



1. Esta Política:

- a) estabelece as diretrizes e responsabilidades para a identificação, a avaliação, o tratamento e o monitoramento dos riscos cibernéticos nas operações e nos sistemas das entidades do Sicoob;
- b) foi elaborada e é revisada, anualmente, por proposta da Superintendência de Gestão Integrada de Riscos do Centro Cooperativo Sicoob (CCS), em decorrência fatos relevantes ou por sugestões encaminhadas pelas cooperativas centrais e singulares;
- c) é aprovada pelo Conselho de Administração do CCS¹;
- d) tem aplicação imediata pelas cooperativas centrais e singulares do Sicoob e deve ser levada ao conhecimento dos respectivos órgãos de administração, mediante registro em ata;
- e) compõe a gestão integrada de riscos definida na *Política Institucional de Gestão Integrada de Riscos*, e abrange os riscos específicos relacionados à segurança de sistemas, redes, infraestruturas, dados e usuários, assegurando uma abordagem abrangente para proteger as entidades do Sicoob contra ameaças no ambiente cibernético;
- f) é complementada por normas técnicas e procedimentos operacionais específicos relacionados aos riscos cibernéticos;

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

- a) *entidades do Sicoob*: as cooperativas centrais e singulares e o Centro Cooperativo Sicoob (CCS);

¹ Sicoob Confederação.



- 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;
- c)** *ameaça:* representa qualquer circunstância ou evento potencial que possa causar dano, interrupção ou comprometimento da informação e/ou dos sistemas de informação. As ameaças cibernéticas podem ser oriundas de agentes externos (*hackers*, ativistas, espiões cibernéticos etc.) ou internos (empregados descontentes, erros não intencionais etc.);
- d)** *ativo:* no contexto do risco cibernético, um ativo refere-se a qualquer item de valor tangível ou intangível que é utilizado pela organização e necessita de proteção. Isso pode incluir informações, *software*, *hardware*, infraestrutura de TI, recursos humanos, reputação da empresa, entre outros. Cada ativo tem um valor associado, e a perda, o dano ou o comprometimento desse ativo pode ter um impacto negativo para a organização;
- e)** *controle:* no contexto do risco cibernético, é uma medida ou ação implementada para mitigar, evitar, transferir ou aceitar um risco. Os controles podem ser administrativos, técnicos ou físicos, e são projetados para tratar vulnerabilidades específicas e proteger os ativos contra ameaças específicas;
- f)** *entidade:* as cooperativas centrais e singulares, e o Centro Cooperativo Sicoob (CCS) – composto por: Confederação Nacional das Cooperativas do Sicoob (Sicoob Confederação), Banco Cooperativo Sicoob (Banco Sicoob), Sicoob Distribuidora de Títulos e Valores Mobiliários (Sicoob DTVM), Sicoob Soluções de Pagamento (Sicoob Pagamentos), Fundação Sicoob de Previdência Privada (Sicoob Previ), Sicoob Administradora de Consórcios (Sicoob Consórcios), Sicoob Seguradora de Vida e Previdência . (Sicoob



Seguradora) e Instituto Sicoob para o Desenvolvimento Sustentável (Instituto Sicoob);

- g) *evento*: qualquer ocorrência observável em um ativo. Nem todos os eventos são indicativos de um problema relacionado ao risco cibernético ou à segurança cibernética; eles podem ser rotineiros ou não rotineiros. Os eventos de segurança cibernética indicam a presença de um potencial incidente ou comprometimento;
- h) *gestão integrada de riscos*: gerenciamento de riscos integrado, possibilitando a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos adversos resultantes das interações entre os riscos que impactam a entidade;
- i) *impacto*: refere-se à magnitude ou à gravidade das consequências ou aos efeitos que resultariam se uma ameaça específica explorasse uma vulnerabilidade. Essas consequências podem ser expressas em termos financeiros, reputacionais, operacionais, legais, entre outros;
- j) *incidente*: evento adverso confirmado ou uma série de eventos indesejados associados à segurança cibernética. Diferentemente dos eventos, os incidentes têm uma implicação negativa para a integridade, disponibilidade ou confidencialidade dos ativos;
- k) *probabilidade*: refere-se à chance ou possibilidade de um evento acontecer dentro de um período especificado ou sob condições específicas. No contexto da gestão de riscos cibernéticos, é a estimativa ou medida da frequência com que se espera que uma ameaça específica se materialize, explorando uma vulnerabilidade em particular;



gestão do risco cibernético, incluindo as metodologias para identificação, avaliação, tratamento e monitoramento das entidades do Sicoob;

- b)** *cooperativas centrais e singulares, sob condução do diretor responsável pelo gerenciamento de riscos:* supervisiona e implementa as diretrizes desta Política e dos manuais operacionais relacionados;
- c)** *Superintendência de Gestão Integrada de Riscos do CCS:* com reporte à Diretoria de Riscos e Controles, supervisiona as atividades de gestão do risco cibernético e revisa periodicamente a eficácia das medidas implementadas.

6. Normas Legais e Conflitos:

- a)** em caso de conflito com as normas legais, elas prevalecerão sobre esta Política;
- b)** as entidades do Sicoob devem estar em conformidade com as normas e regulamentações sobre segurança cibernética.

7. Complementam a presente Política e a ela se subordinam todas as normas internas que regulam o risco cibernético, no âmbito das entidades do Sicoob.



Controle de Atualizações

| Data | Instrumento de Comunicação | Situação |
|------------|--|------------|
| 23/12/2024 | Link CCS – RES CCS 316 Link Cooperativa – RES CCS 316 | Atualizada |
| 25/1/2024 | Link CCS – RES CCS 240 Link Cooperativa – RES CCS 240 | Instituída |