

# DPIA - Avaliação de Impacto

Empresa: Teste

Data: 18/12/2025

## Descrição do Tratamento:

A Empresa Teste, atuante no setor de Tecnologia/Software, realiza tratamento de dados pessoais de clientes para fins de cadastro, autenticação, personalização de serviços e envio de comunicações de marketing. O tratamento envolve coleta de nome, endereço de e-mail, telefone, dados de navegação (cookies, endereço IP) e dados de uso dos serviços. Os dados são armazenados em servidores cloud com medidas de segurança padrão de mercado. O acesso aos dados é restrito a funcionários autorizados e mediante autenticação. A empresa busca aumentar sua maturidade em proteção de dados, atualmente em 44/100, através da implementação de controles mais robustos e processos de gestão da privacidade.

## Riscos Identificados

- Vazamento de dados devido a falha de segurança no servidor cloud. (Alto)
- Acesso não autorizado aos dados por funcionários internos. (Médio)
- Uso indevido dos dados para fins diferentes dos explicitados na política de privacidade. (Médio)
- Não cumprimento dos direitos dos titulares (acesso, retificação, exclusão). (Médio)
- Coleta excessiva de dados desnecessários para a finalidade do serviço. (Baixo)

## Medidas de Mitigação:

- Implementar autenticação de dois fatores (2FA) para todos os acessos aos dados.
- Realizar testes de intrusão e vulnerabilidade regulares nos servidores cloud.
- Criptografar os dados em repouso e em trânsito.
- Implementar um programa de treinamento e conscientização sobre proteção de dados para todos os funcionários.
- Revisar e atualizar a política de privacidade, tornando-a mais clara e transparente.

## Score de Risco Residual: 6/10

- Implementar um Processo formal para responder às solicitações dos titulares de dados (direitos LGPD).
- Realizar o mapeamento do fluxo de dados e identificar os dados minimamente necessários para cada finalidade.
- Implementar controle de acesso baseado em função (RBAC) para limitar o acesso aos dados apenas às pessoas que precisam deles.
- Implementar um sistema de monitoramento e alerta para detectar atividades suspeitas ou anormais nos sistemas.
- Realizar avaliações de impacto à proteção de dados (DPIA) regulares para novos projetos e mudanças nos processos existentes.