POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

E PROTEÇÃO DE DADOS PESSOAIS

Documento corporativo de uso interno, aplicável a colaboradores, prestadores de serviço, parceiros e terceiros com acesso a informações, sistemas ou dados pessoais tratados pela empresa.

SUMÁRIO

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Estabelece diretrizes para proteção dos ativos de informação e dados pessoais da empresa, em conformidade com boas práticas (ISO 27002), LGPD- Lei Geral de Proteção de Dados Pessoais e demais legislações aplicáveis.

Complementa o Código de Conduta, Política de Privacidade e normas internas, reforçando o compromisso com ética, segurança e conformidade.

2. OBJETIVOS

- Definir padrões de segurança da informação e proteção de dados pessoais;
- Garantir confidencialidade, integridade, disponibilidade, autenticidade, legalidade e rastreabilidade das informações;
- Assegurar tratamento adequado dos dados pessoais durante todo o ciclo de vida;
- Atender aos direitos dos titulares;
- Estabelecer regras para gestão de incidentes e terceiros;
- Promover cultura de segurança, privacidade e conformidade.

3. APLICAÇÕES

- Aplica-se a todos os colaboradores e terceiros, em qualquer meio (físico ou digital).
- Ambientes e sistemas corporativos podem ser monitorados.
- Todos devem seguir a política e buscar orientação em caso de dúvida.

4. PRINCÍPIOS

- Uso das informações exclusivamente para fins profissionais;
- Monitoramento dos sistemas para garantir segurança;
- Observância aos princípios da LGPD-Lei Geral de Proteção de Dados Pessoais (finalidade, necessidade, transparência, segurança, etc.);
- Alinhamento com ética e governança corporativa.

5. REQUISITOS

- Formalização de confidencialidade em contratos;
- Treinamento e conscientização dos colaboradores;
- Comunicação imediata de incidentes;
- Implantação de controles de segurança e auditoria;
- Registro das operações de tratamento de dados;
- Procedimentos para atendimento aos titulares;
- Gestão e monitoramento de terceiros;
- Aplicação de medidas disciplinares em caso de descumprimento.

6. DAS RESPONSABILIDADES ESPECÍFICAS

6.1 Colaboradores

- Cumprir a política;
- Proteger informações e dados pessoais;
- Utilizar recursos de forma adequada;
- Comunicar incidentes;
- Participar de treinamentos.

6.2 - Gestores

- Garantir cumprimento da política;
- Definir acessos e supervisionar equipes;
- Apoiar auditorias e atendimento a titulares.

6.3 – T.I- Tecnologia da Informação

- Implementar controles de segurança;
- Monitorar sistemas e incidentes;
- Gerenciar acessos, backups e auditorias.

6.4 – DPO *Data Protection Officer* (Encarregado pelo Tratamento de Dados Pessoais) / Complice/ Jurídico

- Orientar sobre LGPD- Lei Geral de Proteção de Dados Pessoais;
- Atender titulares e ANPD- Autoridade Nacional de Proteção de Dados;
- Avaliar riscos e conformidade.

7. CONTROLE DAS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

Manter registro das operações contendo finalidade, base legal, dados tratados, compartilhamentos, segurança e prazos de retenção.

8. EXERCÍCIO DOS DIREITOS DOS TITULARES

Garantir acesso, correção, eliminação, portabilidade e demais direitos previstos na LGPD- Lei Geral de Proteção de Dados Pessoais, mediante canal oficial e validação de identidade.

9. TERCEIROS

Contratações devem prever:

- Confidencialidade;
- Segurança da informação;
- Proteção de dados;
- Comunicação de incidentes;
- Possibilidade de auditoria.

10. MONITORAMENTO E AUDITORIA

A empresa poderá monitorar sistemas, redes e dispositivos para garantir segurança, conformidade e investigação de incidentes.

11. INCIDENTES DE SEGURANÇA

Devem ser comunicados imediatamente.
O processo inclui identificação, contenção, análise, correção e, quando necessário, comunicação à ANPD- Autoridade Nacional de Proteção de Dados e aos titulares.

12. CICLO DE VIDA DOS DADOS

Os dados devem ser:

- Utilizados apenas pelo tempo necessário;
- Eliminados ou anonimizados ao final do prazo;
- Descartados de forma segura.

13. CAPACITAÇÃO

A empresa promove treinamentos e ações de conscientização sobre segurança da informação e proteção de dados.

14. PENALIDADES

O descumprimento pode gerar medidas administrativas, contratuais e legais.
Canais formais estão disponíveis para denúncias e dúvidas.

15. USO DE RECURSOS TECNOLÓGICOS

- Uso de e-mail e internet deve ser profissional e seguro;
- É proibido compartilhar informações sem autorização;
- Senhas e acessos são pessoais e intransferíveis;
- Equipamentos devem ser utilizados conforme as regras de segurança.

16. BACKUP E DISPOSITIVOS

- Backups devem ser realizados e testados regularmente;
- Dispositivos móveis devem possuir proteção adequada;
- Incidentes com dispositivos devem ser comunicados imediatamente.

17. DISPOSIÇÕES FINAIS

A segurança da informação e a proteção de dados são responsabilidades de todos.
A política pode ser atualizada a qualquer tempo e deve ser amplamente divulgada na organização.