SICOOB Credinorte

Classificação da Informação: Restrita

POLÍTICA INSTITUCIONAL DE SEGURANÇA CIBERNÉTICA

APROVADO EM REUNIÃO DO CA DO DIA 24 DE MARÇO DE 2026

Cooperativa de Crédito Credinorte LTDA – SICOOB CREDINORTE
CNPJ: 64.276.058/0001-45
Rua Paracatu, nº 200 – Centro
Nanuque-MG, CEP: 39.860-000

Esta Política foi aprovada na Reunião do Conselho de Administração 24/03/2026, entrando em vigor e gerando seus efeitos imediato.

Assinatura dos Membros do Conselho de Administração do Sicoob Credinorte.

1. Wagner Luís Dias Cardoso
2. Victor Saúde Caires
3. Antônio Linhares Pinho
4. Diego de Souza Ribeiro
5. Flavio Fernandes de Deus
6. Franklin Robson Dias da Silva
7. Marcelo Carvalho de Oliveira
8. Márcio Roberto de Jesus
9. Nilo Caiado Fraga Neto

Resolução CCS 385

Atualiza a *Política Institucional de Gerenciamento de Risco de Liquidez* e a *Política Institucional de Segurança Cibernética*.

O Conselho de Administração do CCS, em sua 145ª reunião, realizada em 25/2/2026, decidiu:

Art. 1º Atualizar a *Política Institucional de Gerenciamento de Risco de Liquidez*, categorizada no tema Gestão de Riscos, Controles e Segurança, disponível em *Intranet do Sicoob → Menu → Normativos → CCS → Políticas*.

Parágrafo único. A demonstração das alterações do conteúdo está apresentada como anexo, disponível na opção *Download* de Anexos (📎) desta Resolução, na intranet do Sicoob.

Art. 2º Atualizar a *Política Institucional de Segurança Cibernética*, categorizada no tema Apoio e Sustentação ao Negócio, disponível em *Intranet do Sicoob → Menu → Normativos → CCS → Políticas*.

Parágrafo único. A demonstração das alterações do conteúdo está apresentada como anexo, disponível na opção *Download* de Anexos (📎) desta Resolução, na intranet do Sicoob.

Art. 3º Esta Resolução é destinada às entidades do Sicoob.

Brasília/DF, 26 de fevereiro de 2026

Miguel Ferreira de Oliveira
Conselho de Administração
Presidente

~~APRESENTAÇÃO~~

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~~s~~ Área~~s~~ de Defesa Cibernética e da Área de Detecção e Resposta a Incidentes Cibernéticos do Centro Cooperativo Sicoob (CCS);

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

d) tem aplicação imediata pelas entidades do Sicoob, devendo o conteúdo ser levado ~~ao conhecimento~~para aprovação dos seus respectivos órgãos de administração, ~~mediante~~ 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 ~~da~~ 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.

~~I. OBJETIVOS~~

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 ~~a formação e a qualificação dos recursos humanos necessários à Superintendência de Segurança Cibernética do CCS~~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.

~~II. RESPONSABILIDADES~~

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~~Sicoob Confederação~~;

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 ~~a~~ 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) ~~realizar a abertura de~~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) ~~prestar apoio~~apoiar ~~às~~ as entidades do Sicoob~~, relativo~~ sobre ~~à~~ a gestão de segurança cibernética;

e) informar, de forma tempestiva, ~~a~~ à Superintendência de Gestão Integrada de Riscos e à Área de Controles Internos e Conformidade do CCS, ~~sobre os~~ 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 ~~área responsável pela~~ Gestão Sistêmica de Segurança Cibernética do Sicoob, ~~instituída no Projeto de Gestão Sistêmica de Riscos e Segurança Cibernéticos,~~ é de responsabilidade da Superintendência de Segurança Cibernética do CCS, com reporte ao Diretor de Tecnologia da Informação do CCS.

~~III. PROCEDIMENTOS E CONTROLES~~

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 ~~mínimo~~, 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, ~~em que todas as assegurando~~ para assegurar que as fragilidades identificadas ~~são~~ sejam priorizadas e tratadas ~~de acordo~~ conforme o seu nível de criticidade e risco, por meio de planos de ação específicos, com ~~o devido~~ 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, ~~dentre~~ 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) ~~o)~~ 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 ~~Resolução CMN nº 4.893, de 26/2/2021~~;

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 ~~acima~~ 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.

