POLÍTICA DE SEGURANÇA CIBERNÉTICA

Uniprime
cooperativa de crédito

INTRODUÇÃO

O Sistema Uniprime reconhece a segurança cibernética como elemento essencial para a proteção das informações, a continuidade dos negócios e a confiança de parceiros, cooperados, colaboradores e demais partes interessadas.

A Política de Segurança Cibernética estabelece diretrizes e princípios para proteção dos dados, sistemas e serviços, alinhados às melhores práticas de mercado e às exigências regulatórias aplicáveis.

OBJETIVO

Esta Política tem como objetivo:

- Proteger a confidencialidade, integridade e disponibilidade das informações;
- Prevenir, detectar e responder a incidentes de segurança cibernética;
- Promover a continuidade dos negócios e a resiliência operacional;
- Assegurar conformidade com normas legais e regulatórias;
- Fortalecer a cultura de segurança da informação em todo o Sistema Uniprime.

PAPÉIS E RESPONSABILIDADES

A estrutura de governança do Sistema Uniprime é organizada a partir da definição de responsabilidades específicas, divididas entre o Conselho de Administração, Diretoria Executiva, Diretoria Responsável pela Segurança Cibernética, Área de Segurança Cibernética, Área de Gerenciamento de Riscos de Conformidade, Supervisão Auxiliar, Área ou Responsável Técnico pela Tecnologia da Informação e Singulares.

PRINCÍPIOS

As ações de segurança cibernética do Sistema Uniprime são orientadas pelos seguintes princípios:

- Confidencialidade das informações;
- Integridade dos dados e sistemas;
- Disponibilidade dos serviços e operações;
- Autenticidade das informações;
- Conformidade com leis, normas e regulamentos;
- Controle adequado de acessos e privilégios.

DIRETRIZES GERAIS

As diretrizes de segurança da informação e cibernética do Sistema Uniprime determinam a adoção de medidas para proteger dados e informações, assegurando sua disponibilidade, integridade e resiliência. A gestão da segurança deve ser baseada em riscos, alinhada às melhores práticas de mercado e voltada à conscientização dos colaboradores, garantindo também a conformidade com a legislação, normas e regulamentações aplicáveis.

As informações são classificadas em Públicas, Internas, Confidenciais e Sensíveis, de acordo com sua relevância, para que recebam tratamento adequado e compatível com os riscos, os processos e as exigências legais e regulatórias.

INCIDENTES DE SEGURANÇA

O Sistema Uniprime mantém uma estrutura contínua de resposta a incidentes de segurança cibernética e privacidade, visando detectar, conter, eliminar e recuperar rapidamente eventos adversos, reduzindo impactos operacionais,

financeiros, legais e reputacionais. Para isso, são observadas as seguintes diretrizes:

Gestão e tratamento contínuo: os incidentes devem ser registrados, classificados, analisados e tratados, conforme o Plano de Ação e de Resposta a Incidentes.

Registro e Lições Aprendidas (Melhoria Contínua): incidentes relevantes devem ser documentados e analisados para identificar causas e incorporar lições aprendidas aos controles de segurança.

Comunicação e Compartilhamento de Ameaças: devem existir fluxos para notificação tempestiva da Alta Administração, titulares de dados e órgãos reguladores, além do compartilhamento seguro de informações sobre ameaças com instituições do Sistema Financeiro Nacional.

Reporte à Alta Administração: anualmente, o Sistema Uniprime deve elaborar relatório sobre a implementação do plano, incluindo a efetividade das ações, resultados dos controles adotados, incidentes relevantes ocorridos, testes de continuidade de negócios e avaliações de vulnerabilidades.

MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES

Além das diretrizes estabelecidas nesta Política, o Sistema Uniprime adota um conjunto abrangente de medidas de segurança, procedimentos e controles voltados à proteção dos dados, dos ambientes tecnológicos e à continuidade dos negócios.

Essas medidas abrangem o controle de acesso e autenticação, a criptografia, a proteção das informações, a segurança das informações sensíveis, a prevenção de vazamento de dados, os mecanismos de rastreabilidade, a prevenção e detecção de intrusões, a identificação e gestão de vulnerabilidades, a proteção contra softwares maliciosos, o armazenamento e backup de dados, a gestão de ativos de tecnologia, os mecanismos de proteção de rede, a gestão de certificados digitais e os requisitos de segurança para integração de sistemas.

Também compreendem a inteligência de ameaças e o monitoramento contínuo, a gestão de prestadores de serviços e dos riscos na cadeia de suprimentos, a aquisição, desenvolvimento e manutenção segura de sistemas, a segurança física e ambiental, as diretrizes para utilização de Inteligência Artificial e IA Generativa, os controles aplicáveis à comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional (RSFN), a conexão com Sistemas do Mercado Financeiro (SMF) e a gestão da continuidade dos negócios, observando as exigências legais, regulatórias e as melhores práticas de segurança da informação e cibernética.

CONTRATAÇÃO DE SERVIÇOS DE DADOS E COMPUTAÇÃO EM NUVEM

A contratação de serviços de processamento, armazenamento de dados e computação em nuvem deve ser precedida de avaliação formal da capacidade do prestador em garantir a confidencialidade, integridade, disponibilidade e recuperação das informações. A análise deve considerar a criticidade do serviço, a sensibilidade e a classificação dos dados envolvidos, sendo condicionada a estudo de relevância e risco e parecer técnico da área de Tecnologia da Informação da Central. Os requisitos específicos para contratação são

complementados por normativos próprios do Sistema Uniprime.

CULTURA DE SEGURANÇA CIBERNÉTICA

A Uniprime promoverá continuamente ações de conscientização, capacitação e treinamento em segurança da informação e segurança cibernética para colaboradores, prestadores de serviços e profissionais de tecnologia, bem como a divulgação periódica de orientações de segurança digital aos cooperados. As cooperativas singulares deverão prever treinamentos e ações de conscientização específicas para suas estruturas locais.

GOVERNANÇA, CONTROLE E CONFORMIDADE

O Sistema Uniprime manterá mecanismos de acompanhamento e controle para assegurar a efetividade desta Política e de seus normativos complementares, por meio de revisões periódicas, testes de segurança, trilhas de auditoria e procedimentos para correção de deficiências. O descumprimento das disposições estabelecidas sujeitará os responsáveis às medidas disciplinares e penalidades cabíveis, sem prejuízo das responsabilidades legais aplicáveis.

ATUALIZAÇÃO E DIVULGAÇÃO

O Sistema Uniprime reafirma seu compromisso com a transparência e com a ampla divulgação das diretrizes institucionais relacionadas à segurança cibernética.

A Política será revisada sempre que houver alterações relevantes na legislação ou nas práticas de negócios do Sistema Uniprime ou eventos que justifiquem sua atualização.

Uniprime
cooperativa de crédito