

## **Plano de Análise de Riscos da Empresa Municipal de Artes Gráficas do Rio de Janeiro S/A**

### **Objetivo:**

Este plano tem como finalidade identificar, avaliar e mitigar os riscos relacionados à proteção de dados pessoais tratados pela Empresa Municipal de Artes Gráficas do Rio de Janeiro S/A – Imprensa da Cidade, conforme as legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD).

Serão abordados riscos que possam gerar impactos potenciais sobre os titulares dos dados, definindo medidas de mitigação, salvaguardas e mecanismos para reduzir a exposição aos riscos.

---

### **1. Identificação de Riscos**

#### **Risco 1: Acesso não autorizado a dados pessoais**

- **Descrição:** Possibilidade de acesso indevido a informações pessoais contidas nos sistemas da empresa, tanto por agentes internos (colaboradores) quanto externos (hackers).
- **Probabilidade:** Alta
- **Impacto:** Elevado (comprometimento da privacidade dos dados pessoais)
- **Nível de Risco:** Crítico

#### **Risco 2: Vazamento de dados por falha em medidas de segurança**

- **Descrição:** Possibilidade de vazamento acidental ou proposital de dados, seja por ataques cibernéticos ou erros internos.
- **Probabilidade:** Média
- **Impacto:** Alto (exposição de dados sensíveis e danos reputacionais)
- **Nível de Risco:** Alto

#### **Risco 3: Falha na anonimização ou pseudonimização de dados**

- **Descrição:** Inadequação nas técnicas de anonimização ou pseudonimização, permitindo a reidentificação dos titulares dos dados.
- **Probabilidade:** Baixa
- **Impacto:** Médio (violação do princípio da minimização de dados)
- **Nível de Risco:** Médio

#### Risco 4: Armazenamento inadequado de dados pessoais

- **Descrição:** Falha no armazenamento seguro de dados, seja em meios digitais ou físicos, resultando na exposição indevida de informações.
- **Probabilidade:** Média
- **Impacto:** Elevado (vulnerabilidade à violação de dados)
- **Nível de Risco:** Alto

#### Risco 5: Uso indevido de dados pessoais

- **Descrição:** Utilização dos dados pessoais coletados para finalidades não autorizadas ou que não correspondam às expectativas dos titulares.
- **Probabilidade:** Média
- **Impacto:** Médio (não conformidade com a LGPD)
- **Nível de Risco:** Médio

#### Risco 6: Falha no atendimento aos direitos dos titulares de dados

- **Descrição:** Dificuldade ou incapacidade de responder a solicitações de acesso, retificação ou exclusão de dados pessoais.
- **Probabilidade:** Baixa
- **Impacto:** Médio (não conformidade legal e danos à reputação)
- **Nível de Risco:** Baixo

---

## 2. Análise de Probabilidade e Impacto

A tabela abaixo utiliza uma escala de 1 a 5, onde:

- **Probabilidade:** 1 (muito baixa), 5 (muito alta)
- **Impacto:** 1 (baixo), 5 (crítico)

RISCO	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO
Acesso não autorizado a dados	5	5	Crítico
Vazamento de dados	4	5	Alto
Falha na anonimização de dados	2	3	Médio
Armazenamento inadequado de dados	3	5	Alto
Uso indevido de dados	3	4	Médio
Falha no atendimento aos direitos	3	5	Alto

---

### 3. Medidas, Salvaguardas e Mecanismos de Mitigação

Com base nos riscos identificados, as seguintes medidas serão adotadas para mitigar os riscos associados ao tratamento de dados pessoais:

#### 3.1 Medidas Técnicas

- **Criptografia:** Aplicação de criptografia em todos os dados pessoais armazenados, tanto em repouso quanto em trânsito.
- **Pseudonimização:** Sempre que possível, utilizar técnicas de pseudonimização para tratar dados de forma a reduzir os riscos de identificação dos titulares.
- **Controle de Acesso:** Implementar controles de acesso rigorosos para limitar o acesso a dados pessoais apenas a funcionários autorizados e devidamente treinados.
- **Monitoramento e Auditoria:** Utilizar ferramentas de monitoramento para detectar atividades suspeitas e realizar auditorias regulares para garantir a conformidade com as políticas de segurança.

#### 3.2 Medidas Administrativas

- **Políticas de Segurança da Informação:** Desenvolver e manter políticas internas que orientem o tratamento de dados pessoais, reforçando boas práticas entre os colaboradores.
- **Treinamento e Conscientização:** Promover treinamentos periódicos para todos os colaboradores sobre os princípios da LGPD, segurança da informação e privacidade.
- **Procedimentos para Resposta a Incidentes:** Estabelecer um plano claro de resposta a incidentes de segurança, com comunicação rápida e eficiente, tanto para os titulares dos dados quanto para as autoridades competentes.

#### 3.3 Medidas Físicas

- **Controle de Acesso Físico:** Garantir que os locais onde dados pessoais são armazenados fisicamente (arquivos, servidores, etc.) estejam protegidos por medidas de controle de acesso físico, como câmeras de segurança e vigilância.
- **Descarte Seguro de Informações:** Implementar procedimentos para garantir o descarte seguro de informações pessoais, seja em formato digital (deleção permanente) ou físico (destruição de documentos).

---

### 4. Resultados Esperados

Após a implementação das medidas e salvaguardas descritas, espera-se que a Empresa Municipal de Artes Gráficas do Rio de Janeiro esteja:

- Conformidade com a LGPD, especialmente no que tange à proteção de dados pessoais e à transparência nas operações de tratamento de dados.

- Redução dos riscos de violação de dados pessoais e suas consequências, como sanções legais, danos reputacionais e perda de confiança dos titulares.
  - Pronta para a elaboração do **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**, que documentará as medidas adotadas para a mitigação de riscos e conformidade legal.
- 

## 5. Monitoramento e Revisão Contínua

O plano de análise de riscos deve ser revisado periodicamente para garantir que as medidas implementadas continuem adequadas às novas ameaças e desafios. Sugere-se a criação de um comitê de segurança da informação que será responsável por:

- Revisar e atualizar as políticas de segurança.
- Auditar os controles implementados e sua eficácia.
- Realizar simulações de ataques ou incidentes para avaliar a resposta da empresa.

Este processo contínuo de análise e monitoramento assegura a conformidade sustentável e a proteção eficaz dos dados pessoais tratados pela empresa