~~IV. CONSIDERAÇÕES FINAIS~~

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, ~~poderão~~ 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.

1. Diretrizes gerais.

1.1 Incidente cibernético, conforme consta da Circular BCB nº 3.979, de 30/1/2020, é um evento relacionado ao ambiente cibernético que se enquadra em uma das seguintes situações:

a) produz efeito adverso ou representa ameaça aos sistemas de Tecnologia da Informação (TI), ou à informação que esses sistemas processam, armazenam ou transmitem;

b) infringe políticas ou procedimentos de segurança referentes aos sistemas de TI.

1.2 Todos os incidentes de segurança cibernética devem ser comunicados, por todas as entidades do Sicoob, à Área de Detecção e Resposta a Incidentes Cibernéticos do CCS, pelo *e-mail* soc@sicoob.com.br ou pelo telefone (61) 3217-5762, bem como ao diretor responsável na entidade em que ocorreu o incidente.

1.3 Os incidentes considerados relevantes – abordados nos itens 3, 4 e 5 deste Plano – serão comunicados, pelo Centro Cooperativo Sicoob (CCS), ao Banco Central do Brasil (BCB).

1.4 Em casos de incidentes envolvendo violação de dados pessoais, os eventos devem ser comunicados à Área de Privacidade de Dados do CCS, pelo *e-mail* dpo@sicoob.com.br.

1.5 Nos casos de incidentes envolvendo a violação de dados pessoais em cooperativas, os eventos devem ser comunicados, também, ao Encarregado responsável na cooperativa singular e na cooperativa central em que ocorreu a suspeita de violação.

1.6 Os incidentes que podem causar riscos ou danos relevantes aos titulares de dados pessoais são comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e a esses titulares que tiverem seus dados expostos.

1.7 Os incidentes de segurança cibernética envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix – ainda que não possam acarretar risco ou dano relevante aos titulares – devem ser comunicados à Área de Privacidade de Dados do CCS, que informa ao Banco Central do Brasil (BCB) e aos titulares de contas transacionais que sejam pessoas naturais, em atendimento ao Regulamento anexo à Resolução BCB nº 1 (Regulamento do Pix), de 12/8/2020.

1.7.1 Quando o incidente envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix tiver origem externa e o Sicoob for informado pelo BCB, a Área de Privacidade de Dados do CCS comunicará aos titulares de contas transacionais do Sicoob que sejam pessoas naturais, ainda que o incidente de segurança não possa acarretar riscos ou danos relevantes a esses titulares.

1.8 Cada entidade de primeiro e segundo níveis é responsável pelo tratamento e pela resposta aos incidentes cibernéticos que ocorrerem em seu ambiente tecnológico.

1.9 Os incidentes que ocorrerem no CCS serão tratados pela Área de Detecção e Resposta a Incidentes Cibernéticos.

1.10 São executados, anualmente, testes de Continuidade de Negócio, considerando cenários de indisponibilidade causada por incidentes cibernéticos.

1.11 Os empregados e prestadores de serviço terceirizados são orientados e instruídos sobre o comportamento correto de não tomar nenhuma ação própria, mas informar imediatamente o evento ou incidente à equipe responsável pelo tratamento.

1.12 Violações de segurança da informação cometidas por empregados, fornecedores ou profissionais terceirizados são analisadas e tratadas em conjunto pela Área de Gente do CCS, pela área responsável pelo empregado ou terceirizado, e pela área responsável por tratamento e resposta aos incidentes cibernéticos.

1.13 Os contratos firmados com empresas terceirizadas que suportam atividades críticas devem dispor de cláusula informando que elas precisam disponibilizar Plano de Continuidade de Negócios, bem como evidência de realização de testes desse plano.

1.14 O *Plano de Ação e Resposta a Incidentes Cibernéticos do Sicoob* é revisado anualmente e aprovado pelo Conselho de Administração do Sicoob Confederação e do Banco Sicoob.

