CECRESUL

CENTRAL DE COOPERATIVAS FINANCEIRAS

POL-SC – V.2

POLITICA DE SEGURANÇA CIBERNÉTICA

CECRESUL - Central das Cooperativas financeiras

Histórico de Revisão

Versão	Data	Elaborado por	Revisado por	Aprovado por	Descrição
1	25/10/2019	Gestão de Riscos e Controles Internos		Conselho de Administração	Documento inicial.
2	26/02/2021	Gestão de Riscos e Controles Internos		Conselho de Administração	Alteração para CECRESUL

POLÍTICA SEGURANÇA CIBERNÉTICA DO SISTEMA CECRESUL

Abrangência: ***Sistema CECRESUL***	Data da aprovação: 26/02/2021
Versão anterior: 25/10/2019	Órgão: ***Conselho de Administração***

Resumo: Este documento tem por objetivo atender o disposto na Resolução CMN 4.658, de 26 de abril de 2018, que trata sobre a Política de Segurança Cibernética.

Áreas Destinatárias:	**Área Responsável:**
• Todas as áreas	• Controles Internos/TI

Índice

1 Introdução

Atendendo ao disposto da Resolução n° 4.658 do Conselho Monetário Nacional de 26 de abril de 2.018, o Conselho de Administração da Central das Cooperativas de Crédito Mútuo do RS, Santa Catarina e Paraná – CECRESUL, no uso das atribuições que lhe confere o Estatuto Social e com base em deliberaçõestomadas em Reunião do Conselho de Administração, aprovou a Política de Segurança Cibernética do Sistema CECRESUL.

2 Publico Alvo

Dirigentes, colaboradores e prestadores de serviços do Sistema CECRESUL.

3 Definição

Este documento descreve diretrizes sobre a Política de Segurança Cibernética do Sistema CECRESUL e é parte integrante do conjunto de Políticas de Segurança da Informação que tem por objetivo orientar o uso aceitável dos ativos de informação e/ou tecnológicos da instituição, baseada nos princípios de confidencialidade, integridade e disponibilidade.

4 Objetivo

A presente Política tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança cibernética e promover a melhoria continua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com o ambiente cibernético, assim como possibilitar a manutenção da confidencialidade, da integridade e da disponibilidade das informações sob responsabilidade do Sistema CECRESUL.

5 Conceitos

A Segurança Cibernética, constitui-se em um conjunto de ações sobre pessoas, tecnologia e processos contra os ataques cibernéticos, na preservação das propriedades da informação, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

- ✓ **Confidencialidade:** Garantir que as informações são acessadas apenas por aqueles expressamente autorizados.

- ✓ **Integridade:** Preservar a Integridade da Informação. Garantir que todas as informações estão íntegras e precisas durante todo o ciclo: Criação, Processamento, Destruição.

- ✓ **Disponibilidade:** Garantir que os colaboradores, quando devidamente autorizados, tenham acesso às informações sempre que necessitarem.

- ✓ **Riscos Cibernéticos:** riscos de ataques internos ou externos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede, sabotagem, bem como violação de acessos e privacidade, que podem desproteger dados, redes e sistemas da empresa causando danos financeiros e de reputação ou imagem.

6 Procedimentos e Controles

O Sistema CECRESUL possui um conjunto de Políticas e procedimentos que tem por objetivo assegurar que as informações estejam adequadamente protegidas, baseadas nos requerimentos mínimos exigidos e nas melhores práticas reconhecidas pelo mercado, sendo estabelecidas as seguintes diretrizes:

Gestão de Ativos da Informação: os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção atualizados;

Classificação da Informação: as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância: Restrita, Confidencial e Pública;

Gestão de Acessos: as concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transação;

Gestão de Riscos: os riscos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação.

Gestão de Continuidade de Negócios: O gerenciamento de riscos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações;

Prevenção e tratamento de incidentes: Os procedimentos e controles adotados pelos Sistema CECRESUL, voltados a Prevenção e ao tratamento de incidentes, devem também, ser praticados pelas empresas que prestam serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionsis da instituição.

Conscientização e treinamento sobre segurança da informação : o Sistema CECRESUL deve garantir a disseminação dos princípios e diretrizes de Segurança da informação por meio de programas de conscientização e capacitação, fortalecendo a cultura de segurança cibernética e informação em todos os níveis operacionais em todo o Sistema.

7 Controles Específicos

As Políticas de Segurança da Informação do Sistema CECRESUL são revisadas anualmente e abrangem controles para assegurar a confidencialidade, integridade e disponibilidade de informações, assim como medidas preventivas, detectivas de rastreabilidade, corretivas, voltadas ao controle do

ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de pontos de vulnerabilidades. Entre os principais controles adotados , estão:

- Autenticação;
- Criptografia;
- Prevenção e detecção de invasão;
- Prevenção de vazamento de informações;
- Realização periódica de testes e varreduras para detecção de vulnerabilidades;
- Proteção contra softwares maliciosos;
- Estabelecimento de mecanismos de rastreabilidade da informação;
- Controles de acesso e de segmentação da rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações;;
- Gestão de incidentes; e
- Conscientização de usuários, clientes e fornecedores:

8 Processamento, armazenamento de dados e computação em nuvem

O Sistema CECRESUL, quando da utilização de serviços em nuvem, atenderá aos critérios previstos na Resolução 4.658/2018 do CMN, considerando a avaliação de risco que estes representam para o negócio.

9 Responsabilidade e Comunicação

O cumprimento da Política de Segurança Cibernética e demais procedimentos de segurança da informação do sistema CECRESUL é de responsabilidade de todos os colaboradores, dirigentes e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

A Alta Administração é responsável pela aprovação da presente Política e compromete-se com a melhoria contínua dos procedimentos e controles relacionados à Segurança Cibernética.

10 Sanções e Punições

A área de Segurança da Informação realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política.

Caso haja violação das regras nela dispostas, bem como às demais normas e procedimentos de Segurança da Informação, tal infração pode ser classificada como incidente de segurança da Informação, os quais são passíveis de penalidades, que encontram-se descritas em normativo interno.