POLÍTICA INSTITUCIONAL DE SEGURANÇA CIBERNÉTICA DO SICOOB

Política Institucional de Segurança Cibernética do Sicoob

INTRODUÇÃO

Aprovada pelo Conselho de Administração do CCS – Sicoob Confederação, esta Política Institucional de Segurança Cibernética reforça 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 (dirigentes, empregados e estagiários) das entidades do Sicoob e demais pessoas com acesso autorizado às informações do Sicoob, incluindo cooperados, parceiros, empresas prestadoras de serviço e ao público.

OBJETIVOS

São objetivos da Política Institucional de Segurança Cibernética do Sicoob:

- a definição de 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;
- a proteção das informações sob responsabilidade das entidades do Sicoob, preservando sua confidencialidade, integridade, disponibilidade e autenticidade;
- a prevenção de eventual interrupção, total ou parcial, dos serviços de TI acessados pelas entidades do Sicoob e pelos cooperados, e, no caso de sua ocorrência, a redução dos impactos dela resultantes;
- o tratamento e a prevenção de incidentes de segurança cibernética;
- a formação e a qualificação dos recursos humanos necessários à Superintendência de Segurança Cibernética do CCS;
- a promoção do intercâmbio de conhecimentos entre as demais instituições financeiras, os órgãos e as entidades públicas a respeito da segurança cibernética.

RESPONSABILIDADES

- a área responsável pela Gestão Sistêmica de Segurança Cibernética do Sicoob, instituída no Projeto de Gestão Sistêmica de Riscos e Segurança Cibernéticos é a Superintendência de Segurança Cibernética do CCS, com reporte ao Diretor de Tecnologia da Informação;
- a gestão sistêmica não desonera as responsabilidades das entidades do Sicoob, as quais, observando sua natureza e o órgão de fiscalização, devem indicar um diretor responsável pelo gerenciamento da segurança cibernética nas entidades que administram. O diretor indicado pode exercer outras funções, desde que não haja conflito de interesse;

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 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 pelo 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 nas entidades do Sicoob, como a implementação de programas de capacitação e avaliação periódica de pessoal;

- 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;