1.15 Para fins deste Plano, são observados os seguintes conceitos:

a) *Sicoob*: cooperativas centrais e singulares, e as entidades do CCS;

b) *Centro Cooperativo Sicoob (CCS)*: composto por Sicoob Confederação, Banco Sicoob, Sicoob DTVM, Sicoob Pagamentos, Sicoob Previ, Sicoob Consórcios, Sicoob Seguradora, Instituto Sicoob e Fundo de Proteção do Sicoob.

2. Responsabilidades.

2.1 Área responsável pela segurança cibernética nas entidades:

a) ativar o plano de ação e resposta a incidentes de segurança cibernética;

b) seguir as fases do processo para tratamento de incidentes de segurança cibernética;

c) escalar pessoas para executar as fases do plano de ação e resposta a incidentes de segurança cibernética;

d) realizar a comunicação sobre incidentes cibernéticos à Área de Detecção e Resposta a Incidentes Cibernéticos do CCS;

e) comunicar os incidentes de segurança cibernética envolvendo violação de dados pessoais à Área de Privacidade de Dados do CCS;

f) comunicar a ocorrência de incidentes de segurança cibernética envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix à Área de Privacidade de Dados do CCS.

2.2 Área de Detecção e Resposta a Incidentes Cibernéticos do CCS:

a) compartilhar as informações sobre incidentes cibernéticos relativos à segurança com outras instituições financeiras, quando forem relevantes;

b) tratar os incidentes cibernéticos relativos à segurança ocorridos no CCS e apoiar as demais entidades do Sicoob no tratamento dos incidentes ocorridos em seus ambientes;

c) comunicar, à área responsável pelos controles internos do CCS, a ocorrência de incidentes cibernéticos relevantes;

d) comunicar sobre incidentes de segurança cibernética envolvendo violação de dados pessoais à Área de Privacidade de Dados do CCS;

e) comunicar sobre ocorrência de incidentes de segurança cibernética envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix à Área de Privacidade de Dados do CCS.

2.3 Área responsável por controles internos e conformidade do CCS:

a) comunicar as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes ao BCB.

2.4 Área de Privacidade de Dados do CCS:

a) comunicar ao Encarregado responsável na cooperativa central quando houver incidentes envolvendo dados pessoais na referida central ou nas suas cooperativas singulares filiadas, quando o evento for apurado pelo CCS;

b) comunicar os incidentes de violação de dados pessoais que podem causar riscos ou danos relevantes aos titulares dos dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD), e aos titulares de dados pessoais que tiverem seus dados expostos;

c) comunicar, ao BCB e aos titulares de contas transacionais que sejam pessoas naturais, as ocorrências de incidentes envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix;

d) comunicar as ocorrências de incidentes envolvendo banco de dados relacionado a componente ou à infraestrutura do Pix, quando o incidente tiver origem externa e o Sicoob for informado pelo BCB, aos titulares de contas transacionais do Sicoob que sejam pessoas naturais, ainda que o incidente de segurança não cause risco ou dano relevante aos titulares.

2.5 Cooperativas centrais e singulares:

a) informar, quando solicitado pela Área de Privacidade de Dados do CCS, quais são os titulares de contas transacionais impactados no incidente envolvendo banco de dados relacionado a componente ou a infraestrutura do Pix.

3. Critérios adotados para a avaliação da relevância dos incidentes ocorridos:

a) a criticidade do serviço;

b) a sensibilidade dos dados e das informações;

c) o impacto legal (descumprimento de lei e/ou norma ocasionado pelo incidente);

d) o impacto financeiro (gerado pelo não atendimento ao cooperado/cliente em relação ao Patrimônio de Referência, no caso das cooperativas, e ao Patrimônio Líquido do Sicoob Confederação, para os riscos sistêmicos, com base no volume de operações diárias e na perda de oportunidade de negócio);

e) o impacto de imagem (do Sicoob, gerado pela interrupção de atendimento ao cooperado/cliente);

f) a dificuldade de recuperação do incidente.

4. Os critérios para análise de relevância dos incidentes cibernéticos estão detalhados no arquivo *Critérios para Análise de Incidentes Cibernéticos* na opção *Download de Anexos* (📎) da *Política Institucional de Segurança Cibernética*, na intranet do Sicoob.

