POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO				
Área Emitente	**Número**	**Emissão**	**Versão**	**Atualização**
COMPLIANCE	1	08/2025	08/2025	07/2026

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

Na SAFEWAY GESTÃO DE RECURSOS FINANCEIROS LTDA, a informação é considerada um ativo estratégico essencial para a continuidade e credibilidade do negócio. A crescente dependência da tecnologia e o aumento das ameaças digitais tornam indispensável a adoção de medidas robustas de segurança.

Assim, esta Política de Segurança da Informação (PSI) estabelece as diretrizes para proteger a confidencialidade, integridade, disponibilidade e autenticidade das informações da empresa, de seus clientes e parceiros. Inspirada na norma ABNT NBR ISO/IEC 27002, em boas práticas internacionais e em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), esta PSI reforça o compromisso da SAFEWAY com a segurança e a ética no tratamento das informações, bem como com a proteção de dados de clientes parceiros e colaboradores.

2. Objetivo

O objetivo desta política é orientar colaboradores, prestadores e parceiros quanto às boas práticas no uso de sistemas, dispositivos e dados corporativos. Busca-se prevenir riscos, reduzir vulnerabilidades e garantir que as informações sejam utilizadas exclusivamente para fins profissionais e legítimos, preservando a reputação e a continuidade dos negócios da SAFEWAY.

3. Abrangência

Esta política aplica-se a todos os colaboradores, terceiros e prestadores que, de alguma forma, tenham acesso a informações, sistemas ou recursos tecnológicos da SAFEWAY. O uso inadequado ou não autorizado poderá gerar responsabilização administrativa, civil e criminal.

4. Princípios e Diretrizes Fundamentais

4.1. Princípios:

A PSI da SAFEWAY pauta-se nos seguintes princípios:

(i) **Propriedade da informação:** todos os dados e documentos produzidos ou recebidos em razão das atividades profissionais pertencem à empresa.

(ii) **Uso adequado:** recursos tecnológicos (computadores, e-mails, sistemas, dispositivos móveis) devem ser utilizados exclusivamente para finalidades relacionadas ao trabalho.

(iii) **Confidencialidade e sigilo:** qualquer informação estratégica ou pessoal deve ser protegida contra acessos não autorizados, inclusive após o desligamento do

colaborador.

(iv) **Responsabilidade individual:** cada usuário é responsável pelo uso ético e seguro de suas credenciais, equipamentos e acessos.

(v) **Conformidade legal:** todas as práticas de segurança da informação devem estar alinhadas à legislação vigente, especialmente a LGPD.

4.2. **Classificação da informação**:

As informações são categorizadas em níveis:

(a) Pública: pode ser divulgada livremente;

(b) Interna: uso exclusivo dos colaboradores;

(c) Confidencial: acesso restrito a áreas ou funções específicas; e

(d) Sigilosa: envolve dados pessoais sensíveis, informações estratégicas ou protegidas por lei.

Essa classificação orienta o tratamento e o nível de proteção exigido para cada tipo de dado.

4.3. Continuidade de negócios:

A SAFEWAY mantém planos de contingência, recuperação de desastres e testes periódicos para garantir a continuidade de suas operações em caso de incidentes críticos.

5. Responsabilidades

5.1. Colaboradores

Todos os colaboradores têm a obrigação de zelar pela proteção das informações às quais têm acesso. Devem manter senhas em sigilo, relatar incidentes de segurança imediatamente, respeitar o sigilo das informações e utilizar os ativos da empresa de forma ética e profissional.

5.2. Gestores

Os gestores devem assegurar que suas equipes cumpram esta política, autorizando e revisando acessos de acordo com a necessidade do cargo. São também responsáveis por orientar seus subordinados sobre práticas seguras, comunicar desligamentos à área de TI para bloqueio de acessos e apoiar programas de conscientização.

5.3. Área de TI e Segurança

Compete à área de TI implementar controles técnicos de proteção, como antivírus, firewall, backups, criptografia e monitoramento. É sua função administrar acessos, controlar o uso de dispositivos, garantir a rastreabilidade de logs e gerenciar o descarte seguro de mídias e informações.

6. Diretrizes Gerais

6.1. Senhas e Acessos

As credenciais de acesso são pessoais, intransferíveis e devem obedecer a requisitos mínimos de complexidade. Senhas devem ser trocadas periodicamente e nunca anotadas em locais de fácil acesso. A utilização de contas genéricas ou compartilhadas é proibida.

6.2. Uso de Recursos Tecnológicos

Os ativos tecnológicos disponibilizados pela SAFEWAY destinam-se exclusivamente a fins profissionais. É vedada a instalação de softwares não autorizados, bem como a utilização de e-mails corporativos para fins pessoais, spam ou correntes.

6.3. Armazenamento de Arquivos

Todos os documentos corporativos devem ser armazenados apenas em repositórios autorizados, como Google Drive corporativo ou sistemas internos. É proibido o uso de nuvens pessoais ou armazenamento local sem backup.

6.4. Dispositivos e Mídias

O uso de dispositivos móveis e mídias removíveis deve seguir critérios de segurança definidos pela empresa, como criptografia e autorização prévia. Em caso de perda, roubo ou mau funcionamento, o colaborador deve comunicar imediatamente a área responsável.

6.5. Home Office e Acesso Remoto

O acesso remoto só será permitido mediante VPN segura, dispositivos configurados pela TI e mecanismos de proteção como firewall, criptografia e antivírus atualizados.

6.6. Redes Sociais e Mensageiros

O uso de redes sociais, WhatsApp e e-mails pessoais é permitido apenas de forma moderada e desde que não comprometa as atividades da SAFEWAY, nem exponha informações confidenciais ou a imagem da empresa.

7. Proteção de Dados Pessoais

A SAFEWAY reafirma seu compromisso com a LGPD. Dados pessoais coletados e tratados pela empresa serão sempre utilizados para finalidades legítimas, informadas previamente ao titular, respeitando os princípios da necessidade, finalidade e transparência.

Os colaboradores devem coletar e manipular apenas os dados estritamente necessários, mantendo-os em segurança e respeitando os direitos dos titulares, conforme previsto na LGPD.

8. Conscientização

A cultura de segurança da informação deve ser parte do dia a dia de todos. A SAFEWAY promoverá treinamentos, campanhas de conscientização e comunicados periódicos, garantindo que colaboradores compreendam riscos, responsabilidades e boas práticas.

9. Disposições Finais

O respeito a esta política é indispensável para preservar a confiança dos clientes, parceiros e da sociedade. O descumprimento de suas diretrizes sujeitará o infrator a medidas disciplinares, incluindo advertência, suspensão, rescisão contratual por justa causa e, quando aplicável, responsabilização judicial.

Dúvidas, sugestões ou relatos de incidentes devem ser encaminhados ao Comitê de Segurança da Informação pelo e-mail: [compliance@safeway.com.br].

A Política será revisada anualmente, ou sempre que houver alteração relevante no ambiente regulatório, tecnológico, organizacional, operacional ou de risco.

Controle da Elaboração, Validação e Aprovação da Política

ELABORAÇÃO	VALIDAÇÃO	APROVAÇÃO
Millena Vilar	**Comitê de Compliance**	**Diretoria**