PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Cássio Venuto Monteiro
Júlia Persson Mascari
Luís Fernando Moura Santos
Paola Marques Braga
Pedro Augusto Teixeira Silva
Vinicius Henrique de Oliveira Neves

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Cooperativa Bancária

EIXO 5 – ETAPA 4
2025

SUMÁRIO

1. Introdução

A segurança da informação representa um valor essencial para a Cooperativa Bancária. Como organização financeira que lida diariamente com dados pessoais, documentos internos, informações sigilosas e processos críticos, a cooperativa entende que a proteção das informações deve estar alinhada aos objetivos estratégicos, às exigências legais e às expectativas da direção.

A presente Política de Segurança da Informação expressa formalmente o entendimento da cooperativa sobre como a informação deve ser protegida e utilizada, definindo diretrizes e normas que orientam o comportamento dos colaboradores. Seu propósito é promover cultura organizacional, orientar boas práticas e estabelecer limites claros para o uso seguro da informação.

1.1. Objetivo

O objetivo desta política é estabelecer regras e responsabilidades para o adequado manuseio, armazenamento, compartilhamento, transporte e descarte de informações, garantindo sua proteção em conformidade com as necessidades do negócio, com a LGPD (Lei Geral de Proteção de Dados) e com as boas práticas recomendadas pela ISO/IEC 27002.

Busca-se assegurar que todos compreendam a importância da segurança da informação, que saibam como aplicá-la no cotidiano e que conheçam as orientações oficiais da direção.

1.2. Escopo

Esta política se aplica a todos os colaboradores, estagiários, fornecedores, parceiros e prestadores de serviços terceirizados que tenham acesso a informações, sistemas ou dependências da cooperativa.
Inclui:

- dados pessoais de colaboradores, cooperados e terceiros;
- sistemas bancários internos e plataformas online;
- dispositivos corporativos e redes de comunicação;
- documentos físicos e digitais;
- recursos de TI locais e em nuvem;
- e qualquer ambiente físico contendo ativos de informação.

O cumprimento desta política é obrigatório e sua violação pode resultar em medidas disciplinares, administrativas, civis e/ou criminais.

2. Princípios de Segurança

A política baseia sua atuação em três princípios fundamentais que orientam todas as atividades relacionadas à segurança da informação.

2.1. Confidencialidade

A confidencialidade exige que informações sejam acessadas apenas por indivíduos autorizados. Isso significa que credenciais são pessoais e intransferíveis, permissões são atribuídas conforme função.
Colaboradores devem manter sigilo sobre dados pessoais, documentos internos e processos organizacionais. Informações sensíveis não devem ser compartilhadas em redes sociais, conversas informais ou canais não autorizados.

2.2. Integridade

A integridade garante que informações e sistemas permaneçam corretos, completos e livres de alterações não autorizadas. Para assegurar isso, a cooperativa faz uso de registros de auditoria,

backups periódicos, permissões baseadas em papéis e isolamento do banco de dados em rede privada. Alterações relevantes devem ser documentadas e revisadas pela equipe de TI.

As informações devem permanecer corretas, completas e atualizadas.

É proibido a alteração de registros de forma indevida, omitir dados, apagar informações sem autorização ou manipular conteúdos oficiais.

2.3. Disponibilidade

As informações e sistemas devem estar acessíveis quando necessário para o trabalho. Os colaboradores devem utilizar os recursos de forma responsável, evitando práticas que prejudiquem a continuidade das operações.

3. Gerenciamento de Acesso

O gerenciamento de acesso estabelece os controles necessários para garantir que cada colaborador acesse apenas as informações essenciais ao desempenho de suas atividades. Seu objetivo é reduzir riscos relacionados a acessos indevidos, vazamento de dados, uso não autorizado de credenciais e abusos de privilégios. Essa seção define os mecanismos de autenticação, autorização e controle de permissões de usuários, assegurando que o tratamento das informações ocorra de maneira segura, rastreável e alinhada às responsabilidades de cada função.

3.1. Controle de Acesso

A cooperativa concede acessos conforme necessidade do cargo e atividade realizada. Somente profissionais autorizados podem acessar informações ou áreas restritas.

É proibido utilizar acessos ou documentos de terceiros.

3.2. Autenticação

Todos os usuários devem possuir credenciais únicas. É proibido que setores internos definam ou conheçam a senha do usuário. Todos os colaboradores devem criar suas próprias senhas e alterá-las periodicamente. A equipe de TI não solicita senhas e não mantém registro delas. A equipe administrativa utiliza autenticação reforçada, garantindo maior controle sobre recursos críticos.