5. A planilha modelo para o registro e a classificação de incidentes cibernéticos, considerando os critérios definidos, está disponível no arquivo *Avaliação de relevância de incidentes cibernéticos*, na opção *Download de Anexos* (📎) da *Política Institucional de Segurança Cibernética*, na intranet do Sicoob. Dela constam, também, os exemplos de incidentes considerados cibernéticos e não cibernéticos.

6. Diretrizes para observação pela área responsável pelo tratamento e pela resposta a incidentes de segurança cibernética nas entidades do Sicoob:

a) os papéis da equipe de tratamento e resposta a incidentes, e as habilidades necessárias, estão diretamente relacionados aos serviços e às funções desempenhados;

b) a equipe de tratamento e resposta a incidentes deve, frequentemente, ser treinada, de forma que haja o preenchimento de lacuna de habilidades;

c) o ambiente cibernético deve ser monitorado para a identificação de possíveis incidentes de segurança cibernética.

7. Fases do processo de resposta a incidentes cibernéticos:

a) *identificar*: caracterizar todos os sistemas e as plataformas incluídos na infraestrutura, bem como prever, descrever e estar preparado para as possíveis situações de incidentes. A função de identificação inclui cinco categorias-chaves:

a.1) *gerenciamento de ativos*: identificação dos sistemas, dispositivos, usuários, dados e da infraestrutura que suportam os principais processos de negócio, e classificação, de acordo com sua criticidade;

a.2) *ambiente de negócios*: priorização da missão, das metas, dos processos da empresa e dos principais tomadores de decisões de segurança da informação;

a.3) *governança*: entendimento das políticas e dos procedimentos para gerenciar e monitorar os requisitos regulatórios, jurídicos, de risco, ambientais e operacionais;

a.4) *avaliação de riscos*: garantia do entendimento completo dos riscos de segurança cibernética que podem afetar os negócios, seus usuários e os sistemas críticos de TI;

a.5) *estratégia de gerenciamento de riscos*: estabelecimento de prioridades, desafios, tolerâncias e premissa de risco para possibilitar as melhores decisões de risco operacional;

b) *proteger*: reduzir o impacto de um incidente, diminuir consequências relacionadas ao evento e minimizar as perdas;

c) *detectar*: monitorar continuamente alertas ou outros sinais de incidentes que precisam ser investigados; verificar se o evento reportado é realmente um incidente. Nesta fase, ocorrem a coleta e análise dos dados obtidos pelas partes que detectaram o possível incidente, além da triagem do incidente para o início da fase de resposta;

d) *responder*: tomar medidas após a identificação de um incidente para garantir que os dados sejam preservados no processo. Para uma resposta adequada, os seguintes processos-chaves devem ser seguidos:

d.1) *executar este plano de respostas*: após a ameaça ser detectada e reconhecida, a função *Responder* começa com a execução dos procedimentos de resposta. Os planos devem ser executados enquanto o incidente de segurança cibernética estiver ocorrendo;

d.2) *comunicação*: procedimento de notificação formal para relatar os incidentes;

d.3) *análise*: as equipes envolvidas na resposta ao incidente cibernético examinam e investigam as notificações do sistema de detecção para analisar o impacto do incidente, bem como a adequação da resposta, quando a perícia for executada – se for o caso;

d.4) *mitigação*: processos executados para conter o incidente, evitar que ele se espalhe e mitigar o dano potencial da ameaça. Além disso, quaisquer novas vulnerabilidades não identificadas anteriormente devem ser documentadas;

d.5) *aperfeiçoamento*: as pessoas envolvidas no processo e os *stakeholders* examinam as lições aprendidas na resposta ao incidente, e incorporam as descobertas em estratégias futuras de tratamento e resposta a incidentes;

d.6) ao executar o procedimento de resposta ao incidente de segurança cibernética, a preservação de evidências sempre deve ser observada;

d.7) a continuidade dos serviços críticos deve ser priorizada;

e) *recuperar*: após a conclusão da resposta ao incidente, tem início o processo de recuperação e tratamento para o restabelecimento das atividades normais do

ambiente, por meio da eliminação das causas raízes dos alertas ou dos incidentes ocorridos e de seus efeitos. Alguns dos passos do processo de recuperação são:

