CooperSKF

POLÍTICA DE SEGURANÇA CIBERNÉTICA – RESUMO

A Política de Segurança Cibernética foi revisada em atendimento à Resolução nº 4.893 de 26 de fevereiro de 2021, emitida pelo Banco Central do Brasil e estabelece os princípios, conceitos, valores e práticas que devem ser adotados pelo Conselho de Administração, Diretoria, empregados e colaboradores da **Cooperativa de Crédito Mútuo dos Empregados da SKF e Coligadas**, assegurando a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

São princípios básicos da segurança da informação:

- Confidencialidade: Proteção da informação compartilhada contra acessos não autorizados;
- Integridade: Garantia da veracidade da informação;
- Disponibilidade: Prevenção contra as interrupções das operações da instituição como um todo.

Sobre a Política de Segurança Cibernética da **CooperSKF** tem se a observar:

- Foi aprovada pelo Conselho de Administração da Cooperativa;
- A empresa contratada para fornecimento de Software e prestação de serviço de suporte e manutenção, conforme estabelecido em contrato, é responsável pela gestão de segurança cibernética do sistema operacional e pelo armazenamento dos dados em nuvem. São hospedados utilizando a estrutura da Amazon AWS, empresa multinacional e líder mundial na prestação dos serviços de armazenamento em nuvem, com garantia de alta disponibilidade, sigilo, segurança e acessibilidade ao sistema e dados hospedados;
- A gestão contratada não desonera a responsabilidade da Cooperativa, na qual deve também, indicar diretor responsável pelo gerenciamento da segurança cibernética na entidade que administra. O diretor indicado poderá exercer outras funções, desde que não haja conflito de interesses;
- Foi divulgada a todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados) da Instituição e às demais pessoas com acesso autorizado às informações da Cooperativa, incluindo associados, parceiros, empresas prestadoras de serviço e ao público;
- Reforça o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

São objetivos dessa Política:

- A definição de diretrizes para a segurança do espaço cibernético, relacionadas à capacidade da **CooperSKF** de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- A proteção das informações sob responsabilidade da Cooperativa preservando sua confidencialidade, integridade, disponibilidade e autenticidade;
- A prevenção de eventual interrupção, total ou parcial, dos serviços de TI acessados pela Cooperativa e pelos associados e, no caso de sua ocorrência, a redução dos impactos dela resultantes;
- O tratamento e prevenção de incidentes de segurança cibernética;
- A formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;
- A promoção do intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética;
- Os requisitos a serem observados para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Das responsabilidades:

Do Conselho de Administração:

- Revisar e aprovar, anualmente, as políticas e estratégias de gerenciamento de segurança cibernética e da informação;
- Promover a disseminação da cultura de gerenciamento de segurança cibernética.

Da Diretoria Executiva:

- Assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de segurança cibernética;
- Definir o Diretor responsável pela gestão de segurança cibernética.

Do Diretor responsável pela Segurança Cibernética:

- Supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, plano de ação e de respostas a incidentes, incluindo seu aperfeiçoamento;
- Subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética;

- Responsabilizar-se pela capacitação adequada dos empregados que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles.

Da Estrutura Contratada de Gestão de Segurança Cibernética:

- Providenciar o relacionamento com órgãos de supervisão internos e externos;
- Prestar apoio a Cooperativa contratante, relativo à gestão de segurança cibernética;
- Informar à Cooperativa contratante sobre os incidentes cibernéticos relevantes;
- Reportar à Diretoria da Cooperativa as informações relativas à gestão centralizada de segurança cibernética;
- Compartilhar informações sobre incidentes cibernéticos relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Dos Empregados e Colaboradores da Cooperativa:

- Fazer recomendações de aperfeiçoamento da política, planos, controles e procedimentos relacionados à segurança cibernética;
- Executar os procedimentos descritos nas políticas, planos e manuais relativos ao tema;
- Reportar ao Diretor responsável / Diretoria as informações referentes à segurança cibernética.

Dos procedimentos e controles:

Para reduzir a vulnerabilidade da Cooperativa a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, deverão ser adotados procedimentos e controles, conforme o porte e perfil de risco da Cooperativa, tais como:

- Autenticação, criptografia;
- Prevenção e detecção de intruso;
- Prevenção de vazamento de informações;
- Proteção contra softwares maliciosos;
- Mecanismos de rastreabilidade;
- Controles de acesso e segmentação de rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações.

Os procedimentos e controles deverão ser aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

Deverá ser estabelecido plano de ação e de resposta a incidentes, revisado, anualmente.

As informações de propriedade ou sob custódia da Cooperativa, mantidas em meio eletrônico ou físico, deverão ser classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de Informação utilizados.

Todo incidente de segurança cibernético considerado relevante será avaliado e comunicado ao Banco Central do Brasil.

Serão adotados mecanismos para disseminação da cultura de segurança cibernética na Cooperativa, incluindo:

- Implementação de programas de capacitação e de avaliação periódica de pessoal;
- Prestação de informações a associados e usuários sobre precauções na utilização de produtos e serviços financeiros;
- As políticas da Amazon de segurança compliance e SLA podem ser acessadas nos links:
  https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
  https://aws.amazon.com/pt/compliance/programs/
  https://d1.awsstatic.com/legal/amazon-ec2-sla/Amazon_EC2_Service_Level_Agreement_-_Portuguese_Translation__2018-02-12_.pdf

Complementam essa política e a ela se subordinam todas as normas e procedimentos.