3.3. Autorização

A autorização é definida de acordo com as tarefas atribuídas ao colaborador. Quando há mudança de função, licença, afastamento ou desligamento, a equipe de TI deve ajustar ou revogar acessos imediatamente. Revisões periódicas são realizadas para identificar permissões obsoletas ou inadequadas.

Todos os acessos são concedidos segundo o princípio do privilégio mínimo (least privilege) e da necessidade de saber (need to know). Segue-se também o princípio da segregação de funções para prevenir abuso de privilégios, fraudes e conflitos de interesse.

A cooperativa mantém registro formal das solicitações de acesso, alterações e revogações, possibilitando rastreabilidade e auditoria.

4. Segurança Física e Ambiental

A segurança física e ambiental tem como finalidade proteger instalações, equipamentos e documentos contra danos, acesso não autorizado, perdas ou interrupções. Essa seção aborda controles destinados a prevenir ameaças físicas, como furto, vandalismo, desastres naturais, incêndio e falhas elétricas. Ela define como ambientes protegidos devem funcionar, quem pode acessá-los e quais medidas devem ser adotadas para manter continuamente a integridade dos ativos físicos e de infraestrutura da cooperativa.

4.1. Proteção de instalações
A matriz mantém sua sala de servidores permanentemente trancada, com acesso restrito à equipe técnica. As filiais devem assegurar que equipamentos essenciais, como roteadores e máquinas administrativas, estejam protegidos contra manipulação não autorizada. Informações impressas não devem ficar expostas.

4.2. Controle de acesso físico
Ambientes administrativos e salas com informações confidenciais exigem autorização. Visitantes devem ser acompanhados e não podem circular livremente pelas dependências.

Visitantes, prestadores de serviço e fornecedores devem assinar termo de confidencialidade e registro de entrada, sendo acompanhados o tempo todo em áreas sensíveis.

4.3. Segurança ambiental

Para evitar danos, os ambientes que abrigam equipamentos críticos contam com nobreaks, proteção contra sobretensão elétrica e medidas básicas contra incêndio. A continuidade operacional é reforçada pelo armazenamento seguro de backups em estruturas isoladas na nuvem.

A proteção física inclui cuidados com papel, equipamentos e documentos. Materiais sensíveis devem ser armazenados de forma segura para evitar perdas, danos ou exposição.
O descarte de documentos confidenciais deve ocorrer exclusivamente por fragmentação, incineração ou empresa especializada contratada.

5. Segurança de Redes e Comunicações
A segurança das redes e das comunicações visa garantir que os dados trafegados entre sistemas, dispositivos e unidades da cooperativa sejam protegidos contra interceptações, adulterações e interferências. Essa seção trata da proteção das redes internas e externas, do uso adequado dos meios de comunicação corporativos e do monitoramento preventivo para detectar ameaças e tentativas de intrusão. O propósito é assegurar que as comunicações permaneçam seguras, legítimas e alinhadas às necessidades operacionais da organização.

5.1. Proteção de redes
Colaboradores devem utilizar exclusivamente canais autorizados e redes seguras para desempenhar suas atividades profissionais. É proibido enviar documentos internos por e-mail pessoal, WhatsApp ou demais aplicativos não autorizados, bem como utilizar os canais corporativos (como e-mail institucional, sistemas internos e ferramentas de comunicação) para fins pessoais ou não relacionados ao trabalho.

5.2. Monitoramento e detecção de intrusões

O monitoramento é realizado de forma contínua, permitindo acompanhar o estado dos servidores locais e em nuvem. Alertas são gerados automaticamente em caso de falhas, consumo anormal, quedas de CPU, indisponibilidade ou tentativas suspeitas de acesso.

As redes da cooperativa são segmentadas por filial, garantindo maior controle sobre fluxos internos e minimizando impactos de falhas.

6. Gestão de Incidentes de Segurança

A gestão de incidentes de segurança estabelece os procedimentos para detecção, tratamento e prevenção de eventos que possam comprometer informações ou recursos tecnológicos. Sua finalidade é reduzir impactos operacionais, financeiros e regulatórios decorrentes de falhas ou ataques. Essa seção descreve as responsabilidades durante um incidente, o fluxo de comunicação, os registros obrigatórios e as estratégias de resposta — incluindo ações de contenção, recuperação, investigação e melhoria de controles.

