

 <p><b>COOPESF</b> COOPERATIVA DE CRÉDITO</p>	<p><b>Elaborado:</b> Cooperativa de Crédito e Serviços Financeiros de Curitiba e Região Metropolitana - COOPESF</p>
<p><b>POLÍTICA DE SEGURANÇA CIBERNÉTICA</b></p>	
<p><b>Aprovado:</b> Conselho de Administração</p>	<p><b>Ata Nº: 263</b> <b>Data Aprovação: 18/04/2024</b></p>
<p><b>Início Vigência: mai 2022</b></p>	<p><b>Revisado: abr 2024</b></p>

## **POLÍTICA DE SEGURANÇA CIBERNÉTICA – COOPESF**

### **1. INTRODUÇÃO**

O presente instrumento visa atender às regulamentações vigentes no que diz respeito a confidencialidade, integridade e a disponibilidade das informações de propriedade da COOPESF, delineando a estratégia de que a segurança da informação é um atributo imprescindível para a proteção dos ativos tangíveis e intangíveis da organização.

A definição dos controles de segurança cibernética e da informação são alicerces importantes para a construção das políticas dos processos internos no que diz respeito a clientes, fornecedores e parceiros de negócios.

### **2. OBJETIVO GERAL**

A Política de Segurança Cibernética da COOPESF busca assegurar, prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético zelando pelo sigilo das operações de instituições financeiras conforme Lei Complementar nº 105/2001 e a observância à Resolução CMN nº 4.893 de 26/02/2021.

Política que visa garantir a confidencialidade, a integridade, e a disponibilidade de dados sistêmicos de informações utilizados pela Cooperativa, na prestação de seus serviços e execução de seu objeto social zelando pelo sigilo das operações e a proteção dos dados.

### **3. OBJETIVOS ESPECÍFICOS**

Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos, a COOPESF desenvolve controles que:

- I. Evitam a autenticação, a criptografia, a prevenção e a detecção de intrusão;
- II. Previnem vazamento de informações;
- III. Promovem testes periódicos e varreduras para a detecção de vulnerabilidades;
- IV. Buscam a proteção contra softwares maliciosos;
- V. Estabelecem mecanismos de rastreabilidade, verificação dos controles de acesso e de segmentação da rede de computadores;
- VI. Mantém cópias de segurança dos dados e das informações.

Os procedimentos acima citados são igualmente aplicados no desenvolvimento de sistemas de informação e na adoção de novas tecnologias aplicadas nas atividades da COOPESF.

### **4. DIRETRIZES GERAIS**

Os controles existentes permitem a rastreabilidade da informação, de forma a garantir a segurança das informações sensíveis. Em conjunto com a empresa fornecedora do software são feitos registros, análise da causa e o impacto, bem como o controle dos efeitos de eventuais incidentes cibernéticos.

Nesse contexto, foram definidas diretrizes que contemplam a elaboração de cenários de incidentes, com base nos testes de continuidade de negócios realizados em conjunto com a empresa fornecedora do software, sempre levando em conta os níveis de

complexidade, abrangência e precisão compatíveis com o porte da instituição.

Por seu turno, a empresa fornecedora do software comprometeu-se contratualmente a manter controles voltados à prevenção e ao tratamento de incidentes, visando a integridade dos dados ou informações sensíveis relevantes para a condução das atividades operacionais da instituição.

Em face do porte, perfil e do modelo de negócios da instituição, os dados e as informações são todos considerados relevantes, assim como quaisquer incidentes verificados.

Para disseminação da cultura de segurança cibernética, a instituição:

- a) Mantém programa permanente de capacitação e de avaliação periódica do pessoal da área;
- b) Mantém suporte para gerenciamento de controle de todos os processos sistêmicos, seja através de empresa prestadora de serviços e fornecimento de software ou através de contratos com prestador de serviços de IT – Information Technology;
- c) Alerta continuamente os cooperados sobre as precauções na utilização de produtos e serviços financeiros acessados via sistemas;
- d) Tem o compromisso de sua alta administração (conselho e diretoria executiva) com a melhoria contínua dos procedimentos relacionados à segurança cibernética;

Mesmo não possuindo armazenamento de dados e informações em nuvem, a COOPESF mantém relacionamento com outras cooperativas com vistas ao compartilhamento de incidentes

relacionados à segurança das informações, mesmo com aquelas que não se utilizam do mesmo software operacional.

