CooperSKF

ANEXO IV – RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVOS

Esta Política de Segurança Cibernética tem por objetivo estabelecer princípios, diretrizes, procedimentos e controles destinados a assegurar a confidencialidade, a integridade, a disponibilidade e a rastreabilidade dos dados, das informações e dos sistemas utilizados pela **Cooperativa de Crédito Mútuo dos Empregados da SKF e Coligadas,** compatíveis com seu porte, perfil de risco, modelo de negócio, natureza das operações e sensibilidade dos dados sob sua responsabilidade, em conformidade com a Resolução nº 4.893/2021 e a Resolução nº 5.274/2025, publicadas pelo Conselho Monetário Nacional (CMN), bem como demais alterações posteriores.

2. CONCEITO – ESPAÇO CIBERNÉTICO

O Espaço Cibernético é um ambiente resultante da interação de pessoas, software e serviços na internet, suportado por instrumentos físicos de tecnologia da informação e comunicação e redes conectadas e distribuídas e que interagem diretamente com o ambiente de negócios da Cooperativa.

3. APLICAÇÃO

Esta política aplica-se ao Conselho de Administração, Diretoria Executiva, empregados, terceiros (fornecedores e prestadores de serviços) e aqueles tenham acesso aos dados da Cooperativa ou aos sistemas informatizados por ela utilizados.

4. AMEAÇAS

As ameaças à segurança da informação correspondem a eventos, ações ou condições com potencial de explorar vulnerabilidades e comprometer a confidencialidade, a integridade, a disponibilidade, a autenticidade ou a privacidade dos ativos de informação da Cooperativa.

Tais ameaças podem impactar tanto os ativos pessoais quanto os ativos organizacionais, ocasionando prejuízos operacionais, financeiros, reputacionais e regulatórios. Para fins desta Política, as ameaças são classificadas nas seguintes categorias:

a) ameaças aos ativos pessoais**:** ameaças aos ativos pessoais referem-se a questões de identidade, representadas pelo vazamento ou roubo de informações pessoais;

b) ameaças aos ativos organizacionais: ameaças aos negócios referem-se a transações realizadas pela Cooperativa e informações de empregados, associados, terceiros (fornecedores e prestadores de serviços), registros financeiros e a infraestrutura que suporta a internet e o espaço cibernético.

5. DIRETRIZES

A Diretoria Executiva com anuência do Conselho de Administração, comprometida com a melhoria contínua da segurança cibernética, definiu diretrizes para implementação, manutenção e aperfeiçoamento do gerenciamento do risco cibernético, observando, no mínimo, a prevenção, a detecção, a resposta, a recuperação e a rastreabilidade de incidentes, a classificação e proteção dos dados e informações, a capacitação dos usuários, o desenvolvimento seguro de sistemas, a adoção segura de novas tecnologias e a aderência aos requisitos regulatórios aplicáveis.

a) definição de procedimentos e controles voltados à prevenção, detecção, resposta e recuperação de incidentes de segurança cibernética;

b) classificação dos dados e das informações quanto à criticidade, relevância e sensibilidade, com controles de acesso compatíveis;

c) desenvolvimento seguro de sistemas de informação e aplicação dos controles de segurança cibernética na adoção de novas tecnologias, inclusive em sistemas adquiridos ou desenvolvidos por terceiros, quando executados com recursos computacionais da Cooperativa.

6. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES

A Diretoria Executiva estabeleceu plano de ação e de resposta a incidentes visando à implementação desta Política de Segurança Cibernética, contemplando a adequação das estruturas organizacional e operacional, a definição de responsabilidades, os procedimentos de acionamento, escalonamento, registro, tratamento e comunicação de incidentes, bem como as rotinas, os controles e as tecnologias a serem utilizados na prevenção, detecção, resposta e recuperação.

O Diretor responsável pela Política de Segurança Cibernética é responsável pelo registro, monitoramento, controle dos efeitos e reporte interno dos incidentes relevantes, bem como pelo apoio à comunicação tempestiva aos órgãos reguladores, quando aplicável.

7. CONTRATAÇÃO DE SERVIÇOS

A Cooperativa, em conformidade com a regulamentação do Banco Central do Brasil (BCB) e com as políticas internas, estabeleceu critérios para a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, observando a criticidade do serviço, a sensibilidade dos dados envolvidos, a capacidade técnica, operacional e de segurança do prestador e os requisitos contratuais e de monitoramento contínuo aplicáveis, considerando:

a) requisitos de decisão quanto à terceirização de serviços e contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior;

b) processos procedimentos de verificação da capacidade técnica, operacional e tecnológica do potencial prestador de serviços, incluindo a avaliação da criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;

c) procedimentos de comunicação junto ao Banco Central do Brasil (BCB) acerca da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;

d) atendimento aos requisitos para contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, quando aplicável;

e) requisitos quanto a formalização de contratação de prestadores de serviços em conformidade com as diretrizes da Resolução CMN Nº 4.893/21, contendo cláusulas contratuais previstas no regulamento.

