POLÍTICA DE RISCO CIBERNÉTICO

1. OBJETIVO

Estabelecer conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da Cooperativa. Definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

2. ABRANGÊNCIA

Aplica-se a todas as áreas de Negócio da Cooperativa.

3. DIRETRIZES GERAIS

A informação é um ativo essencial para os negócios de uma organização e sendo assim deve ser adequadamente protegida. Isto é especialmente importante em um ambiente de negócios cada vez mais interconectado.

Segurança cibernética e da informação é a proteção das informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade. Isso significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas da empresa.

A Cooperativa, através do departamento de Tecnologia da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da Cooperativa, de seus clientes, fornecedores e parceiros de negócios.

3.1. DEFINIÇÕES

Para efeito deste documento, aplicam-se os seguintes termos e definições:

3.1.1. Recursos

Qualquer recurso, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da Cooperativa, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

3.1.2. Ameaça

Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos d o negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

3.1.3. Boas Práticas de Segurança da Informação

São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas.

3.1.4. Colaborador

Entende-se como Colaborador qualquer pessoa que trabalhe para a Cooperativa, quer seja: Funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

3.1.5. Controle

Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

3.1.6. Gestor

Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

3.1.7. IDS

Intrusion Detection System ou Sistema de Detecção de Intrusão é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos.

3.1.8. IPS

Intrusion Prevention System ou Sistema de Prevenção de Intrusão é uma ferramenta que tem a capacidade de identificar uma intrusão, analisar a relevância do evento/risco e bloquear determinados eventos, fortalecendo assim a tradicional técnica de detecção de intrusos.

3.1.9. Informação

Qualquer conjunto organizado de dados que possua algum propósito e valor para a Cooperativa, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

3.1.10. Princípios de "Least Privilege" e "Need to Know"

Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).

3.1.11. Política de Segurança Cibernética e da Informação

Estrutura de documentos formada pela Política, normas e padrões de segurança cibernética e segurança da informação.

3.2. Risco

Qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou, conforme a ISO 31000, o efeito da incerteza nos objetivos.

3.3. Segurança da Informação (SI)

Segurança da Informação é a proteção das informações, sendo caracterizada pela preservação de:

- **Confidencialidade:** garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- **Integridade:** garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.
- **Disponibilidade:** garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;

- **Conformidade:** Garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

3.4. Segurança Cibernética

Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

3.5. Recursos Críticos

Recursos essenciais para o funcionamento da operação da Cooperativa e que possuem informações críticas ou sensíveis.

3.6. Baselines

Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

3.7. Nuvem (Cloud)

Infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

3.8. IoT (Internet of Things – Internet das coisas)

Conexão de dispositivos eletrônicos, como aparelhos eletrodomésticos, eletro portáteis, máquinas industriais, meios de transporte, dentre outros utilizados no dia-a-dia à internet.