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:

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

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

1.2 Os incidentes de segurança cibernética relevantes deverão 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. Os incidentes considerados relevantes serão comunicados, pelo CCS, ao Banco Central do Brasil (BCB).

1.3 No caso de incidentes envolvendo violação de dados pessoais, os eventos deverão ser comunicados à Área de Segurança da Informação do CCS, pelo *e-mail* dpo@sicoob.com.br, bem como ao *Data Protection Officer (DPO)* responsável na cooperativa singular e na cooperativa central em que ocorreu a suspeita de violação, para o caso de incidentes envolvendo dados pessoais em cooperativas.

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

1.4 Os incidentes de segurança cibernética envolvendo banco de dados relacionado a componente ou a infraestrutura do Pix, ainda que não possam acarretar risco ou dano relevante aos titulares, deverão ser comunicados à Área de Segurança da Informação do CCS que, no que lhe concerne, comunicará 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 12/08/2020.

1.4.1 Quando o incidente envolvendo banco de dados relacionado a componente ou a infraestrutura do Pix tiver origem externa e o Sicoob for informado pelo BCB, a Área de Segurança da Informação 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 aos titulares.

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

1.6 Os incidentes que vierem a ocorrer no Centro Cooperativo Sicoob serão tratados pela Área de Detecção e Resposta a Incidentes Cibernéticos do CCS.

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

1.8 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.

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

1.10 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 deste plano.

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

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

a) *Centro Cooperativo Sicoob (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;

b) *Sicoob*: cooperativas centrais e singulares, e as entidades do CCS.

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 Segurança da Informação do CCS;

f) comunicar a ocorrência de incidentes de segurança cibernética envolvendo banco de dados relacionado a componente ou a infraestrutura do Pix à Área de Segurança da Informação 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 do 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 Segurança da Informação do CCS;

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

2.3 Área responsável pelos controles internos do CCS:

a) comunicar ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes;

2.4 Área de Segurança da Informação do CCS:

a) comunicar o DPO 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 Pessoais (ANPD), e aos titulares de dados pessoais que tiverem seus dados expostos;

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

d) comunicar as ocorrências de incidentes envolvendo banco de dados relacionado a componente ou a 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 possa acarretar risco ou dano relevante aos titulares.

2.5 Cooperativas centrais e singulares:

a) informar, quando solicitado pela Área de Segurança da Informação 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. São adotados os seguintes critérios 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 registro e 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. São diretrizes para observação pela área responsável pelo tratamento e 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 plataformas incluídos na infraestrutura, prever, descrever e estar preparado para as possíveis situações de incidentes. A função de identificação inclui cinco categorias-chaves:

a) *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;

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

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

d) *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;

e) *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. Nessa fase, ocorrem a coleta e análise dos dados obtidos pelas partes que detectaram o possível incidente, e a 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, deve ser sempre observada a preservação de evidências;

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) verificar 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. É elaborado relatório anual sobre a implementação do *Plano de Ação e de Resposta a Incidentes*, com 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.