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) 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;

c) é complementada por normas técnicas e procedimentos operacionais específicos relacionados aos riscos cibernéticos;

d) 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;

e) é aprovada pelo Conselho de Administração do CCS – Sicoob Confederação;

f) tem aplicação imediata pelas cooperativas do Sicoob que adotaram o estatuto-padrão (disponível no Manual de Governança Corporativa), com conhecimento do respectivo órgão de administração, registrado em ata;

f.1) para as cooperativas que ainda estão em processo de adoção do estatuto-padrão, a adesão deve ser aprovada pelo respectivo órgão de administração definido no estatuto;

g) é divulgada internamente, por meio dos canais de comunicação do Sicoob.

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);

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: 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: 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: 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) 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;

g) 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;

h) 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;

i) 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;

j) probabilidade: chance ou possibilidade de um evento acontecer dentro de um período específico 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;

k) risco cibernético: possibilidade de que uma ameaça específica explore uma vulnerabilidade particular, levando a um dano ou uma perda para a organização, incluindo ataques maliciosos, falhas de *software*, falhas humanas em ambiente digital e outros incidentes de segurança da informação ou segurança cibernética. Esse dano pode ser tangível (como perda financeira) ou intangível (como danos à reputação);

l) risco: combinação da probabilidade de um evento ocorrer e das consequências (impacto) desse evento para uma organização;

m) vulnerabilidade: fraqueza ou lacuna em um sistema de segurança que pode ser explorada por uma ameaça para obter acesso não autorizado, causar dano ou interromper o funcionamento normal do sistema. As vulnerabilidades podem ser resultado de erros de *software*, configurações inadequadas, práticas de segurança deficientes, entre outras razões.

3. A gestão do risco cibernético abrange a identificação, a avaliação, o tratamento e o monitoramento dos riscos relacionados à segurança de sistemas, redes, infraestruturas, dados e usuários das entidades do Sicoob.

4. O ciclo de identificação, avaliação, tratamento e monitoramento do risco cibernético – incluindo a reavaliação dos riscos identificados e a realização dos testes de avaliação dos sistemas de controle – é realizado, no mínimo, bienalmente. Em casos excepcionais, a Diretoria Executiva do CCS pode prorrogar ou antecipar o prazo do ciclo.

5. Das responsabilidades:

a) Gerência de Risco Cibernético do CCS: responsável pela estrutura centralizada de gestão do risco cibernético e por coordenar e implementar a 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

Instrumento de comunicação	*Link* CCS	*Link* Cooperativa
Atualizada – Resolução CCS 374, de 17/11/2025	Acesse	Acesse
Atualizada – Resolução CCS 316, de 25/1/2024	Acesse	Acesse
Instituída – Resolução CCS 240, de 25/1/2024	Acesse	Acesse