTE.
- 1.40.19. A CONTRATADA é responsável por quaisquer descumprimentos deste contrato pela empresa SUBCONTRATADA, inclusive em relação a incidentes de segurança com dados pessoais.
- 1.40.20. A CONTRATADA deverá observar os requisitos de privacidade desde a concepção em seus produtos, processos, serviços e soluções tecnológicas relacionadas ao tratamento de dados pessoais referentes a este contrato.
- 1.40.21. A CONTRATADA somente poderá realizar transferência de dados pessoais para terceiros seguindo as instruções da CONTRATANTE ou mediante prévia autorização.