COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS EMPREGADOS DA MAGNESITA REFRATÁRIOS S.A LTDA
Praça Louis Ensch, 240 - Cidade Industrial - Contagem/MG - CEP: 32.210-050 - Tel.31 3368-1440/1441
E-mail: cecrem@cecrem.com.br - CNPJ: 00.913.314/0001-85 - Ouvidoria: 9090 98979-8832

RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA – 2023

1. OBJETIVOS

Atendendo ao art. 5º da Resolução nº 4.893/2021, disponibilizamos resumo da política de segurança cibernética contendo em linhas gerais, orientação aos colaboradores sobre procedimentos e controles em relação à segurança cibernética, contendo os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, assegurando 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 cibe segurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de segurança cibernética.

2. CONCEITO – CIBERESPAÇO

O "**ciberespaço**" é o ambiente criado de forma virtual através do uso dos meios de comunicação modernos destacando-se, entre eles, a internet. Este ambiente tornou-se possível graças a uma grande infraestrutura técnica na área de telecomunicação suportada 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. IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A política de segurança cibernética foi implementada e formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

4. APLICAÇÃO

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

5. AMEAÇAS

5.1 Ameaças aos Ativos Pessoais

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

5.2 Ameaças aos Ativos Organizacionais

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

6. DIRETRIZES

A Diretoria da Cooperativa 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.

7. PLANO DE AÇÃO / RESPOSTAS A INCIDENTES

A Cooperativa conforme diretrizes estabelecidas pela Diretoria, estabeleceu 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 Cooperativa pelo registro e controle dos efeitos de incidentes relevantes, quando aplicável.

8. CONTRATAÇÃO DE SERVIÇOS

A Diretoria da Cooperativa conforme diretrizes do Banco Central do Brasil e políticas interna, 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.

b) Procedimentos de verificação da capacidade técnica, operacional e tecnológica do 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) Comunicação junto ao Banco Central acerca da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

d) Permitir o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações.

9. TRATAMENTO DE INCIDENTES

A Diretoria da Cooperativa 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

10. PROCEDIMENTOS DE GERENCIAMENTO DE RISCOS E DE CONTINUIDADE

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

11. MECANISMOS DE CONTROLE

Garante a segurança das informações sensíveis onde apresentamos a seguir as principais orientações para manter o computador seguro

Softwares de detecção e proteção contra softwares maliciosos
Instalação de programas legítimos, de fonte confiáveis
Teste de intrusão
Prevenção de vazamento de informações
Controles de segurança de hardware e software, firewalls e filtros
Informações confidenciais de maneira criptografada
Centro de operações de segurança

12. COMPARTILHAMENTO DE INFORMAÇÕES

A Cooperativa irá 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.

13. 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 relevante.

14. DIVULGAÇÃO DO RESUMO DA POLÍTICA

O presente resumo da política foi aprovado pela Diretoria e divulgada ao público em linhas gerais, sendo as diretrizes e gerenciamento de riscos estão contidos na Política de Segurança Cibernética.

A Política de Segurança Cibernética será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.

Diretor Responsável

Foi designado diretor responsável pela política de segurança cibernética e pela execução do relatório anual de implementação e do plano de ação e de resposta a incidentes

Contagem/MG, 31 de janeiro de 2024.

Miguel Arcanjo de Barros
Diretor Administrativo
Responsável pela Politica de Segurança Cibernética