SICOOB
CredMetal

POLITICA DE SEGURANÇA CIBERNÉTICA

INTRODUÇÃO

Aprovada pelo Conselho de Administração do Sicoob Confederação, esta Política Institucional de Segurança Cibernética foi elaborada para tratar e prevenir incidentes de segurança cibernética, reforçando o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança Cibernética do Sicoob.

PÚBLICO

Todos os usuários que compõem a estrutura organizacional do SICOOB CREDMETAL (conselheiros, diretores, funcionários e estagiários) e demais pessoas com acesso autorizado às informações do Sicoob, incluindo cooperados, parceiros, empresas prestadoras de serviço e ao público.

OBJETIVOS

A Política Institucional de Segurança Cibernética do Sicoob visa:

- Definir diretrizes para segurança do espaço cibernético relacionadas á capacidade das entidades do Sicoob de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- Proteger as informações sob responsabilidade das entidades preservando sua confidencialidade, integridade, disponibilidade e autenticidade;
- Prevenir eventuais interrupções, totais ou parciais, dos serviços de TI acessados pelas entidades e pelos cooperados e, no caso ocorrência, reduzir os impactos dela resultados;
- Prevenir incidentes de segurança cibernética;
- Formar, se possível, e qualificar os recursos humanos necessário à área de segurança cibernética;
- Promover o intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética.

SICOOB CredMetal

RESPONSABILIDADES

- O Sicoob Confederação, por meio da Superintendência de Governança de TI, Segurança e Inovação com reporte ao Diretor de Tecnologia da Informação, é responsável pela gestão centralizada de segurança cibernética do Sicoob. No Sicoob CredMetal o diretor responsável pela gestão é o Sr. Mauro Lobiano Parra.
- O Banco Sicoob, por meio da Superintendência de gestão de riscos, com reporte ao Diretor de Controle, é o responsável pela gestão centralizada de segurança cibernética do Bancoob, suas empresas controladas e fundação patrocinada.

DO DIRETOR RESPONSÁVEL PELA SEGURANÇA CIBERNÉTICA

- Supervisionar o desenvolvimento, a implantação e o desempenho da estrutura do gerenciamento de gerenciamento de segurança cibernética, incluindo seu aperfeiçoamento;
- Subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética, auxiliando o conselho Administrativo;
- Responsabilizar-se pela capacitação adequada dos empregados que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles;
- Promover a disseminação da cultura de gerenciamento de segurança cibernética.

PROCEDIMENTOS E CONTROLES

- Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, as entidades do Sicoob adotam procedimentos e controles, conforme porte e perfil de risco da entidade. Estes procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros;
- É plano de ação e de resposta a incidentes, revisando anualmente;
- As informações de propriedade ou sub custódia das entidades do Sicoob, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termo sigilo, valor, requisitos legais, sensibilidade e necessidade do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos

sistemas de informação utilizados, conforme Manuel de classificação da informação específico;

- São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição;
- Complementam está política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética no âmbito das entidades do Sicoob;
- Regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade do Sicoob;
- Duplo fator de autenticação nos ambientes em que o recurso está disponível;
- Recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados sob responsabilidade Sicoob;
- Solução de prevenção e detecção de instrução, solução de proteção de dispositivos, procedimentos de hardening, monitoramento de tráfego na rede, monitoramento de atividades em bancos de dados, monitoramento de atividade de usuário privilegiados;
- Testes de invasão realizados por equipe interna da entidade ou por empresa contratada quando a entidade possuir serviços de TI sob sua responsabilidade;
- Processo de gestão de vulnerabilidades de ativos de TI;
- Solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;
- Gerenciador de eventos e incidentes em segurança que mantém registro dos eventos do ambiente, permitindo a rastreabilidade de vários tipos de ocorrências;
- Solução de prevenção de vazamento de dados;
- Segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas;
- Manutenção de cópias de segurança dos dados e das informações;
- Execução de testes de continuidade de negócios, incluindo cenários de incidentes cibernéticos, tais como ataques de negação de serviço, ransomware, desfiguração (defacement), vazamento de dados e acesso não autorizado;
- Critérios de decisão quanto á terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- As informações de propriedade ou sub custódia das entidades do Sicoob, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos legais, sensibilidade, a integridade e a disponibilidade dos dados

e dos sistemas de informação utilizados, conforme manual de classificação da informação específico;

- O conteúdo dos aplicativos e programas de mensagens instantâneas e o conteúdo dos e-mails recebidos ou enviados a partir das caixas corporativas, de uso individual ou compartilhado, bem como o conteúdo dos arquivos de dados criados pelos aplicativos usados para ler e-mails, independentemente do local de armazenamento, poderão ser acessados pela estrutura centralizada de gestão de segurança cibernética do CCS, mediante solicitação formal da Diretoria Executiva.

ACOMPANHAMENTO TÉCNICO

- O TI responsável pela segurança cibernética está a cargo da Magiccomp Engenharia e Serviços de Informática Ltda.

DA ESTRUTURA

- Definir políticas, planos e controles para o gerenciamento da SC;
- Definir e acompanhar indicadores de gestão de SC;
- Providenciar o relacionamento com as áreas internas de supervisão, responsáveis com os órgãos externos;
- Prestar apoio às entidades do Sicoob, relativo a gestão de SC.

Diretoria Executiva – aprovado em 16 de dezembro de 2022

MILTON BAPTISTA DE S. FILHO
DIRETOR PRESIDENTE

MAURO LOBIANO PARRA
DIRETOR OPERACIONAL

MANOEL OSORIO ANDRADE
DIRETOR ADMINISTRATIVO