ÍNDICE

1. OBJETIVO..... 2
2. CONCEITO..... 2
3. APLICAÇÃO..... 2
4. AMEACAS..... 3
4.1. Ameaças aos Ativos Pessoais..... 3
4.2. Ameaças aos Ativos Organizacionais..... 3
5. DIRETRIZES..... 3
6. PLANO DE AÇÃO/RESPOSTA A INCIDENTES..... 4
7. CONTRATAÇÃO DE SERVIÇOS..... 5
8. TRATAMENTO DE INCIDENTES..... 5
9. PROCEDIMENTOS DE GERENCIAMENTO DE RISCOS E DE CONTINUIDADE..... 5
10. MECANISMOS DE CONTROLE CHAVE..... 6
11. COMPARTILHAMENTO DE INFORMAÇÕES..... 6
12. COMUNICAÇÃO AO BANCO CENTRAL..... 7
13. DIVULGAÇÃO DO RESUMO..... 7

RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVOS

Assegurar a proteção dos ativos de informação da Cooperativa 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 Colaboradores da Cooperativa, cooperados e prestadores de serviços com foco em gerenciamento de riscos de segurança da informação, em especial a segurança da informação, 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, que interagem diretamente com o ambiente de negócios da Cooperativa.

3. APLICAÇÃO

Esta política aplica-se aos Colaboradores da Cooperativa 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 colaboradores, clientes, parceiros ou fornecedores, registros financeiros e a infraestrutura que suporta a internet e o espaço cibernético.

5. DIRETRIZES

A Diretoria Executiva da Cooperativa comprometida com a melhoria contínua dos procedimentos relacionados com a segurança cibernética definiu diretrizes para 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 Administração da Cooperativa conforme diretrizes estabelecidas pela Diretoria Executiva, estabelece plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética, abrangendo:

a) Adequação das estruturas 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 Coordenação da Cooperativa pelo registro e controle dos efeitos de incidentes relevantes, quando aplicável.

7. CONTRATAÇÃO DE SERVIÇOS

A Diretoria da Cooperativa, conforme diretrizes do Banco Central do Brasil e políticas internas, 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 4.658/18, contendo cláusulas contratuais previstas no regulamento.

8. TRATAMENTO DE INCIDENTES

A Diretoria da Cooperativa conforme diretrizes do Banco Central do Brasil e políticas internas estabelece, 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

A Diretoria da Cooperativa conforme diretrizes do Banco Central do Brasil e políticas internas, estabelece 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 DDpS
Desenvolvimento Seguro de Sistemas
Centro de operações de Segurança
Prevenção de Vazamento de Informações

11. COMPARTILHAMENTO DE INFORMAÇÕES

A Cooperativa em conjunto com a FNCC-Federação Nacional de Cooperativas de Crédito e demais federadas, criará um grupo de trabalho para avaliar alternativas de compartilhamento de informações sobre incidentes relevantes com instituições congêneres, incluindo no mínimo registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo:

a) Compartilhamento de Informações entre as Federadas da FNCC;

b) Compartilhamento de Informações entre a FNCC e outros componentes do Sistema Cooperativista.

12. COMUNICAÇÂO 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 DO RESUMO DA POLÍTICA

Este resumo foi aprovado pela Diretoria Executiva e está publicado e comunicado para todos os colaboradores, empresas contratadas de serviços, clientes e partes externas relevantes, para o necessário cumprimento.
O resumo da política será atualizado, toda vez que houver a revisão da Política de Segurança Cibernética.

Maria Aparecida Pereira
Diretora Presidente

Valdeci Pereira de Souza
Diretor Secretário