cooperunicamp
Cooperativa de Economia e Crédito Mutuo dos Servidores da UNICAMP

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

SUMÁRIO

1. HISTÓRICO DE REVISÃO

Versão:	**Data da Aprovação:**	**Histórico:**
01	01/09/2025	Elaboração da Política

2. OBJETIVO

Este documento tem por objetivo definir as diretrizes, as responsabilidades e os princípios relativos à Política de Segurança Cibernética da Informação (Política). A Política foi elaborada em linha com as melhores práticas de mercado, considerando adequados ao porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SERVIDORES DA UNIVERSIDADE ESTADUAL DE CAMPINAS – COOPERUNICAMP, bem como em conformidade com a legislação e com regulamentações aplicáveis.

3. RESPONSABILIDADES DAS ÁREAS ENVOLVIDAS

Os serviços de tecnologia da informação utilizados pela COOPERUNICAMP são terceirizados, composto pelas empresas **PRODAF INFORMATICA LTDA** (sistema Syscoop32 e Syscoopweb); **CONSIGNET SISTEMAS LTDA** (sistema de consignação da FUNCAMP), **SISTEMA DE GERENCIAMENTO DE CONSIGNADOS GGBS UNICAMP** (sistema de gerenciamento de consignados da UNICAMP); **EDUARDO FERNANDO DENTELLO ME** (empresa contratada para o gerenciamento da TI), **AGENCIA LOGICA DIGITAL LTDA** (empresa contratada para o gerenciamento e manutenção do site). Os contratos de prestação de serviços são geridos pela Diretoria Executiva e monitorados pelo Gerente.

Diretoria Executiva:

Responsável por:

a) Aprovar a Política de Segurança Cibernética e Segurança da Informação;
b) Monitorar a aplicação dos procedimentos que atendam a legislação;
c) Aprovar as revisões e atualizações.

Gerente:

Responsável por:

a) Elaborar a política em conjunto com os demais responsáveis;
b) Propor aprovação da política;
c) Divulgar e manter a política atualizada;
d) Acompanhar a aplicação da política;
e) Elaborar relatório anual e plano de ação e de resposta a incidentes;
f) Dar ciência aos colaboradores e prestadores de serviços sobre a política.

4. PÚBLICO-ALVO

Esta política destina-se:

A todos os colaboradores da Cooperativa;

Aos prestadores de serviços, pessoas físicas ou jurídicas, que manuseiem dados ou informações sensíveis à condução das atividades operacionais da Cooperativa.

5. FINALIDADE

Estabelecer os princípios, conceitos, valores e práticas de proteção das informações da Cooperativa, dos associados e usuários em geral, visando:

a) Proteger o valor, a reputação e integridade da Cooperativa;

b) Garantir a confidencialidade, integridade e disponibilidade das informações da Cooperativa, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

c) Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos;

d) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres significativos;

e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da Cooperativa;

f) Conscientizar, educar e treinar os colaboradores por meio da Política de Segurança Cibernética e Segurança da Informação, sobre normas e procedimentos internos aplicáveis as suas atividades diárias;

g) Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

6. CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos, abrangendo:

a) Confidencialidade: garantia de que a informação é acessível somente às pessoas autorizadas;

b) Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

d) Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da Cooperativa causando danos financeiros e de reputação consideráveis.

e) Backup: cópia de segurança de dados em mídia magnética (disco, fita ou outro instrumento;

f) Tecnológico de armazenamento de dados em nuvem, que pode ser restaurada pelo processo conhecido como "restore" em caso de perda dos dados originais.

7. RISCOS CIBERNÉTICOS

Os riscos cibernéticos são tentativas criminosas de danificar, roubar ou destruir dados, comprometendo sites, servidores ou interrompendo infraestruturas inteiras de tecnologia, alguns desses riscos são:

a) Malwares: software que causa danos a máquina, rede, softwares e banco de dados;

b) Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

c) Spyware: software malicioso para coletar e monitorar o uso de informações;

d) Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja restabelecido;

e) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

f) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

g) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

h) Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

i) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;

j) Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico;

k) Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição. No caso dos Botnets, o ataque vem de muitos computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

8. PRINCÍPIOS

A proteção e privacidade de dados dos associados e usuários refletem os valores da Cooperativa e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

a) São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;

b) Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;

c) Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;

d) As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

9. DIRETRIZES

O cumprimento da Política de Segurança Cibernética e Segurança da Informação é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

a) As informações da Cooperativa, dos associados e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

b) Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;

c) Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;

d) Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Cooperativa;

e) Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;

f) Garantir a continuidade do processamento das informações críticas de negócios;

g) Atender às leis que regulamentam as atividades da Cooperativa e sua área de atuação;

h) Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

i) Comunicar imediatamente à Diretoria Executiva, quaisquer descumprimentos da Política de Segurança Cibernética e Segurança da Informação;

j) O acesso às informações e recursos só deve ser feito se devidamente autorizado;

k) A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

l) A senha é utilizada como assinatura eletrônica através de verificação através de Multifator e deve ser mantida secreta, sendo proibido seu compartilhamento;

m) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

10. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política de Segurança Cibernética e Segurança da Informação, dentro os quais compreendem:

10.1. Gestão de Acessos às Informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação da Diretoria Executiva, responsáveis pelos quesitos de segurança da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

10.2. Gestão de Riscos

Os riscos devem ser identificados por meio de processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Cooperativa, para que sejam recomendadas as proteções adequadas.

10.3. Proteção do Ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações.

10.4. Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais. Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

10.5. Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

10.6. Processamento, Armazenamento de Dados e Computação em Nuvens

Para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Cooperativa deve assegurar-se de um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

10.7. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

10.8. Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da Cooperativa e às boas práticas de segurança.

11. RESPONSABILIDADE

O Diretor Responsável pela área de Segurança Cibernética e Segurança da Informação se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas em reuniões da Diretoria Executiva da Cooperativa, quando necessário.

12. COMPARTILHAMENTO DE INFORMAÇÕES

O Diretor Responsável pela área de atuação da Segurança Cibernética e Segurança da Informação se compromete a comunicar tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e as interrupções dos serviços relevantes, que configurem uma situação de crise, bem como as providências para o reinício das suas atividades.

13. DISPOSIÇÕES GERAIS

A Cooperativa estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética. O plano mencionado no caput deve abranger, no mínimo:

a) as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

b) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

c) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

A Cooperativa designará diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

A Cooperativa elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, abordando, no mínimo:

a) a efetividade da implementação das ações;

b) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias utilizados na prevenção e na resposta a incidentes descritos

c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

d) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Os relatórios e demais documentos, tais como atas de reuniões, contratos e plano de ação relativo à política de segurança cibernética permanecerão à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos.

14. APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

Esta Política deve ser apreciada em reunião da Diretoria Executiva, aprovada na assembleia geral e divulgada a todos os componentes da estrutura organizacional da Cooperativa e aos prestadores de serviços terceirizados.

A revisão desta política é de responsabilidade da Diretoria Executiva.

A fim de assegurar a constante adequação e eficácia desta política, a revisão deverá ser anualmente ou quando necessário decorrentes de mudanças na legislação ou ainda atualizações de processos internos.

15. BASE REGULATÓRIA

Resolução CMN n° 4.893 de 26/2/2021.

Rafael Lucas Tolentino
Diretor responsável pela Política de Segurança Cibernética e da Informação.

Thiago Sancassani
Presidente

Jhony da Silva Esteves
Diretor Tesoureiro

Rafael Lucas Tolentino
Diretor Secretário