# Plano de Mitigação de Riscos

## Identificação e Mapeamento de Dados

### Inventário de Dados

- Identifique todos os dados pessoais e sensíveis tratados pela instituição pública, incluindo informações coletadas, armazenadas, processadas e compartilhadas.

### Classificação dos Dados

- Classifique os dados por nível de sensibilidade (pessoais, sensíveis, anônimos) e identifique o ciclo de vida dos dados (desde a coleta até a exclusão).

### Mapeamento de Riscos

- Analise os pontos críticos onde pode ocorrer tratamento inadequado, acesso não autorizado ou uso indevido dos dados.

---

## Avaliação de Riscos

### Análise de Impacto de Privacidade (PIA - Privacy Impact Assessment)

- Avaliar as atividades que envolvem tratamento de dados para medir o potencial impacto em caso de vazamento.

### Riscos de Conformidade

- Identificar os riscos associados à não conformidade com a LGPD, como sanções administrativas, danos à reputação e impacto na segurança da informação.

### Riscos Operacionais e Tecnológicos

- Considerar os riscos associados a tecnologias utilizadas, políticas de acesso e falhas em procedimentos internos.

---

## Planejamento de Medidas de Mitigação

### Governança de Dados

- Estabelecer uma política interna de governança de dados pessoais e nomear um Encarregado de Proteção de Dados (DPO) para monitorar e orientar o cumprimento da LGPD.

### Controles de Acesso e Segurança

- Implementar controles de segurança para evitar acessos não autorizados, como autenticação multifatorial, criptografia e anonimização de dados.

### Minimização de Dados

- Coletar e tratar apenas os dados estritamente necessários ao cumprimento da finalidade pública. Reduzir a coleta excessiva e eliminar dados obsoletos.

### Treinamento e Capacitação

- Treinar colaboradores, especialmente aqueles que trabalham com dados pessoais, sobre práticas de proteção de dados e responsabilidades individuais sob a LGPD.

---

## Políticas de Transparência e Comunicação

### Informação ao Público

- Estruturar um canal de comunicação transparente, que permita ao cidadão compreender como seus dados são tratados, armazenados e para que finalidades.

### Política de Privacidade e Termos de Uso

- Publicar uma política clara e objetiva de privacidade e termos de uso para todos os sistemas que coletam dados pessoais, informando sobre os direitos dos titulares.

### Respostas a Incidentes de Segurança

- Criar um plano de resposta a incidentes com protocolos para notificação de incidentes à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

---

## Monitoramento e Auditoria Contínua

### Auditorias Regulares

- Realizar auditorias periódicas para assegurar a conformidade com a LGPD e identificar novas vulnerabilidades no tratamento de dados.

### Indicadores de Conformidade

- Estabelecer indicadores para monitorar a efetividade do plano de mitigação de riscos e sua implementação.

### Revisão e Atualização de Políticas

- Atualizar constantemente as políticas de tratamento de dados e o plano de mitigação de acordo com as diretrizes da ANPD e as novas ameaças cibernéticas.

---

## Documentação e Reportes

### Registros de Operações de Tratamento

- Documentar todas as operações de tratamento de dados, com informações sobre a finalidade, tipo de dado, tempo de retenção e medidas de segurança aplicadas.

### Relatórios de Impacto à Proteção de Dados Pessoais

- Gerar relatórios de impacto sempre que houver alterações significativas no tratamento de dados ou surgirem novos riscos.

---

## Revisão do Plano e Melhoria Contínua

### Feedback Contínuo

- Solicitar feedback das áreas envolvidas para identificar melhorias contínuas no processo de proteção de dados.

### Benchmarking

- Estar atualizado com as melhores práticas do setor público, considerando mudanças legislativas e casos de jurisprudência.