Tipo do Documento: Política
Versão: 00
Classificação: Pública
Ata 1º
Data: 28.05.2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

PÚBLICO-ALVO

Todos aqueles que interagem com a informação da COOPGO, seja internamente ou externamente. Isso engloba todos os colaboradores, prestadores de serviço, clientes, parceiros, acionistas e até visitantes que possam ter acesso aos sistemas e dados da empresa.

INTRODUÇÃO

A informação é o principal ativo da COOPGO. Assim, ficou definida a estratégia de segurança da Informação para proteção da integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta a incidentes e busca fortalecer a gestão do risco de segurança cibernética e a construção de uma base sólida para o melhor ambiente digital.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Na COOPGO, temos o compromisso com o tratamento adequado das informações dos nossos clientes e público em geral, sendo fundamentado nos seguintes princípios:

• Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

• Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

• Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos

DIRETRIZES

Todos os documentos de segurança da informação (política, regras e procedimentos) devem estar disponíveis em local acessível aos colaboradores e protegidos contra alterações.

A Política Corporativa de Segurança da Informação é revisada anualmente pela COOPGO com aplicação para todos colaboradores e protegidos contra alterações.

A inclusão de diretrizes ou eventuais alterações serão identificadas e realizadas pelo responsável pela segurança da informação da COOPGO, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pela Diretoria de Segurança Corporativa da COOPGO..

A adesão a essa Política e eventuais falhas são reportados periodicamente pela Diretoria de Segurança Corporativa aos comitê gestor da COOPGO.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente, conforme descrito em políticas internas.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

As violações a esta política estão sujeitas às sanções disciplinares previstas em documento interno, bem como nas normas internas da COOPGO.

a) Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos

(p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos tecnológicos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação, autorização e monitoramento).

Os ativos da COOPGO, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade, conforme descrito nos documentos internos.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos da COOPGO

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

As revisões de acesso devem ser realizadas de forma contínua, a fim de garantir a inativação de usuários indevidos, a revisão das permissões concedidas e a existência de perfis de acesso com privilégio maior do que o necessário para execução das atividades. No mínimo anualmente, deve ser realizada a revisão integral dos acessos concedidos.

d) Segurança Física do Ambiente

Visamos prevenir acessos não autorizados a equipamentos, instalações, materiais ou documentos.

O processo de Segurança Física da COOPGO estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes, conforme descrito nos documentos internos.

Para evitar o acesso de pessoas não autorizadas a áreas em que se encontram dados e informações críticas da empresa é implantado recursos de identificação de funcionários, como o uso de crachás, senhas e cadastro de digitais.

É controlado a entrada e saída de equipamentos, materiais e pessoas da empresa por meio de registros de data, horário e responsável.

e) Conscientização em Segurança da Informação

A COOPGO promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação,fazendo parte do Programa de Integridade e Ética, conforme descrito em documento interno.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, em mídias ou redes sociais aos colaboradores e clientes.

f) Identificação

Para acessar os sistemas corporativos disponibilizados pela COOPGO, o usuário deverá estar identificado, autenticado e autorizado. Suas ações poderão ser auditadas a qualquer tempo. Os acessos serão concedidos à medida que solicitados e autorizados pela área responsável.

Identificamos, por meio do controle de acesso, cada usuário individualmente e nos casos devidamente comprovados de tratamento indevido da informação corporativa o responsabilizamos. O administrador que lhe concedeu o acesso também poderá ser

responsabilizado caso tenha realizado a concessão de acesso de forma indevida ou que extrapole os limites da sua atuação.

Não é concedido acesso a usuários e entidades externas às redes da COOPGO sem autorização formal do gestor responsável pela área de segurança do COOPGO.

g) Uso de dispositivos

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos/dispositivos particulares não gerenciados ou não homologados pela COOPGO.

.É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (modem 3G/4G, HD externo, pendrive etc.) em equipamentos pertencentes às entidades COOPGO ou de terceiros, salvo os autorizados pela área responsável pela segurança da entidade.

h) Correio eletrônico

Os recursos de correio eletrônico corporativo são monitorados e serão utilizados para suporte das atividades desenvolvidas na COOPGO e seguem as regras de classificação da informação.

i) Senhas

As senhas de acesso são individuais, intransferíveis, de responsabilidade única e exclusiva do usuário e não podem ser compartilhadas ou divulgadas. As senhas respeitarão regras de complexidade mínima definidas.

j) Software

Todos os softwares utilizados deverão ser licenciados. Não devem ser instalados, conectados e utilizados softwares não autorizados pela COOPGO, independentemente da natureza de uso ou aplicação. Deve-se respeitar o direito à propriedade intelectual, na forma da legislação em vigor, não reproduzindo ou divulgando material sem a autorização do autor

SEGURANÇA CORPORATIVA

• Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;

• Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;

• Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do Sistema de Gestão Integrado (SGI).

• Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê Executivo de Segurança da Informação.

• Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.

• Estabelecer e disseminar uma cultura de segurança da informação.

• Propor o investimento para a segurança da informação para atender aos objetivos desta política.

• Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.

• Definir padrões mínimos de segurança para as filiais mantidas ou geridas pelo Matriz COOPGO garantindo alinhamento com os objetivos de segurança da informação definidos.

PAPÉIS E RESPONSABILIDADES

Colaborador:

Cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pela COOPGO. Os empregados das entidades da COOPGO assinam termo de responsabilidade e de confidencialidade relativos aos ativos de informação a que tiver acesso, o qual fica arquivado nas respectivas pastas funcionais.

Tecnologia da Informação:

Propor soluções, metodologias e processos específicos de segurança da informação e segurança cibernética; Manter o patrimônio tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

Área de Negócio:

Proteger as informações da COOPGO sob sua responsabilidade.

Gerência de tecnologia:

Segregar as funções administrativas e operacionais;

Monitorar e auditar o ambiente tecnológico, através da implantação de sistemas de monitoramento de servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede;

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança da informação estabelecidos nesta política;

Coordenar o tratamento de incidentes de Segurança da Informação e cibernética;

Auxiliar o Encarregado pela Proteção de Dados nas investigações e avaliações dos danos decorrentes da quebra de segurança que envolvam dados pessoais;

Tratar de questões, propor soluções, metodologias e processos específicos de segurança da informação. Neste contexto, é a área responsável por analisar criticamente a Política de Segurança da Informação e Cibernética.

Gerência demais áreas :

Zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política. Cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso.

DECLARAÇÃO DE RESPONSABILIDADE

Periodicamente os colaboradores da COOPGO devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com a COOPGO devem possuir cláusula que assegure a confidencialidade das informações e a obrigatoriedade de seguir as regulamentações vigentes, referentes ao tema de segurança da informação.

SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas em documento interno, bem como nas normas internas da COOPGO.

REGULAMENTAÇÕES

- A ANPD, por meio da Resolução CD/ANPD n.º 20/2024;
- A regulamentação da classificação da informação, no contexto da Lei de Acesso à Informação (LAI), é feita pelo Decreto nº 7.724, de 2012. Este decreto, que detalha a Lei nº 12.527, de 2011;
- Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018
- ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes;
- Resolução 4.893 do Banco Central;
- Resolução nº 85 do Banco Central;
- Resolução 4.752 do Banco Central.