LIMA CABRAL ADVOGADOS

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

1. FINALIDADE

A presente Política tem por finalidade estabelecer os princípios, diretrizes e responsabilidades voltados à proteção dos ativos de informação da organização, assegurando o cumprimento dos pilares fundamentais da Segurança da Informação: **confidencialidade**, **integridade** e **disponibilidade** das informações, bem como promovendo a conformidade com os dispositivos legais vigentes, especialmente a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2. ÂMBITO DE APLICAÇÃO

Esta Política é aplicável a todos os colaboradores, estagiários, prestadores de serviços, fornecedores, parceiros e quaisquer terceiros que, no exercício de suas atividades, tenham acesso, manipulem ou processem informações pertencentes à organização ou sob sua guarda, em quaisquer meios, sejam físicos, eletrônicos ou lógicos.

3. PRINCÍPIOS NORTEADORES

A organização adota como princípios estruturantes de sua atuação em Segurança da Informação os seguintes:

- **Confidencialidade:** Garantia de que as informações sejam acessíveis apenas às pessoas autorizadas.
- **Integridade:** Salvaguarda da exatidão e completude da informação e dos métodos de processamento.
- **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso às informações e aos sistemas quando necessário.

- **Rastreabilidade:** Possibilidade de identificar, autenticar e registrar todas as ações executadas nos ativos de informação.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

4.1 OBJETIVO DA CLASSIFICAÇÃO

A classificação da informação tem por objetivo estabelecer critérios para seu tratamento, manuseio, acesso, armazenamento e descarte, conforme o nível de sensibilidade e os impactos potenciais à organização em caso de exposição, modificação ou perda.

4.2 CRITÉRIOS DE CLASSIFICAÇÃO

A classificação da informação deverá considerar:

- *O grau de sensibilidade do conteúdo;*
- *O impacto jurídico, financeiro, operacional ou reputacional de sua divulgação indevida;*
- *Exigências legais, contratuais e regulamentares;*
- *A necessidade de proteção de dados pessoais e sensíveis nos termos da LGPD.*

4.3 NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

Nível	Descrição	Exemplos
Pública	Informação de domínio público ou autorizada para ampla divulgação.	Comunicados institucionais, publicações em mídias oficiais.
Interna	Informação de uso restrito aos membros da organização.	Procedimentos operacionais internos, atas de reunião.
Confidencial	Informação cujo acesso não autorizado pode causar impactos significativos à organização ou a terceiros.	Dados de clientes, contratos, pareceres jurídicos.
Restrita	Informação de alto grau de sensibilidade, com acesso limitado exclusivamente a usuários designados.	Dados processuais sigilosos, credenciais administrativas, estratégias legais.

4.4 TRATAMENTO DA INFORMAÇÃO CLASSIFICADA

- Toda informação deverá ser identificada e manuseada conforme sua classificação.
- Informações "Confidenciais" e "Restritas" devem estar protegidas mediante criptografia, autenticação forte e controles de acesso.
- A classificação será revista periodicamente ou sempre que houver alteração de contexto ou finalidade.

5. DIRETRIZES TÉCNICAS E ADMINISTRATIVAS DE SEGURANÇA

A organização adota medidas preventivas, corretivas e de monitoramento contínuo, incluindo, mas não se limitando a:

- *Controle de acesso baseado em perfil e segregação de funções;*
- *Políticas de senhas fortes e autenticação multifator;*
- *Atualização constante de sistemas de proteção (firewalls, antivírus, EDR);*
- *Criptografia de dados em repouso e em trânsito;*
- *Backups periódicos e testes de recuperação;*
- *Monitoramento contínuo de ativos e detecção de incidentes;*
- *Conscientização e capacitação periódica de usuários.*

6. REMOÇÃO E DESCARTE SEGURO DE INFORMAÇÕES

6.1 OBJETIVO

Garantir que as informações classificadas como sensíveis ou restritas, ao atingirem o final de seu ciclo de vida, sejam eliminadas de forma definitiva e segura, evitando qualquer possibilidade de recuperação ou uso indevido.

6.2 PROCEDIMENTOS PARA REMOÇÃO SEGURA

MEIOS FÍSICOS:

- Documentos em papel devem ser destruídos por meio de trituração ou incineração.
- Mídias ópticas e magnéticas (CDs, DVDs, HDs, fitas) devem ser fisicamente destruídas ou submetidas a técnicas seguras de descaracterização.

MEIOS DIGITAIS:

- Aplicação de softwares especializados de sobrescrita segura (wipe ou secure erase).
- Exclusão lógica completa com verificação da irrecuperabilidade dos dados.
- Para dados de altíssima sensibilidade (nível "Restrito"), recomenda-se a destruição física do dispositivo.

AMBIENTES VIRTUAIS E NUVEM:

- Exclusão definitiva de dados por meio de funções específicas de descarte seguro disponíveis nas plataformas contratadas.
- Certificação de que os dados não serão mantidos em cache, backups paralelos ou sistemas de retenção automatizados.

6.3 RESPONSABILIDADES

- A área de Tecnologia da Informação é responsável por supervisionar tecnicamente os procedimentos de descarte.

- As áreas usuárias são responsáveis por identificar o fim da utilidade da informação e solicitar o procedimento adequado.
- O processo de descarte deve ser documentado e, quando aplicável, auditado.

7. GESTÃO DE INCIDENTES DE SEGURANÇA

Todos os incidentes de segurança devem ser registrados e comunicados imediatamente ao Encarregado de Dados e à área de TI. A resposta seguirá um plano previamente estabelecido, com contenção, análise, documentação e comunicação aos órgãos competentes, conforme a legislação aplicável.

8. PENALIDADES E SANÇÕES

O descumprimento das disposições desta Política acarretará a aplicação de sanções administrativas, civis e, eventualmente, criminais, conforme a natureza e gravidade da infração, respeitados os princípios do contraditório e da ampla defesa.

9. VIGÊNCIA E ATUALIZAÇÕES

Esta Política foi atualizada e entra em vigor na data de sua publicação, no dia 02/01/2025, devendo ser revisada anualmente ou sempre que houver alteração relevante nos processos, tecnologias, estrutura organizacional ou legislação aplicável.

LIMA CABRAL ADVOGADOS ASSOCIADOS