POLÍTICA INSTITUCIONAL DE SEGURANÇA CIBERNÉTICA DO SICOOB

INTRODUÇÃO

Aprovada pelo Conselho de Administração do Sicoob Confederação e do Banco Sicoob, 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 as estruturas organizacionais das entidades do Sicoob (dirigentes, empregados 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 a segurança do espaço cibernético relacionadas à 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 de sua ocorrência, reduzir os impactos dela resultantes;
- Tratar e prevenir incidentes de segurança cibernética;
- Formar e qualificar os recursos humanos necessários à área de segurança cibernética;
- Promover o intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética.

RESPONSABILIDADES

- O Sicoob Confederação, por meio da Superintendência de Segurança Cibernética, com reporte ao Diretor de Tecnologia da Informação, é responsável pela gestão centralizada de segurança cibernética do Sicoob;
- As cooperativas centrais e singulares, por meio da diretoria designada, são responsáveis pelo gerenciamento da segurança cibernética nas entidades que administram.

RESPONSABILIDADES

- 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 estabelecido plano de ação e de resposta a incidentes, revisado anualmente.
- As empresas terceirizadas que manuseiam dados ou informações sensíveis ou que são relevantes para a condução das atividades operacionais estabelecem procedimentos e controles compatíveis aos utilizados pelas entidades do Sicoob.
- As informações de propriedade ou sob custódia das entidades do Sicoob, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, conforme manual de classificação da informação específico.
- São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição.
- Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética no âmbito das entidades do Sicoob.