

MANUAL INTEGRADO DE SEGURANÇA DA INFORMAÇÃO E COMPLIANCE LIMA CABRAL ADVOGADOS

1. INTRODUÇÃO

Este Manual visa estabelecer os fundamentos normativos e operacionais que norteiam a Segurança da Informação e o Compliance no âmbito da LIMA CABRAL ADVOGADOS. Trata-se de um instrumento de governança essencial para mitigar riscos, assegurar a conformidade legal e promover a proteção efetiva dos ativos informacionais da organização.

2. OBJETIVOS

- *Estruturar uma cultura organizacional baseada na integridade, segurança e conformidade;*
- *Proteger os dados institucionais, dos clientes e de terceiros, evitando acessos não autorizados, perdas ou vazamentos;*
- *Garantir a aderência aos requisitos legais, contratuais e éticos, com ênfase na Lei Geral de Proteção de Dados Pessoais (LGPD);*
- *Estabelecer mecanismos formais de prevenção, detecção e resposta a incidentes e não conformidades.*

3. ESCOPO

Este Manual aplica-se a todos os níveis hierárquicos e operações da organização, incluindo:

- *Colaboradores efetivos e temporários;*
- *Estagiários e trainees;*
- *Prestadores de serviço e consultores externos;*
- *Fornecedores, parceiros e terceiros que tenham relação contratual ou institucional com a LIMA CABRAL ADVOGADOS.*



4. PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO

- *Confidencialidade: Proteger as informações contra acessos indevidos, assegurando que apenas indivíduos autorizados possam consultá-las;*
- *Integridade: Preservar a exatidão, consistência e confiabilidade dos dados durante todo seu ciclo de vida;*
- *Disponibilidade: Garantir que os dados e sistemas estejam acessíveis quando necessário aos usuários autorizados;*
- *Rastreabilidade: Possibilitar a identificação, autenticação e auditoria de todas as interações com ativos de informação.*

5. GOVERNANÇA E RESPONSABILIDADES

- *Alta Direção: Responsável por promover a cultura de segurança e compliance, alocar recursos e aprovar políticas;*
- *Encarregado de Dados (DPO): Atua como elo entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), assegurando a conformidade com a LGPD;*
- *TI e Segurança da Informação: Implementa controles técnicos, monitora vulnerabilidades, conduz respostas a incidentes e realiza testes de segurança;*
- *Todos os Colaboradores: Devem cumprir integralmente este Manual e participar de treinamentos periódicos.*

6. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

As informações serão classificadas segundo sua sensibilidade:

- *Pública: Divulgação irrestrita. Ex: Comunicados públicos.*
- *Interna: Uso restrito a membros da organização.*
- *Confidencial: Exige proteção contra acesso externo indevido. Ex: Dados de clientes.*

- *Restrita: Altamente sensível, acesso exclusivo a pessoas designadas. Ex: credenciais, estratégias legais.*

O tratamento deverá incluir criptografia, autenticação robusta, controle de acesso e revisão periódica das classificações.

7. DIRETRIZES TÉCNICAS E ADMINISTRATIVAS

- *Segregação de funções e controle de acesso baseado em privilégios mínimos;*
- *Políticas de senha com complexidade e troca periódica;*
- *Criptografia para proteção de dados sensíveis;*
- *Sistemas de detecção de intrusão, antivírus e firewall atualizados;*
- *Monitoramento contínuo e auditorias regulares;*
- *Programa de capacitação e conscientização em segurança e ética.*

8. GESTÃO DE INCIDENTES

Incidentes de segurança devem ser reportados à TI e ao DPO imediatamente. O tratamento seguirá as fases:

- *Identificação e registro do incidente;*
- *Contenção e análise de causa raiz;*
- *Recuperação e documentação completa;*
- *Notificação a titulares e órgãos reguladores, conforme legislação.*

9. COMPLIANCE E CONFORMIDADE LEGAL

O compliance garante que todos os atos institucionais estejam em conformidade com:

- *LGPD, Marco Civil da Internet, Estatuto da OAB e demais normas aplicáveis;*
- *Código de Ética e Conduta da organização;*
- *Regras contratuais, regulatórias e boas práticas de mercado.*

V.

Auditorias e controles internos avaliam a eficiência dos programas de conformidade.

10. DESCARTE SEGURO DE INFORMAÇÃO

- *Documentos físicos: Destruição mecânica (trituração) ou incineração controlada;*
- *Mídias digitais: Exclusão com ferramentas de sobrescrita seguras (wipe);*
- *Ambientes em nuvem: Utilização de recursos nativos de exclusão definitiva, com certificação de irrecuperabilidade.*

O processo deverá ser supervisionado pelo setor de TI e registrado para fins de auditoria.

11. PENALIDADES E SANÇÕES

Infringências serão objeto de medidas disciplinares, podendo resultar em:

- *Advertências formais;*
- *Suspensão temporária de acesso a sistemas;*
- *Rescisão contratual;*
- *Comunicação às autoridades competentes, quando aplicável.*

12. ATUALIZAÇÕES E VIGÊNCIA

Este Manual entra em vigor na data de sua disponibilização aos seus colaboradores, em 02.01.2025, e será revisado anualmente, ou quando houver mudança significativa em legislação, estrutura organizacional ou tecnologia utilizada pela organização



Lima Cabral Advogados