POLÍTICA DE SEGURANÇA CIBERNÉTICA DA COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS EMPREGADOS DE ESTABELECIMENTOS HOSPITALARES DO SUL DO ESTADO DO ESPÍRITO SANTO – SULCRED.

1. APRESENTAÇÃO

A presente **POLÍTICA DE SEGURANÇA CIBERNÉTICA** estabelece princípios, diretrizes, responsabilidades e controles adotados pela SULCRED, visando proteger as informações, sistemas tecnológicos e dados sob sua responsabilidade.

Esta Política observa a Resolução CMN nº 4.893/2021, que dispõe sobre segurança cibernética e requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem pelas instituições autorizadas pelo Banco Central do Brasil. As diretrizes consideram o porte, natureza, complexidade das operações, estrutura, perfil de risco e modelo de Negócios da **SULCRED**.

2. POLÍTICA DE SEGURANÇA CIBERNÉTICA DA SULCRED

2.1 Objetivo

A Política Institucional de Segurança Cibernética da SULCRED tem como objetivo:

a) definir as diretrizes de segurança cibernética relacionadas à capacidade da Cooperativa de prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados ao ambiente cibernético;

b) reforçar o comprometimento da Diretoria com a melhoria contínua dos procedimentos e controles relacionados à segurança cibernética;

c) proteger as informações sob responsabilidade da Cooperativa, preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

d) prevenir eventual interrupção, total ou parcial, dos serviços tecnológicos utilizados pela Cooperativa e, no caso de ocorrência, reduzir os impactos resultantes;

e) estabelecer procedimentos para prevenção, identificação, tratamento e resposta a incidentes de segurança cibernética;

f) promover a conscientização e capacitação dos colaboradores e demais usuários autorizados quanto às boas práticas de segurança da informação;

g) assegurar que os serviços de tecnologia contratados, incluindo processamento, armazenamento de dados e computação em nuvem, observem os requisitos de segurança e regulamentação aplicáveis.

2.2 Esta Política deve ser observada por todos os componentes da estrutura organizacional da Cooperativa, bem como por prestadores de serviços e demais pessoas com acesso autorizado às informações da instituição.

3. DA POLÍTICA

A Política Institucional de Segurança Cibernética da SULCRED estabelece princípios, diretrizes, responsabilidades e controles destinados à proteção das informações, dos recursos tecnológicos e dos dados sob responsabilidade da Cooperativa.

A SULCRED adota práticas de segurança cibernética compatíveis com seu porte, natureza, complexidade das operações, estrutura, perfil de risco e modelo de negócio, buscando garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações.

3.1 São atribuições da Diretoria:

a) assegurar a aderência da Cooperativa às políticas, diretrizes e estratégias relacionadas à segurança cibernética;

b) assegurar a correção tempestiva de eventuais deficiências identificadas nos processos e controles relacionados à segurança cibernética;

c) promover a disseminação da cultura de segurança cibernética entre colaboradores, prestadores de serviços e demais envolvidos;

d) aprovar e revisar a Política Institucional de Segurança Cibernética, bem como acompanhar sua efetiva implementação;

e) definir e acompanhar planos, procedimentos e controles necessários para o gerenciamento da segurança cibernética da Cooperativa;

f) acompanhar os riscos relacionados ao ambiente cibernético e deliberar sobre medidas necessárias para sua mitigação;

g) designar o responsável pela gestão da Segurança Cibernética da Cooperativa.

3.2 São atribuições do responsável pela Segurança Cibernética:

a) acompanhar a implementação e o cumprimento desta Política;

b) supervisionar os controles e procedimentos relacionados à segurança cibernética, buscando seu constante aperfeiçoamento;

c) apoiar a execução e acompanhamento do Plano de Ação e Resposta a Incidentes;

d) comunicar à Diretoria a ocorrência de incidentes cibernéticos relevantes;

e) promover ações de orientação e conscientização sobre segurança da informação.

3.3 São atribuições dos colaboradores e demais usuários autorizados:

Todos os colaboradores, prestadores de serviços e usuários autorizados são responsáveis pela proteção das informações acessadas durante o exercício de suas atividades, devendo:

a) utilizar os recursos tecnológicos da Cooperativa exclusivamente para as finalidades autorizadas;

b) tratar as informações da Cooperativa, cooperados e terceiros de forma ética, segura e sigilosa;

c) preservar suas credenciais de acesso, sendo as senhas pessoais, sigilosas e intransferíveis;

d) comunicar imediatamente qualquer suspeita ou ocorrência de incidente relacionado à segurança cibernética.

