

**SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS****1 SEGURANÇA DA INFORMAÇÃO - CLÁUSULAS GERAIS DE SEGURANÇA DA INFORMAÇÃO****1.1 Grau de Criticidade: Alto**

- 1.2 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>).
- 1.3 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.
- 1.4 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.
- 1.5 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.
- 1.6 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.
- 1.7 A CONTRATADA deve assegurar que os recursos e informações da CAIXA colocados à sua disposição sejam utilizados apenas para a finalidade contratada.
- 1.8 A CONTRATADA deve garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos.
- 1.9 A CONTRATADA deve cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais.
- 1.10 A CONTRATADA deve atender às Leis que regulamentam a atividade da CAIXA e seu mercado de atuação.
- 1.11 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.
- 1.12 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.

- 1.13 A CONTRATADA deve comunicar imediatamente à CAIXA qualquer descumprimento às cláusulas acima.
- 1.14 A CONTRATADA deve garantir que o(s) seu(s) dirigente(s), empregado(s) e colaborador(es) com acesso às informações da CAIXA assinem o Termo de Responsabilidade de Segurança da Informação – Exclusivo para Prestador de Serviço, anexo.
- 1.15 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, disponível no Portal Licitações CAIXA, devidamente assinado(s) por seu(s) dirigente(s), empregados(s) e colaborador(es).
- 1.16 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 o seguinte conteúdo:
- a) conhecimento da política de segurança da informação da empresa CONTRATADA e da CAIXA, mencionada no item 1.1;
  - b) uso seguro de informações corporativas a que tiver acesso;
  - c) proteção de dados e privacidade – LGPD – direitos do titular dos dados;
  - d) proteção de dados e privacidade – LGPD – responsabilidades do controlador, operador e do agente de tratamento dos dados;
  - e) uso seguro de dispositivos;
  - f) uso seguro de e-mails;
  - g) uso seguro de soluções em nuvem;
  - h) uso seguro de redes sociais e comunicadores instantâneos;
  - i) adoção da política de “mesa limpa”, “tela limpa” e “impressora limpa”;
  - j) formas defensivas contra phishing e smshing;
  - k) formas defensivas contra códigos maliciosos recebidos em dispositivos;
  - l) formas defensivas contra engenharia social;
  - m) formas de reporte de incidentes de segurança da informação na empresa e na CAIXA;
  - n) vazamento de dados e proteção de senhas;
  - o) metodologia e princípios da Privacy by Design e Secure by Design.
- 1.16.1 O treinamento referido será integralmente de responsabilidade da CONTRATADA, inclusive no que se refere aos custos, podendo ser de

forma presencial ou virtual, com carga horária mínima semestral de 04 horas.

- 1.17 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 1.15.
- 1.18 A CONTRATADA deve apresentar semestralmente, até o último dia útil do mês subsequente ao semestre anterior, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA.
- 1.19 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.
- 1.20 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.
- 1.21 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, no último semestre dividido pela Quantidade total de empregados, que atuam na prestação de serviço objeto do contrato, em percentual, medido semestralmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;
- 1.22 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.
- 1.23 No encerramento/extinção do contrato a CONTRATADA se compromete a:
  - a) 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;
  - b) Devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.
- 1.24 O não atendimento pela CONTRATADA de qualquer requisito de segurança definido no presente instrumento contratual, implicará em:
  - a) Multa e/ou
  - b) Suspensão temporária de participação em licitação e contratação com a CAIXA, por prazo não superior a 2 (dois) anos.