e.1) restaurar os recursos remediados;

e.2) restaurar dados de becapes;

e.3) reconstruir sistemas, quando necessário;

e.4) tratar as causas raízes dos alertas ou dos incidentes reportados;

e.5) realizar testes para garantir que as causas raízes não continuam no ecossistema do Sicoob;

f) *registrar/notificar*: procedimento de registro e notificação formal para relatar os incidentes:

f.1) todos os incidentes de segurança cibernética detectados são registrados;

f.2) informações sobre incidentes cibernéticos relevantes são compartilhadas com as outras instituições autorizadas a funcionar pelo Banco Central do Brasil;

f.3) autoridades policiais competentes são comunicadas, para a adoção de medidas legais, quando necessário;

f.4) de maneira proativa, alertas sobre vulnerabilidades e incidentes de segurança em geral são divulgados às cooperativas, possibilitando a preparação contra ameaças;

g) *revisão do processo*: realização da revisão do processo de tratamento e resposta a incidente, visando seu aperfeiçoamento e considerando as seguintes questões:

g.1) quais foram as lições aprendidas;

g.2) se a preparação foi suficiente, se a implementação das ações foi efetiva e se o processo de comunicação (interno e externo) foi claro e eficaz;

g.3) levantar os resultados obtidos pelos procedimentos e controles implementados;

g.4) verificar a necessidade de novos controles, ferramentas e/ou treinamentos adicionais.

8. O relatório anual sobre a implementação do *Plano de Ação e de Resposta a Incidentes* é elaborado com a data-base de 31 de dezembro, contemplando:

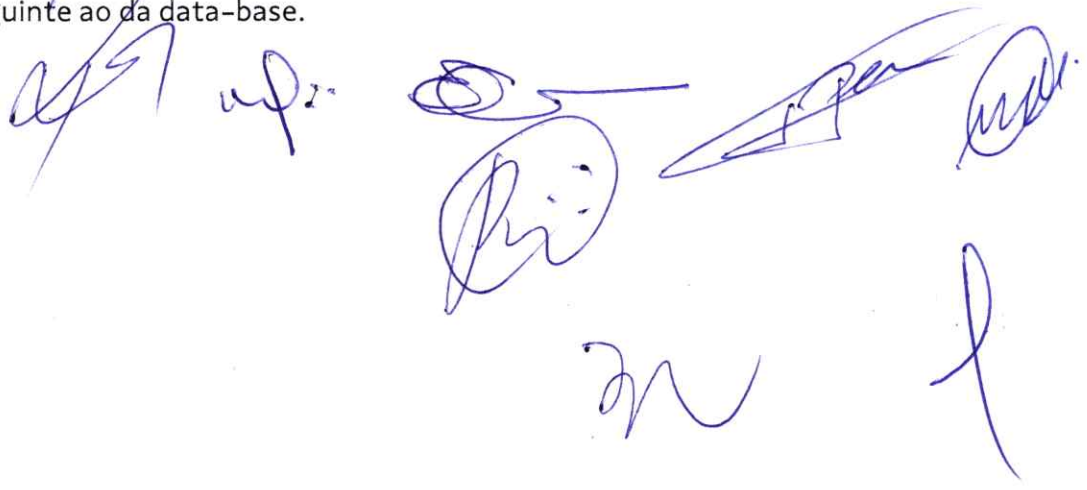
a) a efetividade da implementação das ações desenvolvidas pelas entidades do Sicoob para a adequação das estruturas organizacional e operacional aos princípios, e às diretrizes da *Política Institucional de Segurança Cibernética do Sicoob*;

b) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

c) os incidentes relevantes relacionados ao ambiente cibernético, ocorridos no período;

d) os resultados dos testes de continuidade de negócios, considerando os cenários de indisponibilidade ocasionada por incidentes cibernéticos.

9. Cada entidade do Sicoob elabora o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, o qual será submetido ao Comitê de Riscos, quando existente, e apresentado ao Conselho de Administração até 31 de março do ano seguinte ao da data-base.



1. O objetivo deste documento é apresentar os critérios para a análise de relevância dos incidentes cibernéticos, utilizados pelo Sicoob.