6.1. Resposta a incidentes

A cooperativa mantém um procedimento estruturado para lidar com incidentes. Na ocorrência de eventos inesperados, como tentativa de invasão, falha no servidor, acesso indevido ou comportamento suspeito detectado pela equipe de TI são seguidas as etapas de identificação, contenção, erradicação e recuperação.

Em incidentes envolvendo dados pessoais, a cooperativa segue os requisitos da LGPD e, quando aplicável, notifica autoridades competentes e titulares afetados com transparência e rapidez. Simulações e testes de resposta a incidentes são realizados periodicamente para aprimorar o plano de resposta.

É expressamente proibido que colaboradores tentem resolver incidentes por conta própria. Qualquer situação que represente risco à segurança da informação deve ser imediatamente reportada ao setor responsável, para que a tratativa ocorra de forma adequada, segura e registrada.

Após a resolução, todos os incidentes são documentados para apoiar a melhoria contínua dos controles existentes.

6.2. Relatórios de incidentes

Todos os colaboradores são responsáveis por comunicar imediatamente qualquer situação anômala, fornecendo as informações necessárias para o registro adequado do incidente, tais como: identificação do usuário, descrição do ocorrido, data e horário do fato e sistemas envolvidos. Os incidentes são devidamente registrados e analisados posteriormente, com o objetivo de apoiar a tomada de decisões, aprimorar controles internos e prevenir reincidências.

7. Conscientização e Treinamento em Segurança

A conscientização e o treinamento em segurança têm como propósito promover uma cultura organizacional orientada à proteção da informação. Essa seção define os programas educativos e capacitações periódicas necessárias para que colaboradores, fornecedores e parceiros compreendam seus papéis na segurança, adotem boas práticas e estejam preparados para reconhecer e evitar riscos. A disseminação do conhecimento é essencial para reduzir vulnerabilidades humanas e fortalecer a resiliência institucional.

7.1. Programa de conscientização

A cooperativa mantém ações de sensibilização voltadas para uso seguro da informação. Comunicados internos e campanhas periódicas são utilizados para manter os colaboradores atualizados, todos devem participar e reconhecer seu papel ativo na proteção dos dados.

7.2. Treinamento em segurança

Novos colaboradores recebem treinamento inicial sobre normas e práticas de segurança da informação, garantindo que compreendam desde o primeiro dia suas responsabilidades no tratamento de dados e no uso adequado dos recursos corporativos.

Além disso, a cooperativa oferece treinamentos periódicos sobre uso seguro dos sistemas, proteção de dados pessoais, prevenção a incidentes e boas práticas de segurança. A participação em todas as capacitações é obrigatória, reforçando a cultura de segurança e a contínua atualização dos colaboradores.

Todos os colaboradores devem assinar termo de ciência da PSI anualmente. Fornecedores que tratem dados pessoais ou informações confidenciais são obrigados contratualmente a participar de programas de segurança.

8. Avaliação e Melhoria Contínua

A segurança da informação exige adaptação constante diante de novas ameaças, tecnologias e requisitos legais. Essa seção estabelece os mecanismos de avaliação contínua do desempenho dos controles de segurança, incluindo auditorias, análise de riscos, revisão de políticas e medição de resultados. Seu objetivo é garantir que a cooperativa evolua continuamente, corrigindo fragilidades, aprimorando processos e assegurando sua conformidade operacional e legal.

8.1. Auditorias de segurança

Processos, registros e comportamentos organizacionais são avaliados regularmente por meio de auditorias internas e externas. O objetivo é verificar a conformidade com esta política, identificar fragilidades, analisar desvios e propor ações corretivas. As auditorias podem incluir revisão de documentos, entrevistas, verificação de processos, testes de segurança e validação do cumprimento das diretrizes estabelecidas.

8.2. Revisão de políticas e procedimentos

A Política de Segurança da Informação é revisada anualmente, ou sempre que ocorrerem mudanças significativas no ambiente tecnológico, na legislação vigente ou após incidentes relevantes. A revisão garante que a PSI permaneça atual, eficaz e alinhada às necessidades da cooperativa e às exigências legais. Sempre que atualizada, deve ser divulgada aos colaboradores e disponibilizada em meio oficial.

