RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVOS

Assegurar a proteção dos ativos de informação da CREDITA contra ameaças aos ativos pessoais ou organizacionais, de origem interna ou externa, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo.

Fornecer orientações gerais para funcionários da Cooperativa, cooperados e prestadores de serviços com foco em gerenciamento de riscos de segurança da informação, em especial a segurança de rede, segurança de internet e proteção da infraestrutura da informação.

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, comunicação e redes conectadas e distribuídas e que interagem diretamente com o ambiente de negócios da Cooperativa.

3. APLICAÇÃO

Esta política aplica-se aos funcionários da CREDITA e às empresas prestadoras de serviços de acordo com as funções desempenhadas e com a sensibilidade das informações tratadas.

4. AMEAÇAS

4.1 Ameaças aos Ativos Pessoais

Ameaças aos ativos pessoais referem-se a questões de identidade, representadas pelo vazamento ou roubo de informações pessoais.

4.2 Ameaças aos Ativos Organizacionais

Ameaças aos negócios referem-se a transações realizadas pela instituição e informações de funcionários, clientes, parceiros ou fornecedores, registros financeiros e a infraestrutura que suporta a internet e o espaço cibernético.

5. DIRETRIZES

A Diretoria da CREDITA, comprometida com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, definiu diretrizes para a implementação de gerenciamento de riscos de segurança cibernética visando proteger o espaço cibernético:

a) Elaboração de Cenários de incidentes a serem considerados no plano de continuidade de negócios.

b) A definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes.

c) Classificação dos dados e das informações quanto à sua relevância.

6. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES

A Diretoria estabeleceu plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética, abrangendo:

a) Adequação da estrutura organizacional e operacional às diretrizes da política de segurança cibernética.

b) Rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

c) A responsabilidade da gerência da Cooperativa pelo registro e controle dos efeitos de incidentes relevantes, quando aplicável.

7. CONTRATAÇÃO DE SERVIÇOS

Conforme diretrizes do Banco Central do Brasil e políticas internas, a Diretoria estabeleceu:

a) Critérios 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) 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) Protocolo de comunicação junto ao Banco Central acerca da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

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

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

8. TRATAMENTO DE INCIDENTES

A Diretoria da CREDITA, conforme diretrizes do Banco Central do Brasil e políticas internas, estabeleceu mecanismos de tratamento de incidentes, procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratado e cenários de incidentes considerados nos testes de continuidade de negócios.

9. PROCEDIMENTOS DE GERENCIAMENTO DE RISCOS E DE CONTINUIDADE

Conforme diretrizes do Banco Central do Brasil e políticas internas, a Diretoria estabeleceu procedimentos para gerenciamento de riscos e gestão da continuidade de negócios, incluindo:

- ✓ tratamento previsto para mitigar os efeitos dos incidentes relevantes.
- ✓ prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos.
- ✓ a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes

10. MECANISMOS DE CONTROLE CHAVE

Análise de Vulnerabilidade de Sistemas
Proteção contra Softwares Maliciosos
Teste de Intrusão
Gestão de Acessos Lógicos
Prevenção DDoS
Desenvolvimento Seguro de Sistemas
Prevenção de Vazamento de Informações

11. COMPARTILHAMENTO DE INFORMAÇÕES

A Cooperativa compartilhará as informações referente as ocorrências de incidentes cibernéticos relevantes por meio da Federação Nacional de Cooperativas de Crédito - FNCC, que dará conhecimento do ocorrido às demais cooperativas preservando as identidades dos envolvidos.

12. COMUNICAÇÃO AO BANCO CENTRAL

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

A Comunicação ao Banco Central deve incluir:

- ✓ a descrição do incidente, indicando dado ou informação sensível afetada e de que forma os clientes foram afetados;
- ✓ avaliação sobre o número de clientes potencialmente afetados;
- ✓ medidas já adotadas pelo Cooperativa ou as que pretende adotar;
- ✓ tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e
- ✓ qualquer outra informação considerada importante.

13. DIVULGAÇÃO DA POLÍTICA

Este resumo da política de segurança cibernética foi aprovado pela Diretoria Executiva e está publicado no site da instituição no endereço eletrônico

https://coopcredita.com.br/wp-content/uploads/2025/10/res-da-politica-de-seguranca-cibernetica.pdf, foi divulgado para todos os colaboradores e prestadores de serviços relevantes para o necessário cumprimento.

Este resumo será revisado periodicamente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.

Luciano Donisete Couto
Diretor Responsável pela Segurança Cibernética

Raquel Cássia de Campos
Diretora Presidente

Renata Delalana Figueredo
Diretora Operacional