- c) A CAIXA poderá solicitar a apresentação de Plano de Melhoria à CONTRATADA constatado o não atendimento a qualquer requisito de segurança definido no instrumento contratual.
  - d) Constatada a execução insatisfatória do Plano de Melhoria, a CAIXA, a seu critério, poderá promover a rescisão antecipada do CONTRATO, ressaltado o seu direito à indenização pelos prejuízos eventualmente constatados e aplicação da penalidade contratual a ela associada.
- 1.25 Em caso de indisponibilidade parcial ou total do serviço contratado, a CONTRATADA se compromete a atender e cumprir com suas responsabilidades por meio do plano de continuidade do negócio construído em parceria com a CAIXA.
- 1.26 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.
- 1.27 No encerramento/extinção do contrato a CONTRATADA se compromete a:
  - a) entregar a versão mais atualizada de todos os artefatos, componentes e demais produtos por ele produzidos durante a vigência do contrato;
  - b) executar a exclusão e sanitização de dados e informações confidenciais após a devida cópia/transferência para a CONTRATANTE ou a quem ela indicar, observada a regulamentação vigente;
  - c) devolver ou transferir a quem for designado pela CONTRATANTE todos os ativos que lhe foram cedidos no mesmo estado que estavam no momento da cessão.
- 1.28 Além das cláusulas previstas no item 1, também se aplicam a este tipo de objeto contratual as cláusulas estabelecidas no item 2.
- 1.29 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, disponível no Portal Licitações CAIXA.
- 1.30 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.
- 1.31 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.

- 1.32 A CONTRATADA deve sensibilizar semestralmente seus empregados e colaboradores, por meio de treinamento com conteúdo de segurança da informação, podendo ser de forma presencial ou virtual, com carga horária mínima semestral de 08 horas.
- 1.32.1 O conteúdo de segurança da informação mencionado, consta no item 2.3.
- 1.33 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 3.5 e, caso estabelecido pela CONTRATANTE.
- 1.34 A CONTRATADA deve emitir relatórios, semestralmente, até o último dia útil do mês subsequente ao término do semestre base, relacionados aos seus riscos de segurança da informação e cibernéticos identificados, medidos, mitigados e monitorados e que possam trazer algum impacto à CONTRATANTE.
- 1.34.1 O relatório deve proporcionar à CAIXA identificar até que ponto os riscos de segurança da informação e cibernéticos aos quais a CONTRATADA está submetida pode impactar os negócios da CAIXA.
- 1.35 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.
- 1.36 A CONTRATADA deve manter processo de monitoramento e resposta a incidentes de segurança da informação adequado ao objeto contratual.
- 1.37 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.
- 1.38 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.
- 1.39 A CONTRATADA deverá informar ao CONTRATANTE periodicamente, os resultados dos indicadores mencionados no item 2.10 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 semestralmente e informado à CONTRATANTE anualmente, até o último dia útil do mês subsequente ao ano base;

b) Quantidade de relatórios, referidos no item 3.7, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido semestralmente e informado à CONTRATANTE semestralmente, até o último dia útil do mês subsequente ao semestre base;

c) Quantidade de relatórios, referidos no item 3.12, enviados à CONTRATANTE dentro do prazo estipulado / Quantidade esperada de relatórios a serem emitidos pela CONTRATADA em percentual, medido semestralmente e informado à CONTRATANTE semestralmente, até o último dia útil do mês subsequente ao semestre base.

- 1.40 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.

## **2 PRIVACIDADE DE DADOS**

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

- 2.1.1 As Partes declaram que cumprem a legislação brasileira sobre privacidade, incluindo-se a Lei n. 13.079/2018.

- 2.1.1.1 E, em caso de armazenamento de dados pessoais, a CAIXA se compromete a adotar as medidas de segurança para proteger dados pessoais, e a CONTRATADA atesta que obteve as aprovações necessárias para o uso dos dados cadastrais ora informados, com a finalidade de autenticação e autorização de acesso às dependências da CAIXA e aos equipamentos objeto do contrato.

- 2.1.2 As Partes têm conhecimento que as autorizações poderão ser revogadas a qualquer momento pela respectiva pessoa natural, mediante simples requerimento e, portanto, se comprometem a informar uma a outra a respeito de tais revogações de consentimento, a fim de que as devidas medidas sejam tomadas.