POLÍTICA CORPORATIVA Nº 11/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS (LGPD)

1. OBJETIVO

Estabelecer diretrizes, responsabilidades e controles para garantir a segurança das informações e a proteção dos dados pessoais tratados pela empresa, assegurando sua confidencialidade, integridade, disponibilidade e conformidade com a legislação aplicável, especialmente a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Esta Política visa prevenir acessos não autorizados, vazamentos, perdas, alterações indevidas e demais incidentes que possam comprometer informações corporativas, dados pessoais e a reputação da empresa.

2. ABRANGÊNCIA

Esta Política aplica-se a:

- Sócios e administradores;
- Diretores e gestores;
- Colaboradores próprios e terceirizados;
- Estagiários e aprendizes;
- Prestadores de serviços;

- Fornecedores que tenham acesso a informações da empresa;
- Parceiros comerciais;
- Usuários dos sistemas corporativos;
- Todos os ativos físicos e digitais relacionados à informação.

3. DEFINIÇÕES

Informação

Qualquer dado, documento, registro, comunicação ou conhecimento gerado, armazenado ou utilizado pela empresa.

Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável.

Dado Pessoal Sensível

Dado relacionado à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, dado genético ou biométrico.

Titular dos Dados

Pessoa natural a quem os dados pessoais se referem.

Tratamento de Dados

Toda operação realizada com dados pessoais, incluindo coleta, armazenamento, utilização, compartilhamento, alteração e eliminação.

Incidente de Segurança

Evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade das informações.

LGPD

Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Controlador

Pessoa física ou jurídica responsável pelas decisões referentes ao tratamento dos dados pessoais.

Operador

Pessoa física ou jurídica que realiza tratamento de dados em nome do controlador.

4. DIRETRIZES

4.1 Princípios Gerais

A gestão das informações e dos dados pessoais deverá observar os princípios de:

- Legalidade;
- Transparência;
- Necessidade;
- Finalidade;
- Segurança;
- Prevenção;
- Responsabilização;
- Integridade;
- Confidencialidade.

Toda informação corporativa deverá ser protegida de forma compatível com sua importância e sensibilidade.

4.2 Classificação das Informações

As informações poderão ser classificadas conforme seu grau de criticidade:

Pública

Informação destinada à divulgação sem restrições.

Uso Interno

Informação destinada exclusivamente às atividades internas da empresa.

Confidencial

Informação cujo acesso deve ser restrito a pessoas autorizadas.

Restrita

Informação crítica que exige controles especiais de acesso e proteção.

A classificação deverá orientar as medidas de segurança aplicáveis.

4.3 Controle de Acesso

O acesso às informações e sistemas corporativos deverá observar:

- Necessidade de acesso;
- Perfil de usuário compatível com a função;
- Utilização de credenciais individuais;
- Senhas seguras;
- Registro de acessos quando aplicável.

É proibido compartilhar senhas ou permitir utilização de credenciais por terceiros.

4.4 Uso de Recursos Tecnológicos

Os recursos tecnológicos da empresa deverão ser utilizados exclusivamente para fins profissionais legítimos.

É proibido:

- Instalar softwares não autorizados;
- Compartilhar informações confidenciais sem autorização;
- Utilizar sistemas para atividades ilícitas;
- Contornar mecanismos de segurança.

Todos os usuários deverão zelar pela proteção dos ativos tecnológicos da empresa.

4.5 Proteção de Dados Pessoais

O tratamento de dados pessoais deverá observar:

- Finalidade legítima;
- Base legal adequada;
- Necessidade e minimização dos dados;
- Transparência com os titulares;
- Segurança das informações;
- Respeito aos direitos dos titulares.

A coleta de dados deverá ocorrer apenas quando necessária ao desenvolvimento das atividades da empresa.

4.6 Direitos dos Titulares

A empresa respeitará os direitos previstos na LGPD, incluindo:

- Confirmação do tratamento;
- Acesso aos dados;
- Correção de informações;
- Anonimização ou eliminação quando aplicável;
- Portabilidade dos dados;
- Revogação do consentimento quando cabível.

As solicitações deverão ser tratadas de forma adequada e dentro dos prazos legais.

4.7 Compartilhamento de Informações

O compartilhamento de informações e dados pessoais somente poderá ocorrer quando:

- Houver necessidade operacional;
- Existir base legal aplicável;
- For indispensável à execução contratual;
- For exigido por obrigação legal ou regulatória.

