1. Esta Política:

a) é aprovada pelo Conselho de Administração do Centro Cooperativo Sicoob (CCS), com aplicação imediata pelas cooperativas centrais e singulares do Sicoob, devendo o conteúdo ser levado ao conhecimento dos seus respectivos órgãos de administração;

b) tem o CCS, por meio da Superintendência de Segurança Cibernética com reporte ao Diretor de Tecnologia da Informação, como responsável pela gestão sistêmica de segurança cibernética do Sicoob.

~~**c)**~~ a gestão sistêmica não desonera as responsabilidades das entidades do Sicoob, as quais devem, também, indicar um 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 o 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 do Sicoob*: as cooperativas centrais e singulares, as entidades do CCS – composto pelo Sicoob Confederação, Banco Sicoob, Sicoob DTVM, Sicoob Pagamentos, Sicoob Previ, Sicoob Consórcios, Sicoob Seguradora, Instituto Sicoob e Fundo de Proteção do Sicoob – as 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 do Sicoob 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 Superintendência de Segurança Cibernética do CCS;

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

4. São 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 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 os 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 à Área de Controles Internos do CCS sobre os incidentes cibernéticos relevantes;

f) reportar ao Conselho de Administração e à Diretoria Executiva do CCS as informações relativas à gestão sistêmica 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 (BCB).

4.4. Das cooperativas singulares e centrais:

a) designar o diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes;

b) fazer recomendações de aperfeiçoamento desta Política, das ações, dos planos, dos manuais, dos controles e dos procedimentos relacionados a segurança cibernética;

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

d) reportar, à estrutura centralizada de governança, as informações referentes a segurança cibernética;

e) estar em conformidade com as recomendações de segurança para utilização do Sisbr;

f) integrar a rede local e todos os dispositivos que acessam o Sisbr às soluções de segurança homologadas e monitoradas pelo Centro de Operações de Segurança – SOC do CCS;

g) ser a primeira linha de defesa cibernética contra ameaças e fraudes, no âmbito da cooperativa;

h) realizar a abertura de chamados para tratativa de requisições e incidentes;

i) corrigir as vulnerabilidades apontadas pelo teste anual de simulação de intrusão (*pentest*);

j) evitar a contratação de soluções de terceiros e/ou o desenvolvimento de soluções locais pelas cooperativas, devido à necessidade de gestão permanente do risco cibernético;

k) estar em conformidade com os procedimentos e controles descritos no item 5.1 desta Política.

4.5. Todas as áreas das entidades do Sicoob:

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

5. Dos procedimentos e controles.

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

a) adotar o princípio do privilégio mínimo, limitando os direitos de acesso dos usuários ao que é estritamente necessário para realizar suas atividades;

b) recursos adequados para garantir a privacidade, a integridade e o não repúdio dos dados mantidos e transitados pelo Sicoob;

c) regras para controlar a complexidade, a qualidade e a integridade das credenciais utilizadas para o acesso aos sistemas e aos dados sob responsabilidade do Sicoob;

d) utilizar Autenticação Multifator (MFA) como método de segurança de gerenciamento de identidade e acesso a recursos e dados;

e) controlar as contas privilegiadas que acessam sistemas, banco de dados, aplicativos e a infraestrutura de rede, utilizando soluções de gerenciamento de acesso privilegiado (PAM), protegendo contas com acesso a sistemas, e dados confidenciais e sensíveis;

f) realizar testes de intrusão interno e externo nas camadas de rede e aplicação por equipe interna da entidade e/ou por empresa contratada, com periodicidade mínima anual, em que todas as fragilidades identificadas são priorizadas e tratadas de acordo com o seu nível de criticidade;

g) executar, periodicamente, varreduras em busca de vulnerabilidades no perímetro da rede da entidade do Sicoob, incluindo aplicações. As vulnerabilidades identificadas devem ser priorizadas e tratadas de acordo com seu nível de criticidade;

h) adotar solução de proteção contra ameaças avançadas em e-mail e no acesso a sites com gestão sistêmica pela Área de Segurança Cibernética do CCS;

