1. Compromisso Institucional

A Política Institucional de Segurança Cibernética do Sicoob, aprovada pelo Conselho de Administração do CCS – Sicoob Confederação, reflete o compromisso da alta administração com a melhoria contínua dos procedimentos de defesa digital. Suas diretrizes aplicam-se a todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) das entidades do Sicoob, bem como a parceiros e empresas prestadoras de serviço com acesso autorizado às informações institucionais.

2. Objetivos da Política

A estrutura de segurança do espaço cibernético do Sicoob é orientada pelos seguintes objetivos centrais:

- **Redução de Vulnerabilidades:** Definir diretrizes para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.
- **Proteção da Informação:** Assegurar a proteção das informações sob responsabilidade das entidades do Sicoob, preservando sua confidencialidade, integridade, disponibilidade e autenticidade.
- **Resiliência Operacional:** Prevenir a interrupção, total ou parcial, dos serviços de Tecnologia da Informação (TI) acessados pelas entidades e pelos cooperados, atuando para reduzir os impactos caso ocorram.
- **Tratamento de Incidentes:** Estabelecer ações para o adequado tratamento e a prevenção de incidentes de segurança cibernética.
- **Capacitação e Intercâmbio:** Assegurar a adequada formação dos recursos humanos da área de segurança e promover o intercâmbio de conhecimentos

sobre o tema com as demais instituições financeiras, órgãos e entidades públicas.

3. Governança e Responsabilidades

A gestão de segurança cibernética no âmbito do Sicoob é estruturada de forma compartilhada:

- **Gestão Sistêmica:** A liderança estratégica da segurança cibernética é de responsabilidade da Superintendência de Segurança Cibernética do CCS, com reporte ao Diretor de Tecnologia da Informação do CCS. Cabe a essa estrutura definir as políticas, planos, manuais, controles e indicadores sistêmicos.
- **Responsabilidade das Entidades:** A gestão centralizada não desonera as responsabilidades das cooperativas centrais e singulares. Cada entidade do Sicoob deve indicar um diretor responsável pelo gerenciamento local da segurança cibernética, atuando como primeira linha de defesa contra ameaças e fraudes em seu respectivo âmbito.

4. Procedimentos e Controles de Proteção

Para mitigar riscos cibernéticos e proteger os dados sob sua custódia, as entidades do Sicoob adotam procedimentos e controles tecnológicos compatíveis com seu porte e perfil de risco, aplicados a sistemas internos ou adquiridos de terceiros:

- **Gestão de Acessos:** Implementação de controles de identidades e privilégios baseados no princípio do menor privilégio, além da utilização de Autenticação Multifator (MFA) para o acesso a recursos e dados.
- **Monitoramento e Segurança de Ativos:** Integração de redes e dispositivos a soluções homologadas e monitoradas continuamente pelo Centro de Operações de Segurança (SOC) do Sicoob.

- **Varreduras e Testes Periódicos:** Realização periódica de testes de intrusão (pentests) internos e externos, varreduras de vulnerabilidades no perímetro e testes de continuidade de negócios.
- **Trilhas de Auditoria:** Manutenção de registros automatizados (logs) de autenticação, alterações de privilégios e acessos a informações relevantes para garantir a rastreabilidade das operações.
- **Proteção contra Vazamento de Dados:** Utilização de ferramentas para prevenção de perda e vazamento de dados confidenciais (DLP) e bloqueio de soluções não corporativas que possam representar riscos de exfiltração.
- **Classificação da Informação:** Classificação dos dados e informações (meio eletrônico ou físico) conforme critérios de sigilo, valor, sensibilidade e requisitos legais.
- **Exigências para Terceiros:** Empresas terceirizadas que manuseiam dados sensíveis ou relevantes devem estabelecer controles de segurança com abrangência e precisão compatíveis com os padrões do Sicoob.

5. Disseminação da Cultura e Orientações ao Usuário

- **Capacitação Interna:** Adoção de mecanismos para a disseminação da cultura de segurança digital, incluindo programas de capacitação e avaliação periódica de pessoal nas entidades.
- **Informações a Clientes e Cooperados:** Prestação de orientações formais, por meio dos canais institucionais oficiais, sobre precauções na utilização de produtos e serviços financeiros, incluindo segurança cibernética, prevenção a fraudes, proteção de credenciais e privacidade de dados.