POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E RISCO CIBERNÉTICO

COOPERATA - CONTROLES INTERNOS – 2026

ÍNDICE

1. INTRODUÇÃO

A Cooperativa de Economia e Crédito Mútuo dos Funcionários do Atacadão – **COOPERATA** incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios se baseiam em princípios éticos, os quais devem ser compartilhados por todos os seus colaboradores. Na constante busca do seu desenvolvimento e da satisfação dos associados, a cooperativa busca transparência e cumprimento da legislação aplicável às atividades de administração e gestão de recursos de terceiros.

A Política de Segurança da Informação e Risco Cibernético se dedica em esclarecer e nortear quais as melhores práticas adotadas pela organização para a proteção das informações estratégicas, gerenciais e operacionais. Como também a sua aderência às leis, normas e regulamentos aplicáveis ao porte, perfil de risco, modelo de negócio, natureza e complexidade das operações e a sensibilidade dos dados e informações sob responsabilidade da instituição.

Este documento constitui o resumo contendo as linhas gerais da Política de Segurança da Informação e Risco Cibernético da COOPERATA, em atendimento ao Art. 5º da Resolução CMN nº 4.893/2021.

2. ABRANGÊNCIA E VIGÊNCIA

A Política de Segurança da Informação e risco cibernético tem abrangência corporativa para estrutura organizacional da **COOPERATA,** ou seja, afeta todas as suas áreas de negócio, atendimento, administração e demais operações no que se refere a ocorrência de incidentes de segurança da informação.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, diretoria, conselho fiscal, delegados, cooperados e prestadores de serviço e se aplica à informação em qualquer meio ou suporte.

Considera-se o início da vigência quando aprovada pela Diretoria Executiva, com revisões periódicas a cada ano, ou em menor intervalo, caso haja necessidade de qualquer alteração que afete as instruções aqui descritas.

3. OBJETIVO

Com objetivo de fortalecer e aprimorar as práticas adotadas, demonstrar compromisso com a segurança dos dados e todas as partes relacionadas à **COOPERATA,** estabelecemos diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

a) proteger o valor e a reputação da instituição;
b) garantir a confidencialidade, integridade e disponibilidade das informações, 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, dentre outros;
d) implementar controles voltados a rastreabilidade da informação, de modo a garantir a segurança das informações sensíveis;
e) garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
f) atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

g) conscientizar, educar e treinar os colaboradores sobre a temática de segurança da informação e risco cibernético, normas e procedimentos internos aplicáveis às suas atividades diárias;
h) estabelecer e melhorar continuamente o processo de gestão de riscos de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: controle de acesso, autenticidades e riscos cibernéticos. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas.

Confidencialidade: proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntária ou involuntariamente dados restritos que deveriam ser acessíveis apenas por um determinado grupo de usuários.

A principal forma de manter a confidencialidade é por meio da autenticação, controle e restrição de acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem.

Sem a confidencialidade, as empresas ficam vulneráveis a ciberataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros.

Integridade: garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança

acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

Disponibilidade: prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

Acesso controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

Autenticidade: Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação.

Todos esses métodos são importantes para garantir a segurança das informações corporativas das possíveis ameaças, que podem ter origens tanto externas quanto internas. Elas podem ser uma pessoa, um evento ou uma ideia capaz de causar danos ao sistema.

As ameaças externas são tentativas de ataque ou desvio de informações vindas de fora da empresa, normalmente originadas por pessoas com a intenção de prejudicar a corporação. As internas podem ser causadas por colaboradores de forma acidental ou intencional. Essas ameaças podem causar pequenos incidentes e até prejuízos graves, por isso também devem ser levados em conta na hora do planejamento dos processos de segurança da empresa.

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 empresa causando danos financeiros e de reputação consideráveis.

5. SEGURANÇA CIBERNÉTICA

Segurança Cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

As diretrizes de segurança voltadas a salvaguardar o conjunto tecnológico utilizado pela COOPERATA estão elencadas no item 7.

Destaca-se que no desenvolvimento desta política, a COOPERATA avaliou a estrutura de segurança da informação e os resultados obtidos estão evidenciados no checklist de Segurança da Informação e serão contemplados no relatório anual de Risco Cibernético.

6. DIRETRIZES DE SEGURANÇA

A COOPERATA implementa diretrizes de segurança abrangendo aspectos físicos e digitais relacionados à Dados e Informações, acessos, privacidade e proteção de dados, promoção de cultura de segurança e outros aspectos que permitem prevenir, detectar de forma tempestiva e responder a incidentes cibernéticos.

Dentre os controles adotados estão a restrição de acesso conforme perfil do colaborador e horário de expediente, criptografia de dados, prevenção de

vazamento de informações, rastreabilidade, segmentação de rede e realização periódica de testes de vulnerabilidade.

7. AVALIAÇÃO E CONTRATAÇÃO DE SERVIÇOS DE TI E DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a **COOPERATA** adotará procedimentos com objetivo de avaliar o prestador de serviço nos aspectos legais e técnicos necessários.

8. RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES

Sempre que a **COOPERATA**, identificar a necessidade de execução de testes de segurança, ela poderá contratar especialistas para atendimento de escopo especifico ou acionar o departamento de TI da Prodaf, que realizará testes nos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos colaboradores, individualização dos usuários, dentre outros.

Estes testes serão realizados anualmente pela equipe de suporte de TI contratada e a documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, estarão disponíveis na rede interna da **COOPERATA** como evidência em eventuais questionamentos internos ou de órgãos reguladores.

9. REGISTROS DE INCIDENTES RELEVANTES

Entende-se como incidente cibernético a ação/ocorrência inesperada que demonstre vulnerabilidade de infraestrutura de TI, como:

a) Malware – software malicioso com objetivo de causar danos ou prejuízo ao usuário, contemplando roubo de dados, interceptação de informações, danos ao sistema, corrupção dos dados entre outros;
b) Phishing – prática de envio de informações alteradas para obtenção de dados através de fraude;
c) Ataque de senha – quando um invasor tenta adivinhar ou quebrar a senha de um usuário.

Quando identificado a tentativa ou incidente cibernético, a gestão informará tempestivamente ao Diretor Administrativo, e a **COOPERATA** manterá registro, analisará a causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as suas atividades.

Se confirmado um incidente cibernético relevante, que gere exposição de dados pessoais protegidos pela Lei Geral de Proteção de Dados, a **COOPERATA** reportará aos órgãos previsto em legislação.

10. PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Quando identificados incidentes cibernéticos, a cooperativa elaborará plano de ação e de resposta a incidentes visando a correção e mitigação dos riscos identificados.

Será elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, que deverá abordar, no mínimo:

I. a efetividade da implementação das ações a serem desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II. o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

III. os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

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

O relatório será apresentado à Diretoria até 31 de março do ano seguinte ao da data-base.

11. CONTINUIDADE DOS NEGÓCIOS

O processo de gestão de continuidade de negócios relativo a segurança da informação e risco cibernético, 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.

Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos. Os procedimentos adotados para gerenciamento de riscos estão previstos na política de continuidade de negócios.