POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Sumário

CREDCOL
COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO
DOS EMPREGADOS DO GRUPO colorado

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A presente Política de Segurança da Informação tem como objetivo definir as diretrizes da Cooperativa de Economia e Crédito Mútuo dos Empregados do Grupo Colorado que nortearão as normas e padrões que tratam a proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que ela esteja contida.

2. APLICABILIDADES

Aplica-se a Diretoria Executiva, empregados, estagiários, que utilizam as informações constantes nos ativos da Cooperativa.

3. CONCEITOS

Para esta política são definidos:

a) ativo: algo que tenha valor para a Cooperativa;

b) segurança da informação: refere-se à proteção do conjunto de informações, no sentido de preservar o valor que possuem para a Cooperativa;

c) backup: é uma cópia de segurança dos seus dados (física ou em nuvem) de um dispositivo de armazenamento ou sistema;

d) firewall: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

e) incidente: são eventos que trazem prejuízos à Cooperativa.

4. RESPONSABILIDADES

Na Cooperativa é imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

É de responsabilidade da ***Diretoria Executiva***, conselho fiscal, empregados, estagiário, terceiros (fornecedores e prestadores de serviços) e visitante, observarem e seguirem as diretrizes, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação.

Todas as atividades executadas na Cooperativa devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

As diretrizes estabelecidas nesta política são extensíveis aos terceiros (fornecedores e prestadores de serviços) da Cooperativa.

A estrutura da Cooperativa atua nos processos de gerenciamento de segurança da informação com a estrutura descritas nos próximos itens.

4.1. DIRETORIA EXECUTIVA

São responsabilidades da Diretoria Executiva:

a) aprovar as diretrizes desta Política de Segurança da Informação (PSI);

b) aprovar as exceções que não conflitem com as normas legais;

c) avaliar e aprovar o plano de continuidade de negócios;

d) aprovar as requisições de aquisições de software e hardware;

e) estabelecer diretrizes para a gestão da segurança da informação;

f) aprovar o orçamento em atendimento aos projetos referente a segurança da informação.

4.2. GERÊNCIA

São responsabilidades Gerência:

a) aprovar em conjunto com a Diretoria Executiva as requisições de aquisições de software e hardware;

b) tomar conhecimento e apresentar a Diretoria Executiva os incidentes de segurança da informação e das ações adotadas para resolução dos problemas;

c) aprovar em conjunto com a Diretoria Executiva o registro de ocorrências referente a segurança da informação, do tratamento e documentação dos problemas ocorridos e ações realizadas;

d) estabelecer o orçamento em atendimento aos projetos referente a segurança da informação;

e) monitorar os serviços da empresa contratada, abrangendo custos, prazos e qualidade dos produtos entregues referentes a segurança da informação.

4.3. INFORMÁTICA

São responsabilidades da Informática:

a) garantir a integridade da rede da Cooperativa através do uso de firewalls e programas antivírus;

b) instalar e monitorar o Firewall e VPN;

c) garantir segurança nos e-mails e implantar antivírus;

d) monitorar o servidor de serviços de rede;

e) instalar e desinstalar qualquer software considerado nocivo à integridade da rede por meio de chamado técnico;

f) orientar os empregados sobre os princípios e procedimentos de segurança da informação, para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas;

g) atender as demandas dos usurários da Cooperativas com relação dúvidas e ocorrências de segurança da informação.

4.4. TODOS OS USUÁRIOS

Os critérios a seguir deverão ser cumpridos rigorosamente por todos os usuários:

a) responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;

b) relatar prontamente a Gerência qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas e diretórios de rede, acesso indevido à *internet*;

c) relatar prontamente, quando identificado, quaisquer programas instalados sem conhecimento*;*

d) assegurar que as informações e dados de propriedade da Cooperativa não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos ou em áreas expostas como transporte público, restaurantes, encontros sociais etc.

5. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios da Cooperativa, refere-se a um ativo com constantes ameaças e quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos a Cooperativa**.**

Assim, a Política de Segurança da Informação torna-se alicerce dos esforços de proteção à informação da Cooperativa.

A segurança da informação é aqui caracterizada pela preservação da confidencialidade, integridade, disponibilidade.