8. TRATAMENTO DE INCIDENTES

A Diretoria Executiva, conforme diretrizes do Banco Central do Brasil (BCB) e políticas internas, estabeleceu mecanismos para tratamento de incidentes, incluindo procedimentos de registro, análise, escalonamento, contenção, resposta, recuperação e comunicação, bem

como medidas aplicáveis em caso de interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, observados os cenários considerados nos testes de continuidade de negócios.

9. PROCEDIMENTOS DE GERENCIAMENTO DE RISCOS E DE CONTINUIDADE

A Diretoria Executiva conforme instruções do Banco Central do Brasil (BCB) e políticas internas, estabeleceu procedimentos para gerenciamento de riscos e gestão da continuidade de negócios, incluindo:

a) tratamento previsto para mitigar os efeitos dos incidentes relevantes;

b) prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;

c) a comunicação tempestiva ao Banco Central do Brasil (BCB) das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes.

10. MECANISMOS DE CONTROLE CHAVE

A Cooperativa adota mecanismos de controle compatíveis com a criticidade de seus ativos, processos e integrações, observando, no mínimo, os controles técnicos e administrativos exigidos pela regulamentação vigente, considerando:

a) autenticação;

b) mecanismos de criptografia;

c) mecanismos de prevenção e detecção de intrusão;

d) mecanismos de prevenção de vazamento de informações;

e) mecanismos de proteção contra softwares maliciosos;

f) mecanismos de rastreabilidade;

g) gestão de cópias de segurança dos dados e das informações;

h) avaliação e correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação;

i) controles de acesso;

j) definição e implementação de perfis de configuração segura de ativos de tecnologia;

k) mecanismos de proteção da rede;

l) gestão de certificados digitais;

m) requisitos de segurança para integração de sistemas de informação por meio de interfaces eletrônicas;

n) ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de interesse da instituição na internet, na Deep Web, na Dark Web e em grupos privados de comunicação.

11. COMPARTILHAMENTO DE INFORMAÇÕES

O Compartilhamento de Informações sobre Incidentes Cibernéticos Relevantes poderá ser realizado por intermédio da Federação Nacional das Cooperativas de Crédito – FNCC, por meio do registro na Central de Atendimento, por meio do link: https://fncc.octadesk.com/helpcenter/list-ticket/ e pelo e-mail fncc@fncc.com.br.

12. COMUNICAÇÂO AO BANCO CENTRAL DO BRASIL (BCB)

Todo incidente de segurança cibernética considerado relevante será avaliado e comunicado tempestivamente ao Banco Central do Brasil (BCB), nos termos da regulamentação aplicável.

A comunicação deverá contemplar, no mínimo, informações suficientes para caracterizar a ocorrência, avaliar seus impactos e demonstrar as medidas adotadas para tratamento e mitigação do evento, observados os seguintes aspectos:

a) a descrição do incidente, indicando dado ou informação sensível afetada e de que forma os associados foram afetados;

b) avaliação sobre o número de associados potencialmente afetados;

c) medidas já adotadas pelo Cooperativa ou as que pretende adotar;

d) tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

e) qualquer outra informação considerada importante.

13. DIVULGAÇÃO DA POLÍTICA

A Política de Segurança Cibernética, bem como este resumo contendo suas diretrizes gerais, foram aprovados pelo Conselho de Administração estando devidamente publicados e divulgados a todos os envolvidos na administração da Cooperativa, empresas prestadoras de serviços, associados e demais partes externas relevantes, para o seu devido cumprimento.

14. CONSIDERAÇÕES FINAIS

Os detalhamentos das orientações com relação ao processo de segurança cibernética determinada pela Cooperativa estão descritos na Política de Segurança Cibernética.

A Política de Segurança Cibernética e seu resumo, serão revisados, no mínimo, anualmente ou sempre que ocorrerem mudanças relevantes no ambiente operacional, tecnológico, regulatório ou no perfil de risco da Cooperativa, de modo a assegurar sua contínua pertinência, adequação, eficácia e aderência às Resoluções CMN nº 4.893/2021 e nº 5.274/2025.

Cajamar, 26 de agosto de 2026.