## **5. PLANO DE AÇÃO E RESPOSTA A INCIDENTES**

A COOPESF mantém Plano de Ação e de Resposta a Incidentes, o qual está sob a responsabilidade do Diretor Administrativo Financeiro, e que abrange:

- a) O desenvolvimento e a adequação de suas estruturas organizacional e operacional aos princípios e diretrizes do presente Plano de Segurança Cibernética; e
- b) Manutenção de rotinas, procedimentos, controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes cibernéticos.
- c) Manual de Segurança da Informação, onde constam todas as diretrizes e procedimentos a serem adotados em caso de situações análogas e que comprometam o desenvolvimento das atividades e paralizações do sistema computacional.

## **6. GERENCIAMENTO DE RISCOS**

Além disso, a política de gerenciamento de riscos da COOPESF prevê, no tocante à continuidade de negócio:

- a) Verificação do tratamento dos incidentes relevantes relacionados com o ambiente cibernético, bem como o tratamento previsto para mitigar as consequências de eventual interrupção de serviços;
- b) Procedimentos a serem seguidos no caso da interrupção de serviços de processamento e armazenamento de dados e de

informações e a previsão de prazo para o reinício ou normalização das atividades;

- c) Realização de testes de continuidade de negócios com base em cenários de incidentes cibernéticos; e
- d) Comunicação ao Banco Central do Brasil das ocorrências de incidentes relevantes.

A COOPESF mantém mecanismos de acompanhamento e controle, os quais são sistematicamente submetidos a testes pela auditoria interna e Conselho Fiscal, incluindo:


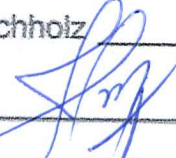
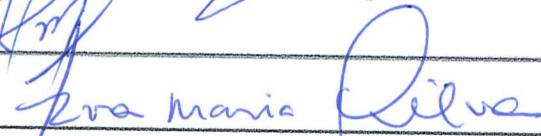


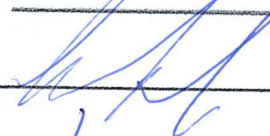
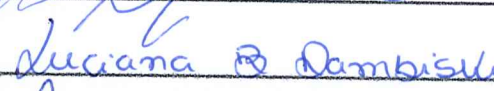

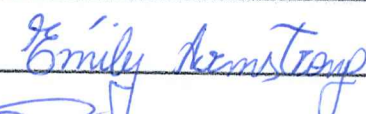

- a) Definição de processos, testes e trilhas de auditoria;
- b) Definição de métricas e indicadores adequados, compatíveis com o porte e complexidade de suas operações; e
- c) Identificação e correção de eventuais deficiências.

O presente Plano de Segurança Cibernética foi aprovado pelo Conselho de Administração e seu conteúdo foi divulgado aos funcionários da instituição, por meio de circular interna e formalmente à empresa fornecedora do software operacional. Também foram divulgadas aos cooperados, através da página na Internet da COOPESF, as linhas gerais do presente documento.

**COOPERATIVA DE CRÉDITO E SERVIÇOS FINANCEIROS  
DE CURITIBA E REGIÃO METROPOLITANA  
DIRETORIA EXECUTIVA**

Curitiba, 24 de abril de 2024

**CONFIRMAÇÃO DE CIÊNCIA/CONHECIMENTO DA REVISÃO DA  
ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA**

<b>NOME</b>	<b>ASSINATURA</b>
Claudinei Fernando Eschholz	
Jorge Luiz Moreira	
Eva Maria Quiles da Silva	
Nelsi Pischke	
Márcia Fernandes da Silva	
Moacir Cardoso Júnior	
Luciana Barroso Dambiski	
Patricia Bail de Oliveira	
Emily Paola Armstrong da Cruz	
Wallace Gois do Amaral	

**COOPERATIVA DE CRÉDITO E SERVIÇOS FINANCEIROS DE CURITIBA E  
REGIÃO METROPOLITANA - COOPESF**