2. Na Tabela 1, abaixo, são apresentados os detalhes das fases e dos critérios de classificação de relevância de incidente cibernético. Os critérios foram selecionados a partir de *framework* de mercado (Ref. 1 e Ref. 2, citadas no item 4 deste documento) e da experiência anterior com a análise de impacto de negócios, que faz parte do processo de gestão de continuidade de negócios (Ref. 3, citada no item 4 deste documento).

3. *Análise de relevância de incidentes cibernéticos*: a determinação da relevância do incidente possui 4 (quatro) fases, listadas a seguir:

3.1 *1ª fase – Avaliação do incidente cibernético*

a) incidentes relacionados a sistemas de TI geralmente afetam os negócios e as funcionalidades que eles fornecem, resultando em algum impacto negativo para os usuários. A equipe de tratamento de incidentes não deve considerar somente o impacto atual, causado pelo incidente, mas também um provável impacto futuro, caso não seja tratado imediatamente;

b) na primeira etapa de avaliação, os incidentes são classificados sob 4 (quatro) critérios: *criticidade do serviço*, *impacto legal*, *impacto financeiro* e *impacto de imagem*. Cada critério possui peso diferenciado, conforme as tabelas a seguir:

Tabela 1 – Criticidade do Serviço

Criticidade do serviço (impacto na funcionalidade) – Peso 5	
Nenhum – 0	Não afeta a capacidade da organização em fornecer todos os serviços a todos os usuários.
Baixo – 1	Efeito mínimo – a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu em eficiência.
Médio – 2	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto – 3	A organização não pode fornecer alguns serviços críticos a qualquer usuário enquanto não se recuperar do incidente.

Tabela 2 – Impacto Legal - Impacto

Impacto legal (descumprimento de lei/norma) – Peso 2	
Nenhum – 0	Não há impacto legal ou regulatório para a organização.
Baixo – 1	Pode gerar advertência ou multa pecuniária por órgãos reguladores e fiscalizadores externos pelo não cumprimento de leis e normas, e a terceiros ou parceiros por força de contrato.
Médio – 2	Pode gerar, além de advertência e/ou multa, outras sanções administrativas, como rescisão de contrato, suspensão e/ou inabilitação temporária ou permanente para o exercício de cargos de direção na administração ou gerência em instituições financeiras, bem como a impossibilidade de atuação em determinados setores e/ou com determinados produtos, pelo não cumprimento de leis e/ou normas, ou por força de contrato.

Alto – 3	Pode gerar, além das sanções previstas nas respostas anteriores, a cassação da autorização de funcionamento da instituição e/ou detenção e/ou reclusão de executivos, ou a suspensão da efetividade de negócio por força de contrato.

Tabela 3 – Impacto Financeiro

Impacto financeiro (em caso de parada do serviço) – Peso 3 *	
Nenhum – 0	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *insignificante* na *Matriz de avaliação de riscos operacionais* da entidade.
Baixo – 1	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *menor* na *Matriz de avaliação de riscos operacionais* da entidade.
Médio - 2	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *moderada* na *Matriz de avaliação de riscos operacionais* da entidade.
Alto - 3	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *maior ou extrema* na *Matriz de avaliação de riscos operacionais* da entidade.

b.1) como cada entidade possui sua própria matriz de avaliação de riscos, construída com base nos valores de Patrimônio de Referência (PR), em caso de dúvidas quanto à avaliação do impacto financeiro o *Manual de Risco Operacional* deverá ser consultado.

Impacto de imagem (em caso de parada do serviço) – Peso 4	
Nenhum – 0	Não compromete a imagem.
Baixo – 1	O comprometimento é insignificante.
Médio – 2	O comprometimento merece atenção e ações corretivas.
Alto – 3	O comprometimento é significativo/severo.

3.2 *2ª fase – Avaliação da sensibilidade dos dados e das informações envolvidas no incidente*

a) incidentes podem afetar a confidencialidade, integridade e disponibilidade das informações da organização. Incidentes cibernéticos que geram vazamentos de dados pessoais, dados pessoais sensíveis ou confidenciais, por exemplo, são mais relevantes do que incidentes cibernéticos que geram vazamento de dados de uso restrito;

b) na segunda etapa de avaliação de relevância dos incidentes, o responsável pela análise deverá selecionar uma das seguintes opções:

Sensibilidade das informações – Peso 5	
Nenhum – 0	Nenhuma informação foi vazada, alterada, excluída ou comprometida.
Baixa – 1	Informações estão indisponíveis temporariamente.