3.4 Diretrizes e Controles de Segurança Cibernética

Para reduzir vulnerabilidades, prevenir incidentes e proteger as informações, a Cooperativa adotará procedimentos e controles compatíveis com sua estrutura, contemplando:

a) controle de acesso aos sistemas e informações conforme as responsabilidades atribuídas a cada usuário;

b) aplicação do princípio do menor privilégio, permitindo acesso somente às informações e recursos necessários para execução das atividades;

c) segregação de funções, sempre que aplicável, evitando que uma única pessoa execute e controle integralmente atividades críticas;

d) utilização de mecanismos de autenticação, incluindo duplo fator de autenticação quando disponível;

e) proteção contra softwares maliciosos e ameaças cibernéticas;

f) atualização e monitoramento dos recursos tecnológicos utilizados;

g) utilização de mecanismos que permitam a rastreabilidade das operações realizadas;

h) proteção contra vazamento, alteração indevida ou perda de informações;

i) manutenção de cópias de segurança (backup) das informações relevantes;

j) adoção de critérios de segurança na contratação de prestadores de serviços relacionados ao processamento, armazenamento de dados e computação em nuvem.

3.5 Prestadores de Serviços

Os procedimentos e controles de segurança cibernética devem ser observados também pelos prestadores de serviços que tenham acesso a dados, informações ou sistemas relevantes da Cooperativa.

As empresas contratadas deverão possuir capacidade técnica e controles adequados para garantir a confidencialidade, integridade, disponibilidade e segurança das informações sob sua responsabilidade.

3.6 Cultura de Segurança Cibernética

A SULCRED promoverá ações de conscientização e orientação visando fortalecer a cultura de segurança da informação, incentivando boas práticas na utilização dos recursos tecnológicos e na proteção dos dados da Cooperativa.

4. Diretrizes

A Política de Segurança Cibernética da SULCRED observa as seguintes diretrizes para a proteção das informações, dos sistemas e do ambiente cibernético, considerando seu porte, estrutura, perfil de risco, modelo de negócio e complexidade das operações.

São diretrizes da Política de Segurança Cibernética:

a) As informações da Cooperativa, dos cooperados, colaboradores, prestadores de serviços e demais envolvidos devem ser tratadas de forma ética, segura e sigilosa, de acordo com a legislação vigente e normas internas, evitando uso inadequado, alteração, perda ou exposição indevida.

b) A informação deve ser utilizada de forma transparente e exclusivamente para a finalidade para a qual foi coletada ou autorizada.

c) Os processos devem observar, sempre que aplicável, a segregação de funções, evitando que uma única pessoa execute e controle integralmente atividades críticas.

d) O acesso às informações, sistemas e recursos tecnológicos deve ocorrer somente quando devidamente autorizado e conforme as atribuições de cada usuário.

e) A identificação de cada usuário deve ser única, pessoal e intransferível, possibilitando a rastreabilidade das ações realizadas.

f) A concessão de acessos deve seguir o princípio do menor privilegio, permitindo que os usuários tenham acesso somente aos recursos e informações necessários para o desempenho de suas atividades.

g) As senhas e demais credenciais de acesso são pessoais, sigilosas e intransferíveis, sendo proibido seu compartilhamento.

h) Devem ser adotados procedimentos e controles visando prevenir, detectar e reduzir vulnerabilidades relacionadas a incidentes cibernéticos.

i) Devem ser mantidos mecanismos de segurança destinados à proteção das informações, incluindo controles de acesso, rastreabilidade, proteção contra ameaças cibernéticas e cópias de segurança.

j) Os riscos, fragilidades ou incidentes relacionados à segurança cibernética devem ser comunicados ao responsável designado para avaliação e adoção das medidas necessárias.

k) Prestadores de serviços que tenham acesso a dados, sistemas ou informações da Cooperativa devem observar requisitos de segurança, sigilo e confidencialidade.

l) As responsabilidades relacionadas à Segurança da Informação devem ser divulgadas aos colaboradores e demais envolvidos, visando fortalecer a cultura de segurança cibernética.

5. RESPONSABILIDADES

5.1 Diretoria

Compete à Diretoria assegurar a aderência da Cooperativa às diretrizes relacionadas à segurança cibernética, aprovar e revisar esta Política, acompanhar sua implementação, promover melhoria contínua dos controles e designar o Diretor responsável pela Segurança Cibernética.

