1. Esta Política:

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

b) foi elaborada e é revisada, no mínimo, anualmente, por proposta da Superintendência de Segurança Cibernética, por meio da Área de Defesa Cibernética e da Área de Detecção e Resposta a Incidentes Cibernéticos do Centro Cooperativo Sicoob (CCS);

c) é submetida à Diretoria Executiva e aprovada pelo Conselho de Administração do CCS – Sicoob Confederação;

d) tem aplicação imediata pelas entidades do Sicoob, devendo o conteúdo ser levado para aprovação dos seus respectivos órgãos de administração, com registro em ata;

e) é divulgada internamente, por meio dos canais de comunicação do Sicoob, a todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) das entidades do Sicoob;

f) é divulgada às demais pessoas com acesso autorizado às informações do Sicoob, incluindo cooperados, parceiros, empresas prestadoras de serviço e o público, na forma resumida, contendo as linhas gerais desta Política no *site* oficial do Sicoob;

g) não desonera as cooperativas centrais e singulares de desenvolverem seus Planos de Resposta a Incidentes Cibernéticos internos para cada tipo de incidente.

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

a) entidades do Sicoob: cooperativas singulares, cooperativas centrais e entidades do Centro Cooperativo Sicoob (CCS);

b) entidades do CCS: Sicoob Confederação; Banco Sicoob; Sicoob DTVM; Sicoob Pagamentos; Sicoob Previ; Sicoob Consórcios; Sicoob Seguradora; Instituto Sicoob; e Fundo de Proteção do Sicoob.

3. 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.

4. 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 do Sicoob, 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) o estabelecimento de diretrizes para assegurar a adequada formação e qualificação dos recursos humanos necessários ao desempenho das atividades da Superintendência de Segurança Cibernética do CCS, garantindo que possuam conhecimentos técnicos compatíveis com as responsabilidades atribuídas;

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

5. São responsabilidades 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.

6. São responsabilidades do diretor responsável pela segurança cibernética das 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) certificar-se de que a entidade está atuando em conformidade com as diretrizes corporativas do Sicoob, em especial quanto aos itens relacionados à gestão da estrutura local (redes, *wi-fi*, servidores, estações de trabalho que não sejam de uso do Sisbr, dispositivos IoT, ATMs, *links* MPLS e de internet etc.), bem como inibir práticas que podem representar riscos significativos à segurança sistêmica;

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

7. São responsabilidades das cooperativas singulares e centrais e das entidades do CCS:

a) designar o diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes que, no caso das entidades do CCS, é o Diretor de Tecnologia da Informação do CCS;

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

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

d) atuar em conformidade com as diretrizes corporativas do Sicoob, em especial quanto aos itens relacionados à gestão da estrutura local da entidade (redes, *wi-fi*, servidores, estações de trabalho que não sejam de uso do Sisbr, dispositivos IoT, ATMs, *links* MPLS e de internet etc.);

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

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

g) 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 – em inglês, *Security Operations Center (SOC)* – do Sicoob;

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

i) abrir chamados, por meio do Portal de Atendimento, para tratativa de requisições e incidentes;

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

k) 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;

l) criar e revisar planos de resposta a incidentes relacionados à infraestrutura local não relacionados a incidentes de segurança cibernética;

m) estar em conformidade com os procedimentos e controles descritos nesta Política.

8. Todas as áreas das entidades do Sicoob devem notificar sobre quaisquer incidentes de segurança cibernética ao SOC do Sicoob.

9. São responsabilidades 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 contato com as áreas internas de supervisão, responsáveis pelo relacionamento com os órgãos de supervisão externos nos assuntos de segurança cibernética;

d) apoiar as entidades do Sicoob sobre a gestão de segurança cibernética;

e) informar, de forma tempestiva, à Superintendência de Gestão Integrada de Riscos e à Área de Controles Internos e Conformidade do CCS, acerca de incidentes ou fragilidades cibernéticas relevantes;

f) reportar, ao Conselho de Administração e à Diretoria Executiva do CCS – Sicoob Confederação, 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).

10. A Gestão Sistêmica de Segurança Cibernética do Sicoob, é de responsabilidade da Superintendência de Segurança Cibernética do CCS, com reporte ao Diretor de Tecnologia da Informação do CCS.

11. 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 controles de gestão de identidades, acessos e privilégios, observando o princípio do menor privilégio, limitando os direitos de acesso dos usuários ao que é estritamente necessário para o desempenho de suas atividades;

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

c) manter 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, protegendo contas com acesso a sistemas, e dados confidenciais e sensíveis;

f) realizar testes de intrusão interno e externo nas camadas de rede e de aplicação por equipe interna da entidade e/ou por empresa contratada, com periodicidade mínima anual, para assegurar que as fragilidades identificadas sejam priorizadas e tratadas conforme o seu nível de criticidade e risco, por meio de planos de ação específicos, com registro nas plataformas institucionais, acompanhamento e manutenção de evidências à disposição dos órgãos de supervisão;

