1. Esta Política Institucional de Segurança Cibernética do Sicoob:

   a) é aprovada pelo Conselho de Administração do Sicoob Confederação e do Banco Sicoob;

   b) o Sicoob Confederação, por meio da Superintendência de Governança de TI, Segurança Cibernética com reporte ao Diretor de Tecnologia da Informação, é responsável pela gestão centralizada de segurança cibernética do Sicoob;

   c) a gestão centralizada não desonera as responsabilidades das entidades do Sicoob as quais devem, também, indicar diretor responsável pelo gerenciamento da segurança cibernética nas entidades que administram. O diretor indicado poderá exercer outras funções, desde que não haja conflito de interesse;

   d) é divulgada a todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) das entidades do Sicoob e às demais pessoas com acesso autorizado às informações do Sicoob, incluindo cooperados, parceiros, empresas prestadoras de serviço e ao público;

   e) reforça o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

2. Para fins desta Política são observados os seguintes conceitos:

   a) *entidades*: as entidades do Centro Cooperativo Sicoob (CCS), as cooperativas centrais e singulares do Sicoob e as entidades não cooperativas integrantes do Sistema;

      a.1) *entidades do CCS*: Sicoob Confederação, Banco Sicoob, Sicoob DTVM, Sicoob Pagamento, Sicoob Previ, Sicoob Administradora de Consórcios, Sicoob Seguradora, Instituto Sicoob e o Fundo de Proteção do Sicoob.

      a.2) entidades não cooperativas integrantes do Sicoob:

   b) outras entidades não cooperativas que venham a integrar o Sicoob.

3. São objetivos desta Política:

   a) 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;

   b) a proteção das informações sob responsabilidade das entidades preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

   c) a prevenção de eventual interrupção, total ou parcial, dos serviços de TI acessados pelas entidades e pelos cooperados e, no caso de sua ocorrência, a redução dos impactos dela resultantes;

   d) o tratamento e a prevenção de incidentes de segurança cibernética;

e) a formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;

f) a promoção do intercâmbio de conhecimentos entre as demais instituições financeiras, órgãos e entidades públicas a respeito da segurança cibernética.

4. Das responsabilidades.

4.1. Do Conselho de Administração das entidades do Sicoob:

a) revisar e aprovar anualmente as políticas e estratégias de gerenciamento de segurança cibernética;

b) assegurar a aderência das entidades às políticas e estratégias de gestão da segurança cibernética;

c) assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de segurança cibernética;

d) promover a disseminação da cultura de gerenciamento de segurança cibernética.

4.2. Do diretor responsável pela segurança cibernética nas entidades do Sicoob:

a) supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, incluindo seu aperfeiçoamento;

b) subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética, auxiliando o Conselho de Administração;

c) responsabilizar-se pela capacitação adequada dos empregados que compõem a estrutura de gerenciamento de segurança cibernética, acerca das políticas, dos planos e dos controles.

4.3. Da estrutura centralizada de gestão de segurança cibernética do CCS:

a) definir políticas, planos, manuais e controles para o gerenciamento de segurança cibernética das entidades do Sicoob;

b) definir e acompanhar indicadores de gestão da segurança cibernética no Sicoob;

c) providenciar o relacionamento com as áreas internas de supervisão, responsáveis pelo relacionamento com os órgãos de supervisão externos;

d) prestar apoio às entidades do Sicoob, relativo à gestão de segurança cibernética;

e) informar à Superintendência de Gestão Integrada de Riscos e Área de Controles Internos do CCS sobre os incidentes cibernéticos relevantes;

f) reportar ao Conselho de Administração do Sicoob Confederação e do Banco Sicoob e à Diretoria Executiva do CCS as informações relativas à gestão centralizada de segurança cibernética;

g) compartilhar informações sobre incidentes cibernéticos relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

4.4. Das cooperativas singulares, centrais e do CCS:

a) definir o diretor responsável pela gestão de segurança cibernética;

b) fazer recomendações de aperfeiçoamento da política, dos planos, manuais, controles e procedimentos relacionados à segurança cibernética;

c) implementar e executar os procedimentos descritos nas políticas, planos e manuais relativos ao tema;

d) reportar à estrutura centralizada de governança as informações referentes à segurança cibernética.

4.5. Todas as áreas das entidades do Sicoob:

a) notificar sobre incidentes de segurança cibernética à área responsável pela gestão centralizada de segurança cibernética no CCS.

5. Dos procedimentos e controles.

5.1 Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos, prevenir o vazamento de informações e atender aos demais objetivos de segurança cibernética, as entidades devem adotam procedimentos e controles, conforme porte e perfil de risco da entidade, tais como:

a) privilégio mínimo;

b) regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade do Sicoob;

c) duplo fator de autenticação nos ambientes em que o recurso está disponível;

d) recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos pelo Sicoob;

e) solução de prevenção e detecção de intrusão, solução de proteção de dispositivos, procedimentos de hardening, monitoramento de tráfego na rede, monitoramento de atividades em bancos de dados, monitoramento de atividade de usuários privilegiados;

f) testes de invasão realizados por equipe interna da entidade ou por empresa contratada quando a entidade possuir serviços de TI sob sua responsabilidade;

g) processo de gestão de vulnerabilidades de ativos de TI;

h) solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;

i) gerenciador de eventos e incidentes em segurança que mantém registro dos eventos do ambiente, permitindo a rastreabilidade de vários tipos de ocorrências;

j) solução de prevenção de vazamento de dados;

k) segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas;

l) manutenção de cópias de segurança dos dados e das informações;

m) 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;

n) critérios de decisão quanto à terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem.

5.2 Os procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

5.3 As empresas terceirizadas que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da entidade deverão estabelecer procedimentos e controles com complexidade, abrangência e precisão compatíveis com os utilizados pelo Sicoob.

5.4 É estabelecido plano de ação e de resposta a incidentes, revisado anualmente.

6. 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.

7. 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

ou do Conselho de Administração do Sicoob Confederação e Banco Sicoob, para esclarecimentos de fatos que, em tese, configurem irregularidade funcional ou ética.

8. São adotados mecanismos para disseminação da cultura de segurança cibernética na entidade, incluindo:

   a) implementação de programas de capacitação e de avaliação periódica de pessoal;

   b) prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

9. 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.