Assim, a segurança da informação são esforços contínuos para a proteção dos ativos de informação e para tanto, visa atingir os seguintes objetivos:

a) confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

b) integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas acidentais ou propositais;

c) disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

5.1. PROTEÇÃO DA INFORMAÇÃO

A informação é um importante ativo para a operação das atividades comerciais da Cooperativa e deve ser adequadamente manuseada e protegida e pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e meio da comunicação oral.

Toda a informação gerada ou desenvolvida nas dependências da Cooperativa constitui ativo essencial à condução de negócios, e em última análise, à sua existência e deve ser utilizada unicamente para a finalidade para a qual foi autorizada, independente da forma ou por meio pelo qual é compartilhada.

É imprescindível estabelecer como diretriz fundamental a proteção de todas as informações pertencentes à Cooperativa, a fim de mitigar riscos e ameaças que possam comprometer a confidencialidade, integridade e disponibilidade desses dados.

5.2. CORREIO ELETRÕNICO

Com objetivo de garantir a integridade dos sistemas de informação a área de Informática poderá monitorar, investigar, ler ou verificar toda a atividade dos empregados e prestadores de serviços, abrangendo:

a) sem limites as informações;

b) dados;

c) conteúdo e mensagens ou arquivos enviados, recebidos ou armazenados;

d) acesso e as atividades aos sites da internet visitados.

5.3. ACESSO A INTERNET

O acesso à internet deve ser utilizado para fins corporativos visando buscar informações que possam contribuir para o desenvolvimento das atividades relacionadas a Cooperativa.

A área de Informática poderá monitorar ou bloquear o acesso à internet em caso de risco ao funcionamento do ambiente.

São permitidas o acesso à *internet* para fins pessoais (home *banking,* lojas virtuais, redes sociais e afins) desde que o empregado tenha bom senso e respeitando os direcionamentos de segurança estabelecidos.

O acesso externo à rede interna, para fins de manutenção de infraestrutura ou sistemas somente poderão ser realizados pela área de Informática.

.

5.4. CONTROLE DE ACESSO

A Cooperativa deverá manter restrito, o acesso as áreas onde serão processadas ou armazenadas informações pertinentes à operação da Cooperativa, mantendo lista de acesso a estes ambientes.

O empregado / usuário é responsável por todos os atos executados com suas credenciais de acesso, portanto deverá:

a) manter a confidencialidade, registrando as senhas em ambientes seguros;

b) alterar a senha sempre que existir qualquer suspeita de comprometimento de sua confidencialidade;

c) selecionar senhas de qualidades, cuidando para não usar datas de aniversários, entre outros;

d) evitar o uso dos equipamentos por outros empregados enquanto este estiver conectado com suas credenciais;

e) bloquear o equipamento ao se ausentar da estação de trabalho;

f) é proibido compartilhar a senha e o uso de logins automáticos e recursos de memorização de senhas são proibidos.

5.5. AUTENTICAÇÃO E SENHAS

Na Cooperativa é realizada a autenticação de senhas que visa a evitar o acesso não autorizado a dados pessoais.

As pessoas não autorizadas são aquelas que não detêm legitimidade legal, regulamentar ou estatutária para o tratamento de dados. Assim, autenticação nos sistemas é realizada através de senha pessoal e intransferível, ou seja, de responsabilidade exclusiva do empregado / usuário.

O padrão de senha deve ser complexo, contendo:

a) tamanho mínimo de 6 caracteres;

b) proibição de reuso das últimas 6 (seis) senhas utilizadas na alteração;

c) exigência de complexidade alta (maiúscula, minúscula, caracteres especiais e números. Ex: 1234@Mudar);

d) expiração de senha a cada 90 dias;

e) bloqueio de senha após 6 (sies) tentativas erradas;

f) desbloqueio de senha somente por acesso administrativo;

g) armazenamento em banco de forma criptografada.

A senha deverá ser trocada, através de solicitação periódica, seguindo o padrão descrito no item anterior e ser alterada pelo empregado / usuário sempre que existir suspeita de comprometimento de sua confidencialidade.

O empregado / usuário deverá:

a) evitar o uso de seu equipamento por outros empregados / usuários enquanto estiver conectado com suas credenciais;
b) bloquear sempre o equipamento ao se ausentar da estação (Ctrl+Alt+Del).

O empregado / usuário não poderá transferir ou compartilhar senha com ninguém, ou seja, terminantemente proibido o compartilhamento de login.