8.3. Análise de riscos

A cooperativa realiza análises periódicas de riscos considerando aspectos organizacionais, humanos, tecnológicos e físicos. Esse processo permite identificar ameaças e vulnerabilidades, avaliar os impactos potenciais, definir prioridades de tratamento e implementar controles mitigatórios que reduzam a probabilidade de incidentes. A análise de riscos orienta decisões estratégicas e contribui para o aprimoramento contínuo da segurança da informação.

8.4. Medição de desempenho

Para assegurar a proteção das informações, a cooperativa executa um processo contínuo de gerenciamento de vulnerabilidades e atualizações. Esse processo inclui identificar fragilidades, aplicar correções e aprimorar constantemente os controles internos, além de realizar testes periódicos que verifiquem a eficácia das correções implementadas. Todas essas ações são conduzidas observando boas práticas no tratamento de dados pessoais, garantindo que informações corporativas permaneçam protegidas ao longo de todo o seu ciclo.

9. Conformidade Legal e Regulatória

A conformidade legal e regulatória assegura que todos os processamentos de dados, controles de segurança e práticas organizacionais estejam alinhados às legislações em vigor e às normas do setor financeiro. Essa seção reforça a obrigatoriedade do cumprimento da LGPD, do Banco Central e de demais regulamentações aplicáveis, além de formalizar o compromisso da cooperativa com boas práticas reconhecidas nacional e internacionalmente. Trata também da necessidade de acompanhar mudanças legais e ajustar processos sempre que necessário.

9.1. Conformidade com leis e regulamentações

A cooperativa cumpre a Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais e estabelece direitos aos titulares, seguindo também as normas do Banco Central e demais legislações financeiras aplicáveis. Além disso, adota práticas alinhadas à ISO/IEC 27002, que reúne boas práticas internacionais de segurança da informação, especialmente no controle de acesso, proteção de dados e prevenção de incidentes.

Além da legislação nacional, esta PSI considera normativos do Banco Central, do Conselho Monetário Nacional e referências internacionais amplamente adotadas por instituições financeiras.

9.2. Gerenciamento de vulnerabilidades e patches

Para manter a segurança das informações, é adotado um processo contínuo de gerenciamento de vulnerabilidades e atualizações. Esse processo abrange a identificação de fragilidades, a aplicação de correções, o ajuste de configurações inseguras e a melhoria constante dos controles internos, além do acompanhamento de boas práticas relacionadas ao tratamento de dados pessoais. Tais medidas asseguram que as informações corporativas e os dados pessoais permaneçam protegidos ao longo de todo o seu ciclo de vida.

10. Responsabilidades

A segurança da informação é responsabilidade de toda a organização e requer participação ativa de todos os envolvidos. Esta seção define claramente os papéis da direção, da equipe de segurança da informação, das lideranças e dos colaboradores, assegurando que todos compreendam suas atribuições formais no tratamento dos dados e na proteção dos ativos. O detalhamento das responsabilidades garante alinhamento, transparência e responsabilização em relação às práticas de segurança.

10.1. Direção

A direção possui responsabilidade central na promoção da segurança da informação. Cabe a ela aprovar esta política, garantir os recursos necessários para sua implementação e incentivar uma cultura organizacional voltada à proteção dos dados. Também deve acompanhar relatórios e auditorias para assegurar que a segurança esteja alinhada aos objetivos estratégicos da cooperativa.

10.2. Equipe de segurança da informação

A equipe de Segurança da Informação e TI é responsável por aplicar e manter os controles previstos nesta política, orientar os colaboradores sobre boas práticas, monitorar sistemas, responder a incidentes e registrar ocorrências. Também deve garantir que os acessos sejam concedidos, revisados e revogados corretamente, além de assegurar que o tratamento de dados pessoais esteja em conformidade com a LGPD.

10.3. Funcionários

Todos os colaboradores devem cumprir esta política, proteger as informações sob sua responsabilidade e utilizar corretamente os sistemas e equipamentos da cooperativa. É obrigatório comunicar qualquer incidente ou suspeita, bem como respeitar as regras de confidencialidade, privacidade e uso ético dos recursos. Em caso de dúvidas sobre procedimentos, responsabilidades ou práticas de segurança, o colaborador deve buscar orientação da direção, das lideranças ou da equipe de TI. O descumprimento dessas responsabilidades pode gerar medidas disciplinares.

Todos os colaboradores, independentemente do cargo, são corresponsáveis pela proteção das informações e devem agir imediatamente ao identificar riscos, comportamentos suspeitos ou violações.