LGPD

GOVERNANÇA E POLÍTICA INTERNA

-> Criação de uma Política de Privacidade clara e acessível, explicando como os dados são coletados, usados, armazenados e compartilhados.

-> Mapeamento de dados (Data Mapping): identificar quais dados pessoais são coletados, por quem, para que finalidade, onde são armazenados e com quem são compartilhados.

-> Nomeação de um Encarregado de Dados (DPO): responsável por intermediar a comunicação entre a empresa, os titulares dos dados e a ANPD (Autoridade Nacional de Proteção de Dados).

SEGURANÇA DA INFORMAÇÃO

-> Criptografia de dados sensíveis em repouso e em trânsito.

-> Controle de acesso: uso de autenticação forte e permissões de acesso com base em funções.

-> Auditoria e monitoramento contínuos para detectar e responder a incidentes de segurança.

-> Backups seguros e planos de recuperação de desastres.

//CONSETIMENTO E DIREITO DOS TITULARES

-> Coleta de consentimento explícito e informado, especialmente para dados sensíveis.

-> Facilidade para revogação do consentimento a qualquer momento.

-> Atendimento a solicitações dos titulares, como:

-> Acesso aos próprios dados;

-> Correção de dados;

-> Exclusão de dados ("direito ao esquecimento");

-> Portabilidade de dados.

//MINIMIZAÇÃO DE DADOS

-> Coleta apenas de dados necessários para a finalidade específica (princípio da necessidade).

-> Anonimização ou pseudonimização de dados sempre que possível, especialmente para análises estatísticas ou testes.

//TREINAMENTO E CONSCIENTIZAÇÃO

-> Capacitação contínua de colaboradores sobre a LGPD e boas práticas de proteção de dados.

-> Criação de uma cultura organizacional voltada à privacidade e à ética no uso da informação.

//CONFORMIDADE LEGAL E CONTRATUAL

-> Revisão de contratos com terceiros e fornecedores, garantindo cláusulas específicas sobre proteção de dados.

-> Avaliação de impacto à proteção de dados (DPIA) para atividades de alto risco.

-> Atualização de termos de uso e contratos de serviço para refletir as obrigações da LGPD.

// ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

-> É a principal norma internacional para segurança da informação.

-> Estabelece um conjunto de controles e processos para proteger a confidencialidade, integridade e disponibilidade das informações.

-> Apoia diretamente os princípios da LGPD, como segurança e prevenção.

// ISO/IEC 27701 – Extensão da ISO 27001 para Gestão da Privacidade

-> Complementa a ISO/IEC 27001 e ISO/IEC 27002.

-> Foca especificamente na gestão de informações pessoais identificáveis (PII).

-> Ajuda na implementação de um Sistema de Gestão da Privacidade da Informação (SGPI).

-> Considerada uma das normas mais alinhadas à LGPD e outras legislações de proteção de dados, como o GDPR europeu.

// ISO/IEC 27002 – Código de práticas para controles de segurança da informação

-> Fornece diretrizes práticas para implementar os controles definidos na ISO/IEC 27001.

-> Inclui práticas como controle de acesso, criptografia, segurança física e continuidade de negócios.

// ISO/IEC 29100 – Estrutura de Privacidade

-> Fornece uma estrutura de alto nível para proteção de privacidade em sistemas de informação.

-> Define princípios de privacidade, como consentimento, limitação de propósito, retenção limitada, etc.

-> É complementar à ISO/IEC 27701.

// ISO/IEC 29134 – Avaliação de Impacto à Privacidade (PIA/DPIA)

-> Fornece diretrizes sobre como realizar uma Privacy Impact Assessment (PIA), ou seja, avaliações de impacto à proteção de dados.

-> Essencial para lidar com atividades de tratamento de dados que representem riscos aos titulares.

6. ISO 9001 – Sistema de Gestão da Qualidade

-> Embora não trate diretamente da privacidade, suporta a padronização e melhoria contínua de processos, o que pode fortalecer práticas de compliance com a LGPD.