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) garantir que as soluções de segurança sistêmicas estejam instaladas, ativas e monitoradas continuamente pelo SOC do Sicoob em todos os dispositivos da cooperativa (estações de trabalho Sisbr, estações de trabalho não Sisbr, *totens*, ATMs, servidores, entre outros);

i) adotar solução de proteção contra ameaças avançadas em *e-mail* e no acesso a *sites* com gestão sistêmica pelo CCS;

j) manter as trilhas de auditoria automatizadas, 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:

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

j.2) alterações de privilégios de acesso;

j.3) ações executadas por acessos privilegiados;

j.4) acesso a informações relevantes;

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

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

l) 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, entre 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;

m) 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;

n) 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;

o) definir, implementar e manter perfis de configuração segura dos ativos de tecnologia, de forma compatível com a criticidade dos ativos e o perfil de risco da entidade, observadas as diretrizes desta Política e os normativos internos complementares;

p) 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;

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

r) manter todas as soluções de proteção atualizadas;

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

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

u) manter 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;

v) vedar a utilização de ferramentas não sistêmicas de suporte remoto como TeamViewer, AnyDesk, VNC, entre outras;

w) restringir a utilização de rede privada virtual – em inglês, *virtual private network* (*VPN*) – corporativa por empresas terceiras para acesso ao ambiente da cooperativa, principalmente ao Sisbr;

x) executar periodicamente testes de continuidade de negócios, incluindo cenários de indisponibilidade ocasionada por incidentes cibernéticos, como ataques de negação de serviço, *ransomware*, desfiguração (*defacement*), vazamento de dados e acesso não autorizado;

y) adotar critérios de decisão, avaliação de riscos, requisitos contratuais e mecanismos de supervisão quanto à terceirização de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, conforme a Resolução CMN nº 5.274, de 18/12/2025;

z) gerir os certificados digitais, abrangendo sua emissão, seu uso, seu armazenamento, sua renovação e sua revogação, bem como a proteção das chaves privadas associadas;

aa) adotar mecanismos de integração segura entre sistemas internos e externos, assegurando a implementação de controles de autenticação, autorização e criptografia de forma a proteger as informações trafegadas e os acessos realizados;

bb) adotar ações de inteligência cibernética, por meio do monitoramento contínuo de ameaças, vulnerabilidades e riscos emergentes, bem como de

informações de interesse institucional no ambiente cibernético, incluindo a internet, a *deep web* e a *dark web* e, quando aplicável, grupos privados de comunicação, observados os limites legais e regulatórios;

cc) realizar a rastreabilidade e o registro de transações e operações, garantindo a manutenção de trilhas de auditoria completas, íntegras, invioláveis e passíveis de verificação por auditoria;

dd) aplicar correções e atualizações de segurança (*patches*) de maneira tempestiva, observando processo formal de gestão de vulnerabilidades, com priorização conforme o nível de risco e criticidade dos ativos;

ee) adotar requisitos de segurança da informação e cibernética no desenvolvimento, na aquisição e na contratação de soluções tecnológicas próprias ou de terceiros, abrangendo, no mínimo, práticas de desenvolvimento seguro, controles de acesso, proteção de dados, gestão de vulnerabilidades, testes de segurança e critérios de conformidade regulatória.

12. Os procedimentos e controles citados no item 11 desta Política também devem ser aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

13. 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.

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

15. 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 o manual de classificação da informação específico.

16. 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, podem 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 – Sicoob Confederação, para esclarecimentos de fatos que, em tese, configurem irregularidade funcional ou ética.

17. São adotados mecanismos para a disseminação da cultura de segurança cibernética nas entidades do Sicoob, como a implementação de programas de capacitação e de avaliação periódica de pessoal.

18. São adotados, também, mecanismos formais para a prestação de informações a clientes, cooperados e usuários sobre precauções na utilização de produtos e serviços financeiros, incluindo orientações sobre segurança cibernética, fraudes, proteção de credenciais e boas práticas de privacidade e proteção de dados, por meio de canais institucionais oficiais.

19. Na contratação de serviços de tecnologia da informação, computação em nuvem, processamento e armazenamento de dados, devem ser observados os critérios de decisão, a avaliação de riscos, os requisitos contratuais, a análise de relevância e os mecanismos de supervisão estabelecidos pela Resolução CMN nº 5.274, bem como pelas normas corporativas do Sicoob.

20. 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

Instrumento de Comunicação	*Link* CCS	*Link* Cooperativas
Atualizada – RES CCS 385, de 26/2/2026	Acesse	Acesse
Atualizada – RES CCS 348, de 2/6/2025	Acesse	Acesse
Atualizada – RES CCS 269, de 29/5/2024	Acesse	Acesse
Atualizada – RES CCS 213, de 27/10/2023	Acesse	Acesse
Atualizada – RES CCS 127, de 24/10/2022	Acesse	Acesse
Atualizada – RES CCS 069 de 14/10/2021	Acesse	Acesse
Atualizada – RES Sicoob Confederação 356, de 9/6/2020	Acesse	Acesse
Instituída – RES Sicoob Confederação 283, de 10/4/2019	Acesse	Acesse