i) implementar trilhas de auditoria automatizada, para todos os componentes do sistema considerados relevantes, para o armazenamento dos registros das ações, dos eventos ou das atividades realizadas pelos usuários, contendo minimamente:

i.1) *logs* de autenticação de usuários (tentativas de acesso válidas e malsucedidas);

i.2) alterações de privilégios de acesso;

i.3) ações executadas por acessos privilegiados;

i.4) acesso a informações relevantes;

i.5) ações executadas pelos usuários, incluindo criação, alteração ou remoção de objetos do sistema;

j) implementar controles para prevenção de perda e vazamento de dados confidenciais (DLP), nas soluções oficiais de colaboração, como o Office 365;

k) bloquear acesso a sites com soluções não corporativas que permitam a troca de informações e arquivos, como aplicativos de mensagens, *e-mail* não corporativo, armazenamento em nuvem, dentre outros. Para necessidades especiais de liberação de acesso a esses tipos de soluções, em condição de exceção, deve ser utilizada a solução de DLP homologada pelo CCS como solução compensatória;

l) implementar DLP nas estações de trabalho operadas por usuários que manipulam dados de cartão de crédito, observando sempre o atendimento a leis e regulações vigentes que obriguem sua utilização;

m) adotar solução de prevenção e detecção de intrusão (IDS/IPS), solução de proteção de dispositivos (computadores, *notebooks*, servidores e outros), procedimentos de *hardening*, monitoramento de tráfego na rede, atividades em bancos de dados e de atividade de usuários privilegiados;

n) controlar e bloquear o acesso indevido de equipamentos e dispositivos externos via USB, a exemplo de pendrives, modems, HDs externos ou outros que podem expor o ambiente a infecção, invasão ou exfiltração de dados;

o) utilizar soluções de criptografia em conexões, autenticações, senhas, base de dados e em qualquer outra informação relevante do Sicoob;

p) manter todas as soluções de proteção atualizadas;

q) manter os ativos de TI (computadores, *notebooks*, servidores e outros) atualizados com as últimas versões de *patches* de segurança;

r) efetuar e manter cópia de segurança dos dados e das informações com execução periódica de teste de recuperação dos dados copiados;

s) segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas, incluindo as redes de acesso ao Sisbr, às redes ATM, à rede *wi-fi* de visitantes e a outras;

t) execução periódica 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;

u) adotar critérios de decisão quanto à terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, conforme a Resolução CMN nº 4.893, de 26/2/2021.

5.2 Os procedimentos e controles citados acima também devem ser aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

5.3 As empresas terceirizadas que manusearem 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 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 sistêmica de gestão de segurança cibernética do CCS, mediante solicitação formal da Diretoria Executiva ou do Conselho de Administração do CCS, para esclarecimentos de fatos que, em tese, configurem irregularidade funcional ou ética.

8. São adotados mecanismos para a disseminação da cultura de segurança cibernética na entidade, como a implementação de programas de capacitação e de avaliação periódica de pessoal.

9. Complementam esta Política e a ela se subordinam todas as normas internas que regulam a segurança cibernética no âmbito das entidades do Sicoob.

Controle de Atualizações

Data	Instrumento de Comunicação	Situação
29/5/2024	*Link* CCS – RES CCS 269 *Link* Cooperativas – RES CCS 269	Atualizada
27/10/2023	*Link* CCS – RES CCS 213 *Link* Cooperativas – RES CCS 213	Instituída
24/10/2022	*Link* CCS – RES CCS 127 *Link* Cooperativas – RES CCS 127	Ratificada
14/10/2021	*Link* CCS – RES CCS 069 *Link* Cooperativas – RES CCS 069	Atualizada
9/6/2020	*Link* CCS – RES Sicoob Confederação 356 *Link* Cooperativas – Sicoob Confederação 356	Atualizada
10/4/2019	*Link* CCS – RES Sicoob Confederação 283 *Link* Cooperativas – Sicoob Confederação 283	Instituída