Também não é permitido habilitar logins automáticos com recurso de memorização de senha.

5.5.1. ACESSO A TERCEIROS (FORNECEDORES E PRESTADORES DE SERVIÇOS)

Os terceiros (fornecedores e prestadores de serviços), visitantes devem ter seus “Logins” diferentes dos empregados da Cooperativa.

5.6. FLUXO DE CRIAÇÃO E BLOQUEIO DE ACESSOS

A área de Informática estabeleceu um fluxo de criação e bloqueio através que abrange as seguintes etapas:

a) admissão e demissão de empregados;

b) terceiros (fornecedores e prestadores de serviços) e visitantes;

c) ativação ou bloqueio do login do empregado para acesso a rede, e-mail, outros;

d) definição de acessos e permissão do empregado pelo gestor.

5.7. BACKUP

A Cooperativa utiliza sistemas de gestão de atendimento, contábil e de riscos contratados junto à empresa **Fácil Cred**, que é a responsável pela realização e armazenamento dos backups das informações da Cooperativa em data center próprio.

Diretrizes:

- A Fácil Cred deve executar rotinas periódicas de backup, assegurando a integridade, confidencialidade e disponibilidade dos dados.
- Os backups devem ser armazenados em ambiente seguro, com recursos de redundância, controle de acesso e proteção contra incidentes físicos ou lógicos.
- Cabe à Cooperativa acompanhar, por meio de relatórios e evidências fornecidos pela Fácil Cred, a execução e a eficácia dos procedimentos de backup.
- Testes de restauração devem ser realizados periodicamente pela Fácil Cred, garantindo a confiabilidade dos processos.
- A Cooperativa manterá a responsabilidade de monitorar a conformidade contratual e assegurar que os padrões de backup atendam às exigências legais e regulatórias aplicáveis.

5.8. SOFTWARES

Na Cooperativa somente são permitidas as instalações de softwares homologados.

A cooperativa deverá possui um inventário em todas as estações de trabalho e caso seja identificados softwares não homologados, poderá ser desinstalado sem aviso prévio ao empregado e comunicado ao responsável da área.

5.9. ANTIVIRUS

Todos os equipamentos da Cooperativa possuem antivírus instalados.

5.10. CLASSIFICAÇÃO DE DADOS

Os dados poderão ser classificados em:

a) público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;

b) somente interno: conteúdo produzido pela Cooperativa para conhecimentos exclusivos dos empregados, terceiros (fornecedores e prestadores de serviços);

c) confidencial: conteúdo sensível e de acesso apenas a pessoas que devem conhecer o conteúdo.

O acesso aos dados somente será autorizado aos empregados / usuários que tiver necessidade de conhecer a respectiva informação.

5.11. CRIPTOGRAFIAS E CERTIFICADOS DIGITAIS

A guarda das chaves de criptografia para acessos aos recursos computacionais devem ser mantidas de forma segura, bem como o registro de todas as chaves de criptografia e certificados digitais existentes.

Devem ter controles e documentar o processo de guarda, renovação, revogação e inutilização de certificados digitais.

5.12. TESTES DE INVASÃO

A área responsável pela Segurança da Informação da Cooperativa, em conjunto com a **Fácil Cred** (fornecedora dos sistemas de gestão), assegura a execução periódica de rotinas de testes de defesa contra possíveis ataques aos sistemas de informação.

Diretrizes:

- A Fácil Cred realiza monitoramento contínuo, aplicação de atualizações de segurança e testes de vulnerabilidade em seus sistemas e data centers.
- Sempre que solicitado, a Fácil Cred deve fornecer relatórios ou evidências dos testes realizados, garantindo transparência no processo.
- Cabe à área de Segurança da Informação da Cooperativa acompanhar, fiscalizar e validar a execução desses testes, assegurando que os procedimentos estejam alinhados às boas práticas de segurança da informação e à legislação vigente.
- Eventuais falhas ou vulnerabilidades identificadas devem ser registradas, tratadas e monitoradas até sua resolução, em conjunto entre a Cooperativa e a Fácil Cred.

5.13. COMUNICAÇÃO

As informações sobre potenciais ameaças à integridade dos sistemas de informação são repassadas periodicamente a todos os empregados.