Média – 2	Informações não sensíveis (sem dados pessoais) foram indevidamente acessadas, vazadas, alteradas ou excluídas.
Alta – 3	Informações pessoais e/ou sensíveis/confidenciais foram indevidamente acessadas, vazadas, alteradas ou excluídas.

3.3 *3ª fase – Avaliação da recuperabilidade do incidente*

a) a capacidade de recuperação de um incidente determina os possíveis procedimentos que a equipe de tratamento deve seguir para o tratamento. Um incidente de alto impacto aos negócios da organização e de fácil recuperação pode ser aquele em que a equipe de resposta a incidentes atue primeiro, tratando e solucionando o incidente. No entanto, pode haver casos de vazamento de dados pessoais em que seria necessário envolver não só pessoas e equipes internas da organização, mas titulares de dados e o órgão de fiscalização (ANPD). Dessa forma, a comunicação e a recuperação podem ser realizadas de forma simultânea. A equipe de tratamento deve priorizar a resposta a cada incidente de acordo com as estimativas de impacto e os recursos e esforços necessários para a sua recuperação;

b) a criticidade do incidente e os tipos de recursos afetados determinarão a quantidade de tempo e os recursos que deverão ser gastos na recuperação desse incidente. Em alguns casos, não é possível recuperar-se de um incidente (por exemplo, se a confidencialidade de informações sensíveis tiver sido comprometida) e não faria sentido gastar recursos limitados em um ciclo prolongado de tratamento de incidentes, a menos que esse esforço fosse direcionado para garantir que um incidente semelhante não ocorra no futuro.

Dificuldade de recuperação do incidente – Peso 5	
Nenhuma – 0	O tempo de recuperação é previsível, com recursos existentes.
Baixa – 1	O tempo para recuperação é previsível, com recursos adicionais.
Média – 2	O tempo para recuperação é imprevisível.
Alta – 3	A recuperação do incidente não é possível (por exemplo: dados confidenciais vazados e publicados)

3.4 *4ª fase – Determinação da relevância do incidente cibernético*

a) a relevância do incidente cibernético é determinada a partir da seleção dos critérios definidos neste documento, considerando os respectivos pesos na fórmula abaixo:

$$Relevância = (CS*5 + IL*2 + IF*3 + II*4 + SI*5 + RC*5)$$

CS - Criticidade do serviço
IL - Impacto legal
IF - Impacto financeiro
II - Impacto na imagem
SI - Sensibilidade da informação
RC - Recuperabilidade do incidente

Figura 1 – Fórmula da relevância do incidente cibernético.

b) o resultado da análise da relevância do incidente cibernético é apresentado na tabela abaixo, com a seguinte descrição:

b.1) *Incidente de relevância baixa (Incidente não relevante)*: incidente com impacto baixo/leve, de acordo com os critérios definidos neste documento;

b.2) *Incidente de relevância média (Incidente não relevante)*: incidente com impacto médio/significativo, de acordo com os critérios definidos neste documento;

b.3) *Incidente de relevância alta (Incidente relevante)*: incidente com impacto alto/grave, de acordo com os critérios definidos neste documento. O incidente com esta classificação é considerado relevante para atendimento à Resolução CMN nº 4.893/2021.

Relevância do incidente cibernético	
Baixo = de 0 a 45	INCIDENTE NÃO RELEVANTE
Médio = de 46 a 59	INCIDENTE DE RELEVÂNCIA MÉDIA
Alto >= 60	INCIDENTE DE RELEVÂNCIA ALTA

O resultado **ALTO** classifica o incidente como **RELEVANTE**.

4. Referências:

Computer Security Incident Handling Guide – NIST. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NCCIC Cyber Incident Scoring System. National Cybersecurity and Communications Integration Center. Disponível em: https://www.uscert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf
Manual de Risco Operacional
National Cyber Security Centre. Disponível em: https://www.ncsc.gov.uk
FBI. *Cyber Incident Reporting*. Disponível em: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view