1. Esta Política estabelece as diretrizes e responsabilidades para a identificação, avaliação, o tratamento e monitoramento dos riscos cibernéticos nas operações e nos sistemas das entidades do Sicoob. A gestão do risco cibernético compõe a gestão integrada de riscos definida na *Política Institucional de Gestão Integrada de Riscos*, e abrange os riscos específicos relacionados a segurança de sistemas, redes, infraestruturas, dados e usuários, assegurando uma abordagem abrangente para proteger as entidades do Sicoob contra ameaças no ambiente cibernético.

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

a) *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.);

b) *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;

c) *controle*: no contexto do risco cibernético, é uma medida ou ação implementada para mitigar, evitar, transferir ou aceitar um risco. Controles podem ser administrativos, técnicos ou físicos, e são projetados para tratar vulnerabilidades específicas e proteger os ativos contra ameaças específicas;

d) *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 Ltda. (Sicoob DTVM), Sicoob Soluções de Pagamento Ltda. (Sicoob Pagamentos), Fundação Sicoob de Previdência Privada (Sicoob Previ), Sicoob Administradora de Consórcios Ltda. (Sicoob Consórcios), Sicoob Seguradora de Vida e Previdência Privada Ltda. (Sicoob Seguradora) e Instituto Sicoob para o Desenvolvimento Sustentável (Instituto Sicoob);

e) *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 potencial de um incidente ou comprometimento;

f) *gestão integrada de riscos*: gerenciamento de riscos integrado, possibilitando a identificação, mensuração, avaliação, o monitoramento, reporte, controle e

a mitigação dos efeitos adversos resultantes das interações entre os riscos que impactam a entidade;

g) *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;

h) *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;

i) *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;

j) *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);

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

l) *vulnerabilidade*: refere-se a uma 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, avaliação, o tratamento e monitoramento dos riscos relacionados à segurança de sistemas, redes, infraestruturas, dados e usuários das entidades do Sicoob.

4. Esta Política foi aprovada pelo Conselho de Administração do Sicoob Confederação e do Banco Sicoob. As entidades do Sicoob devem aderir e seguir este normativo.

5. Esta Política é revisada, no mínimo, anualmente, por proposta da gerência responsável pelo gerenciamento do risco cibernético do CCS, em decorrência de fatos relevantes ou por sugestões encaminhadas pelas cooperativas centrais e singulares.

6. 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 poderá prorrogar ou antecipar o prazo do ciclo.

7. Das responsabilidades:

   a) *Gerência de Risco Cibernético do CCS*: responsável pela estrutura centralizada de gestão do risco cibernético das entidades do Sicoob;

   b) *cooperativas centrais e singulares, sob condução do diretor responsável pelo gerenciamento de riscos*: devem supervisionar e implementar 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, supervisionará as atividades de gestão do risco cibernético e revisará periodicamente a eficácia das medidas implementadas;

   d) *Gerência de Risco Cibernético do CCS*: responsável por coordenar e implementar a gestão do risco cibernético, incluindo as metodologias para identificação, avaliação, tratamento e monitoramento.

8. Normas Legais e Conflitos:

   a) em caso de conflito com as normas legais, elas prevalecerão sobre esta Política;

   b) esta Política é complementada por normas técnicas e procedimentos operacionais específicos relacionados a riscos cibernéticos;

   c) as entidades do Sicoob devem estar em conformidade com as normas e regulamentações sobre segurança cibernética.

9. Esta Política é aprovada, no âmbito das entidades do Sicoob, pelos respectivos órgãos de administração, e tem efeito a partir da data de aprovação.