5.14. ARMAZENAMENTO E DESCARTE DE INFORMAÇÃO

Na Cooperativa tem as seguintes diretrizes com relação ao armazenamento e descarte de informações:

a) as informações confidenciais não devem ser deixadas à vista, seja em papel ou em quaisquer dispositivos eletrônicos;

b) ao usar uma impressora coletiva, recolher o documento impresso imediatamente;

c) os empregados ou terceiros (fornecedores e prestadores de serviços) não devem discutir ou comentar assuntos confidenciais em locais públicos.

5.15. EQUIPAMENTOS PARTICULARES/PRIVADOS

Os equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Cooperativa.

5.16. DIVULGAÇÃO

Para uniformidade da informação, esta Política de Segurança da Informação deve ser divulgada no âmbito da Cooperativa, tão logo aprovada pela ***Diretoria Executiva***, seja na sua constituição ou em quaisquer atualizações que se façam necessárias.

Adicionalmente, deve ser disponibilizada na Cooperativa, permitindo fácil acesso ou consulta a qualquer empregado / usuário.

Esta política também deve ser divulgada para novos empregados, no processo de integração.

Os empregados, ao receberem os equipamentos de trabalho (notebook), deverão assinar o termo de responsabilidade de uso de equipamentos de informática se responsabilizando pelo uso do hardware e software conforme esta Política de Segurança da Informação.

5.17. VIOLAÇÃO DA POLÍTICA E SANÇÕES

O descumprimento das diretrizes desta política, mesmo que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

É dever de todo empregado comunicar ao Gestor a ocorrência de incidente que afete a segurança da informação, que por sua vez escalará a ***Diretoria Executiva***, para análise quando assim for necessário.

6. ATENDIMENTO A LEI Nº 13.709/2018

Todos os procedimentos e diretrizes desta política são realizados em conformidade e observância a Lei nº 13.709/2018 (LGPD).

7. PERIODICIDADE DE REVISÃO

Para garantir a sua contínua pertinência, adequação e eficácia, essa política será revisada a cada 02 anos, em decorrência de alterações nos processos internos, alterações regulatórias ou ainda apontamentos de auditorias.

8. CONSIDERAÇÕES FINAIS

Os empregados / usuários estão proibidos de acessar informações da Cooperativa que não sejam explicitamente autorizados.

9. APROVAÇÃO

Este normativo foi aprovado na reunião da ***Diretoria Executiva)*** realizada em 22/08/2025 conforme Ata de Reunião nº 07/2025 e passa a vigorar na data de sua publicação.

10. REFERÊNCIAS NORMATIVAS

Normativo	Data	**Epígrafe**
Lei nº 13.709	14/08/2018	Lei Geral de Proteção de Dados Pessoais (LGPD).

11. CONTROLES DE ATUALIZAÇÕES

Edição	**Data**	**Instrumento de atualização**	**Atualizações**

Valter Marcos Lorenti – Diretor Presidente

Eli Norberto Ferreira – Diretor Tesoureiro

José Antônio Pimenta – Diretor Secretário

Página de assinaturas

Valter Lorenti
442.363.368-04
Signatário

eli ferreira
041.239.898-29
Signatário

HISTÓRICO

21 ago 2025 09:49:31 — **CREDCOL COOPERATIVA** criou este documento. (Empresa: CREDCOL, CNPJ: 02.024.442/0001-01, Email: credcolcolorado@gmail.com, CPF: 325.343.978-00)

21 ago 2025 10:10:55 — **Valter Marcos Lorenti** *(Email: valter.lorenti@colorado.com.br, CPF: 442.363.368-04)* visualizou este documento por meio do IP 177.200.72.34 localizado em Ribeirão Preto - São Paulo - Brazil

21 ago 2025 10:11:02 — **Valter Marcos Lorenti** *(Email: valter.lorenti@colorado.com.br, CPF: 442.363.368-04)* assinou este documento por meio do IP 177.200.72.34 localizado em Ribeirão Preto - São Paulo - Brazil

21 ago 2025 14:17:23 — **eli norberto ferreira** *(Email: eli.ferreira@colorado.com.br, CPF: 041.239.898-29)* visualizou este documento por meio do IP 177.21.47.210 localizado em Itajobi - São Paulo - Brazil

21 ago 2025 14:17:27 — **eli norberto ferreira** *(Email: eli.ferreira@colorado.com.br, CPF: 041.239.898-29)* assinou este documento por meio do IP 177.21.47.210 localizado em Itajobi - São Paulo - Brazil