POLITICA DE SEGURANÇA CIBERNÉTICA

INFORMAÇÕES GERAIS

Título	Política de Segurança Cibernética
Nome de Referência	PSC_V1
Versão	V1
Status	Em elaboração
Área Responsável pela Política	Tecnologia da Informação
Escopo do Negócio	Cooperativa de Crédito
Resoluções e normas base	Resolução Nº 4.658, de 26 de abril de 2018
Palavras –chave para Procura Rápida	Segurança Cibernética, Segurança da Informação, Incidentes, Invasão, Controles, Rastreabilidade

HISTÓRICO DE VERSÕES

Versão	Motivo da Alteração	Data	Autor	Departamento
1	Versão Inicial	10/12/2020	Fabio Fleck Kamyla Silveira	Segurança da Informação Diretoria

Sumário

1. OBJETIVO 4
2. VIGÊNCIA 4
3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO 4
4. INFORMAÇÕES CONFIDENCIAIS 5
5. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA 5
5.1 Gestão de Acesso às Informações 5
5.2 Proteção do Ambiente da Cooperativa 5
5.2.1 Autenticação 6
5.2.2 Gestão de Incidentes de Segurança da Informação 6
5.2.3 Prevenção a Vazamento de Informações 6
5.2.4 Testes de Intrusão 6
5.2.5 Identificação de Vulnerabilidades 6
5.2.6 Controle Contra Software Malicioso 7
5.2.7 Criptografia 7
5.2.8 Rastreabilidade 7
5.2.9 Segmentação de Rede 7
5.2.10 Desenvolvimento Seguro 7
5.2.11 Cópias de Segurança (Backup) 8
5.3 Continuidade dos Negócios 8
5.4 Processamento, Armazenamento de Dados e Computação em Nuvem 8
5.5 Autenticação e Senha 8

1. OBJETIVO

A Política de Segurança Cibernética da Cooperativa de Economia e Crédito Mútuo dos Servidores da Administração Pública Municipal de Porto Alegre – MUNICRED, visa garantir a proteção dos dados de sua propriedade e/ou sob sua guarda. A proteção dos dados compreende a manutenção de sua integridade, privacidade, garantia de disponibilidade e confidencialidade, assim como, prevenção, detecção e redução da vulberabilidade do ambiente cibernético. A Política também tem como objetivo definir as regras de segurança, que representam, em nível estratégico, os princípios fundamentais incorporados pela Alta Administração da Cooperativa, para o alcance dos objetivos de Segurança da Informação, assim como, demonstra o compromisso da Organização em tratar as informações de seus cooperados com extrema responsabilidade. Demonstra também o compromisso com os aspectos regulatórios, estando assim, em conformidade com as principais regulamentações vigentes que tangem o tema de Segurança Cibernética.

2. VIGÊNCIA

Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas da Cooperativa, alteração de diretrizes de Segurança da Informação, objetivos de negócio ou se requerido pelo regulador local.

3. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

Sendo a informação um dos ativos mais importantes e relevantes no mercado financeiro, a MUNICRED preocupa-se em garantir que todos os dados e informações armazenados em seu ambiente cibernético estejam protegidos e íntegros. Neste sentido, está atenta aos princípios da segurança da informação, cujos objetivos constituem a preservação da propriedade, sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. Está Política dispõem sobre Confidencialidade, Integridade e Disponibilidade, conforme segue:

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas, sejam elas acidentais ou propositais;
Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a acessá-las ou alterá-las.

4. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela MUNICRED é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas.

A MUNICRED poderá revelar as informações confidenciais nas seguintes hipóteses:

- Mediante exigência de autoridade competente, ordem ou mandado judicial;

- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Cooperativa a defender seus direitos e créditos;

- Aos órgãos reguladores do mercado financeiro e para outras instituições financeiras, desde que dentro dos parâmetros estabelecidos pela legislação vigente.

5. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O Gerenciamento de Segurança Cibernética tem como objetivo assegurar que os procedimentos operacionais sejam desenvolvidos, implantados, mantidos e readequados, de acordo com os objetivos estabelecidos nesta Política.

5.1 Gestão de Acesso às Informações

Os acessos às informações são controlados, monitorados e restritos conforme a necessidade de acesso para execução de cada processo de negócio da Cooperativa. As permissões de acesso são revistas periodicamente e cancelados ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

5.2 Proteção do Ambiente da Cooperativa

A proteção do ambiente cibernético da MUNICRED se dá através de controles e da definição de responsabilidades pela gestão e operação dos recursos de processamento das informações. Estas diretrizes visam garantir um monitoramento efetivo, tratando e respondendo aos incidentes, com o intuito de minimizar o risco de falhas e aplicar uma administração segura da redes de comunicações.

Os colaboradores e prestadores de serviço são treinados periodicamente quanto aos conceitos de segurança da informação. Esta ação tem como objetivo a conscientização e disseminação da cultura de segurança cibernética dentro da Cooperativa.

5.2.1 Autenticação

O acesso ao ambiente tecnológico e dados da MUNICRED é permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.
O controle de acesso aos sistemas deve ser formalizado e contemplar os seguintes controles:
- Utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);
- Remoção de autorizações dadas a usuários afastados ou desligados da Cooperativa, ou que tenham mudado de função; e
- Revisão periódica das autorizações concedidas.

5.2.2 Gestão de Incidentes de Segurança da Informação

Possíveis ataques são identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, Antispam, entre outros.

5.2.3 Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

5.2.4 Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

5.2.5 Identificação de Vulnerabilidades

As redes internas e externas devem ser verificadas periodicamente, testadas quanto a sua vulnerabilidade. Sendo identificada alguma vulnerabilidade, as mesmas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

5.2.6 Controle Contra Software Malicioso

Todos os ativos que estejam conectados à rede corporativa ou façam uso de informações da Cooperativa, devem ser protegidos com uma solução anti-malware determinada pela área de Segurança da Informação. Somente colaboradores da área de tecnologia da informação ou prestadores de serviço autorizados por ela, podem instalar ou alterar configurações de softwares nos computadores e servidores da Cooperativa.

5.2.7 Criptografia

Toda solução de criptografia utilizada na MUNICRED deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

5.2.8 Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:
- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;

5.2.9 Segmentação de Rede

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;

- A solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, serão analisados criteriosamente pela área de Tecnologia da Informação e podem não ser executados caso representem ameaça à segurança da rede da Cooperativa.

5.2.10 Desenvolvimento Seguro

A Cooperativa mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

5.2.11 Cópias de Segurança (Backup)

O processo de execução de backups é realizado, periodicamente, nos ativos de informação da Cooperativa, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5.3 Continuidade dos Negócios

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.
Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

5.4 Processamento, Armazenamento de Dados e Computação em Nuvem

A Cooperativa assegura-se de procedimentos efetivos para cumprimento das regras previstas na regulamentação vigente - Resolução 4.658/2018 (e sua alteração 4.752/2019), do Conselho Monetário Nacional.

5.5 Autenticação e Senha

Os cooperados e funcionários são responsáveis pelos atos executados com suas credenciais (login/usuário), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.