O compartilhamento deverá ocorrer mediante controles adequados de segurança.

4.8 Armazenamento e Retenção

As informações e dados pessoais deverão ser armazenados de forma segura e mantidos apenas pelo período necessário para:

- Cumprimento de obrigações legais;
- Execução contratual;
- Atendimento de finalidades legítimas da empresa.

Após o término da necessidade, os dados deverão ser eliminados ou anonimizados, quando aplicável.

4.9 Segurança dos Sistemas

A empresa adotará medidas de proteção compatíveis com seus riscos, incluindo:

- Controle de acesso;
- Antivírus e ferramentas de proteção;
- Backup periódico;
- Monitoramento de sistemas;
- Atualizações de segurança;
- Gestão de vulnerabilidades;
- Controle de dispositivos e equipamentos.

As medidas poderão ser ampliadas conforme a evolução dos riscos tecnológicos.

4.10 Incidentes de Segurança

Todo incidente ou suspeita de incidente deverá ser comunicado imediatamente ao responsável designado pela empresa.

Exemplos:

- Vazamento de dados;
- Perda de equipamentos;
- Acesso não autorizado;
- Compartilhamento indevido de informações;
- Ataques cibernéticos.

Os incidentes deverão ser registrados, investigados e tratados adequadamente.

4.11 Treinamento e Conscientização

A empresa promoverá treinamentos periódicos relacionados a:

- Segurança da Informação;
- Proteção de Dados Pessoais;
- Boas práticas digitais;
- LGPD;
- Prevenção de incidentes.

As ações de conscientização integrarão o Programa de Integridade da empresa.

4.12 Uso de Equipamentos e Dispositivos

Os equipamentos fornecidos pela empresa deverão ser utilizados de forma responsável e segura.

O usuário deverá:

- Proteger suas credenciais;
- Bloquear o equipamento quando ausente;
- Comunicar perdas ou furtos;
- Zelar pelas informações armazenadas.

5. RESPONSABILIDADES

Alta Direção

- Aprovar esta Política;
- Disponibilizar recursos necessários;
- Promover a cultura de proteção de dados e segurança da informação.

Comitê de Integridade

- Monitorar riscos relacionados à integridade das informações;
- Apoiar ações corretivas e preventivas.

Área de Tecnologia da Informação

- Implementar controles de segurança;
- Gerenciar acessos;
- Realizar backups;
- Monitorar incidentes e vulnerabilidades.

Gestores

- Garantir o cumprimento desta Política em suas áreas;
- Orientar colaboradores quanto às boas práticas.

Colaboradores e Terceiros

- Cumprir esta Política;
- Proteger informações e dados pessoais;
- Comunicar incidentes ou irregularidades.

6. MONITORAMENTO E CONTROLE

O cumprimento desta Política será acompanhado por meio de:

- Auditorias internas;
- Monitoramento de acessos;
- Controle de incidentes;
- Avaliação de vulnerabilidades;
- Revisões periódicas de permissões;
- Indicadores de segurança;
- Treinamentos e campanhas de conscientização.

Os resultados poderão ser reportados periodicamente à Alta Direção.

7. PENALIDADES

O descumprimento desta Política poderá resultar em:

Para Colaboradores

- Orientação formal;
- Advertência verbal;
- Advertência escrita;
- Suspensão;
- Desligamento por justa causa, quando aplicável.

Para Terceiros

- Aplicação de penalidades contratuais;
- Suspensão de acessos;
- Rescisão contratual;

- Responsabilização por danos causados.

As medidas serão aplicadas conforme a gravidade da infração identificada.

8. DISPOSIÇÕES FINAIS

Esta Política integra o Programa de Integridade da empresa e deve ser observada em conjunto com:

- Código de Ética e Conduta;
- Política Anticorrupção;
- Política de Gestão de Riscos;
- Política do Canal de Denúncias;
- Política de Treinamento e Cultura de Integridade;
- Política de Gestão Documental;
- Demais normativos internos aplicáveis.

Os casos omissos serão analisados pela Alta Direção, pelo Comitê de Integridade e pelos responsáveis pela gestão da segurança da informação.

9. APROVAÇÃO E VIGÊNCIA

Aprovada por: Diretoria Executiva da Empresa

Data de Aprovação: 05/2026

Versão: 01

Próxima Revisão: 12 meses após sua aprovação ou sempre que houver alteração legal, regulatória, tecnológica ou necessidade identificada pela empresa.