POLÍTICA DE SEGURANÇA CIBERNÉTICA

Banricoop

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes, papeis e responsabilidades para a correta utilização dos ativos de informação da organização.

2. DIRETRIZES

a. Tratar e classificar as informações respeitando os princípios de confidencialidade, integridade, disponibilidade de acordo com sua relevância;
b. Atender a Resolução 4.893 do Banco Central do Brasil;
c. Identificação única, pessoal, limitada, intransferível e rastreável para acesso a informações;
d. Controles que garantam a proteção de ativos de informação;
e. Identificação contínua dos riscos relacionados à segurança da informação, de forma integrada com os demais riscos da instituição;
f. Normatizar e aplicar procedimentos e controles da Segurança da Informação;
g. Contratar prestadores de serviços e de computação em nuvem, de acordo com critérios estabelecidos;
h. Manter critérios mínimos de segurança através de cláusulas contratuais na relação com terceiros e exigência de comunicação incidentes relevantes;
i. Promover a cultura de segurança da informação e cibernética em todos os níveis da organização e terceiros contratados;
j. Definir cenários para realização de testes de continuidade de negócios;
k. Definição de relevância dos incidentes conforme impacto nos processos e legislação vigente.

3. PROCEDIMENTOS E CONTROLES

a. Gestão de acessos - concessões e exclusões de acessos com regras de complexidade, qualidade e periodicidade das credenciais;
b. Os ativos de informação são identificados, inventariados e protegidos;
c. As informações classificadas quanto à sua relevância, nos níveis Pública, Interna e Confidencial;
d. Análise, tratamento e comunicação dos alertas, de acordo com os critérios definidos pela estrutura;
e. Manutenção de cópia de segurança, replicação e o tempo de recuperação;
f. As comunicações por voz são gravadas e mantidas em mídias de longa retenção.

5. RASTREABILIDADE DA INFORMAÇÃO

A rastreabilidade é a capacidade de detalhar o histórico através de informações previamente registradas no ERP, e-mails, ligações por voz e acesso físico através de monitoramento.

6. REGISTRO E ANÁLISE DA CAUSA E DO IMPACTO

Os incidentes relevantes são registrados, classificados e tratados conforme os cenários previstos, assim como disponibilizados sistematicamente ao Comitê de Riscos e do Conselho de Administração.

7. PAPÉIS E RESPONSABILIDADES

Em relação a Segurança da Informação e Cibernética, é responsabilidade de todos os conselheiros, dirigentes, colaboradores, terceiros prestadores de serviços e estagiários da Banricoop, conhecer e disseminar esta política, aderir à postura alinhada às boas práticas de segurança da informação e cibernética adotadas pela Banricoop e disseminadas em comunicados e treinamentos.

8. ABRANGÊNCIA

Esta política abrange todos os níveis da Cooperativa, associados e prestadores de serviços.

9. VIGÊNCIA

Esta política passa a vigorar a partir de sua aprovação pelo Conselho de Administração e é parte integrante do ambiente normativo interno da Banricoop.