5.2 Diretor Responsável pela Segurança Cibernética

O Diretor responsável pela Política de Segurança Cibernética será designado pela Diretoria da SULCRED, podendo desempenhar outras funções, desde que não haja conflito de interesses.

Compete acompanhar a implementação da Política, supervisionar controles, acompanhar o Plano de Ação e Resposta a Incidentes e comunicar eventos relevantes à Diretoria.

A política deverá ser divulgada aos colaboradores, prestadores de serviços e demais partes interessadas aplicáveis.

5.3 Colaboradores e usuários autorizados

Devem proteger as informações, utilizar recursos tecnológicos de forma segura, manter sigilo das credenciais e comunicar suspeitas de incidentes.

6. ESTRUTURA, SEGURANÇA FÍSICA E CONTROLE DE ACESSO

A SULCRED manterá estrutura tecnológica compatível com seu porte e atividades, adotando controles destinados à proteção dos recursos tecnológicos e informações.

O acesso aos sistemas deverá ocorrer mediante identificação individual e perfis compatíveis com as responsabilidades atribuídas.

7. SEGURANÇA E TRATAMENTO DAS INFORMAÇÕES

Os sistemas utilizados pela Cooperativa, inclusive contratados de terceiros, deverão possuir controles destinados à segurança, confidencialidade, integridade e disponibilidade das informações.

A Cooperativa manterá procedimentos de backup das informações relevantes visando recuperação e continuidade das atividades.

As informações deverão ser protegidas conforme seu grau de confidencialidade.

8. RISCOS CIBERNÉTICOS E ATIVOS DA INFORMAÇÃO:

Os riscos relacionados ao ambiente tecnológico deverão ser identificados, avaliados e tratados conforme sua relevância.

São considerados ativos da informação os sistemas, equipamentos, conectividades, dados, documentos e demais recursos necessários às atividades da Cooperativa.

9. PROCEDIMENTOS E CONTROLES

A Cooperativa adotará controles compatíveis com sua estrutura, incluindo:

a) proteção contra softwares maliciosos;

b) atualização de sistemas;

c) controle de acessos;

d) autenticação adicional quando disponível;

e) prevenção contra vazamento de informações;

f) manutenção de cópias de segurança.

10. PROCESSO DE SEGURANÇA DA INFORMAÇÃO

A Cooperativa manterá processos relacionados à gestão de ativos da informação, classificação das informações, gestão de acessos e gestão dos riscos cibernéticos.

11. CONTROLE DE PRESTADORES DE SERVIÇOS

Prestadores de serviços que tenham acesso a dados, sistemas ou informações relevantes deverão possuir controles adequados de segurança, confidencialidade e proteção das informações.

12. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A SULCRED manterá Plano de Ação e Resposta a Incidentes contemplando procedimentos para prevenção, identificação, comunicação, tratamento, recuperação e melhoria contínua dos controles relacionados à segurança cibernética.

São considerados incidentes de segurança da informação eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações e dos serviços tecnológicos da Cooperativa, incluindo:

a) indisponibilidade de sistemas essenciais utilizados pela Cooperativa;

b) falhas de conexão ou interrupção de acesso à internet;

c) indisponibilidade de recursos tecnológicos necessários à continuidade das atividades;

d) comprometimento de equipamentos por vírus, ou outras ameaças cibernéticas;

e) tentativa ou ocorrência de acesso não autorizado aos sistemas e informações;

f) vazamento, perda, alteração indevida ou exposição de informações.

Qualquer colaborador que identificar ou suspeitar de incidente deverá comunicar imediatamente ao Diretor responsável pela Segurança Cibernética para avaliação dos impactos e adoção das medidas necessárias.

Os incidentes identificados deverão ser registrados, analisados e tratados conforme sua criticidade, contemplando ações de contenção, recuperação e prevenção de recorrência.

13. MONITORAMENTO, TESTES E CONSCIENTIZAÇÃO

O ambiente tecnológico deverá ser acompanhado visando identificar vulnerabilidades e oportunidades de melhoria.

A Cooperativa promoverá ações para disseminar a cultura de Segurança da Informação.

14. APROVAÇÃO, DIVULGAÇÃO E REVISÃO

Esta Política foi aprovada pela Assembleia Geral Ordinária realizada em 29 de abril de 2026 e homologada pelo Conselho de Administração, conforme Ata de 22 de maio de 2026. Será revisada periodicamente ou sempre que houver alterações regulatórias, tecnológicas ou operacionais relevantes.