POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA CREDISIS (RESUMO)

CrediSIS
Sistema de Crédito Cooperativo

www.credisis.com.br

FICHA-CONTROLE

Título:	**Política de Segurança da Informação do Sistema CrediSIS (Resumo)**
Autoria	Setor de Segurança da Informação
Status	Aprovado
Órgão Homologador	Conselho de Administração
Data da Homologação	27/08/2025
Classificação do Documento	Público

HISTÓRICO DE VERSIONAMENTO

Versão	Descrição	Responsável	Aprovação
1.0	Versão inicial do documento	Segurança da Informação	Reunião Extraordinária do CONSAD de 27/08/2025

SUMÁRIO

1. OBJETIVO

Art 1º Este documento descreve diretrizes e responsabilidades sobre os principais aspectos relacionados à Política de Segurança da Informação divulgada internamente, visando preservar a confidencialidade, integridade e disponibilidade das informações sob responsabilidade do CrediSIS.

2. PÚBLICO ALVO

Art 2º Este documento é direcionado ao público geral e também aos prestadores de serviço e terceiros que mantêm relacionamento com as instituições do Sistema CrediSIS.

3. RESPONSABILIDADES

Art 3º O Sistema CrediSIS define responsabilidades específicas para todos os colaboradores, terceiros, bem como a Alta Administração.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

Art 4º O Sistema CrediSIS adota uma política específica que define diretrizes claras para a classificação, manuseio e rotulagem das informações. Essas diretrizes são baseadas na sensibilidade e importância de cada tipo de informação, garantindo a sua integridade, confidencialidade e disponibilidade conforme necessário.

5. PROTEÇÃO DE DADOS

Art 5º O Sistema CrediSIS mantém em sua estrutura organizacional um Encarregado de Proteção de Dados, que é responsável pelas atribuições legalmente estabelecidas na LGPD e por coordenar as diretrizes e operações do tema.

6. POLÍTICA DE SENHA

Art 6º O Sistema CrediSIS adota um conjunto de normas e diretrizes para assegurar a segurança das senhas. Isso inclui requisitos como comprimento, uso de caracteres

especiais, letras maiúsculas e minúsculas, números, e a necessidade de atualização periódica das senhas. Essas medidas visam fortalecer a segurança do sistema, protegendo as informações confidenciais contra acessos não autorizados.

7. SEGURANÇA FÍSICA

Art 7º O Sistema CrediSIS implementa medidas de segurança física rigorosas para proteger suas instalações contra potenciais ameaças, como perda, roubo, furto ou acesso não autorizado. Essas medidas visam garantir a integridade e a proteção dos recursos físicos da instituição, proporcionando um ambiente seguro para seus clientes, colaboradores e demais partes interessadas.

8. LICENCIAMENTO DE SOFTWARES

Art 8º O Sistema CrediSIS segue rigorosos padrões para o uso ético, legal e eficiente de softwares, evitando assim violações de direitos autorais e possíveis penalidades legais. É estritamente proibido o uso de softwares piratas ou não licenciados.

9. CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Art 9º Programas de conscientização, divulgação e reciclagem do conhecimento da política ou de seus temas são estabelecidos e praticados regularmente, para garantir que todos que tenham relação com informações de responsabilidade do CrediSIS saibam as diretrizes e as responsabilidades relacionadas à sua segurança.

10. PRÁTICAS DE MESA LIMPA E TELA LIMPA

Art 10 O Sistema CrediSIS adota uma política interna que orienta práticas de limpeza de mesas e telas, visando evitar a exposição indevida de informações sensíveis e prevenir o acesso não autorizado a dados confidenciais. Essa abordagem garante a proteção dos dados da instituição e dos seus clientes, promovendo a segurança da informação em todos os níveis operacionais.

11. CRIPTOGRAFIA

Art 11 O Sistema CrediSIS estabelece uma política interna que inclui recursos técnicos robustos para a utilização de criptografia e certificados digitais. Essas medidas visam proteger as informações sensíveis e confidenciais da cooperativa contra acesso não autorizado e prevenir o vazamento de dados internos. Essa abordagem reforça a segurança da informação, assegurando a integridade e confidencialidade dos dados da instituição.

12. GESTÃO DE VULNERABILIDADE

Art 12 O processo de Gestão de Vulnerabilidades realiza a identificação de vulnerabilidades, por meio de verificações contínuas, realizadas por ferramentas de varredura automatizadas no ambiente de infraestrutura do Sistema CrediSIS, visando garantir a segurança e integridade do ambiente de TI, bem como o tratamento eficaz das vulnerabilidades para mitigar riscos e proteger os ativos da instituição.

13. PROTEÇÃO CONTRA MALWARE

Art 13 O Sistema CrediSIS implementa uma política de proteção contra malware que inclui diretrizes e práticas para prevenir, detectar e responder a ameaças desse tipo, contando com software antivírus e anti-malware atualizados. Isso garante a segurança dos sistemas e dados, protegendo-os contra danos, roubo ou comprometimento causado por ameaças maliciosas.

14. DESENVOLVIMENTO SEGURO

Art 14 O Sistema CrediSIS adota uma política interna de desenvolvimento de software com foco em requisitos de segurança da informação. O objetivo é garantir a entrega de aplicações seguras e confiáveis para os cooperados, integrando requisitos de segurança desde a concepção inicial até a implementação em ambientes de produção. Essa abordagem visa proteger os dados dos cooperados e promover a confiança nas soluções tecnológicas oferecidas pela cooperativa.

15. GESTÃO DE FORNECEDOR

Art 15 Para garantir a segurança em todas as etapas da cadeia de suprimentos, o Sistema CrediSIS estabelece uma política interna de gestão de fornecedores. Esta política inclui a verificação da conformidade dos fornecedores com as principais leis e normas de segurança da informação do mercado. Além disso, realiza o acompanhamento anual dos planos de ação dos fornecedores, quando aplicável, para assegurar a integridade e confidencialidade dos dados em todo o processo de fornecimento.

16. CONTINUIDADE DE NEGÓCIOS

Art 16 São elaborados cenários de incidentes de segurança da informação, especialmente de segurança cibernética, que avaliem os procedimentos e controles aplicados, observando como diretrizes:

I. O possível impacto aos negócios;
II. A tendência do cenário de ameaças.

17. BACKUP

Art 17 O Sistema CrediSIS adota soluções de Backup e Disaster Recovery para a proteção de seus dados contra perda de informação, sendo realizado testes periódicos para garantir a integridade dos dados de backup.

18. GESTÃO DE INCIDENTES

Art 18 O Sistema CrediSIS implementa uma política dedicada a este assunto, que abrange as responsabilidades das diversas áreas no que diz respeito à prevenção e resposta. Essa política inclui diretrizes detalhadas sobre como priorizar incidentes e avaliar sua gravidade, seguindo as melhores práticas reconhecidas.

19. DISPOSIÇÕES FINAIS

Art 19 Esta política deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

Art 20 A política a que se refere este resumo foi aprovada em reunião extraordinária realizada em 24 de abril de 2024.