DPIA - Avaliação de Impacto

Empresa: Teste
Data: 18/12/2025

Descrição do Tratamento:

Desenvolvimento e operação de uma plataforma de software SaaS (Software as a Service) que coleta, processa e armazena dados pessoais de usuários para fins de autenticação, personalização da experiência, fornecimento de funcionalidades específicas do serviço e geração de relatórios analíticos. A plataforma também integra com sistemas de terceiros para otimizar a entrega de serviços e coletar dados adicionais relevantes para aprimorar a qualidade da plataforma. Os dados coletados incluem nome, endereço de e-mail, informações de contato, dados demográficos básicos, dados de uso da plataforma (logs de acesso, páginas visitadas, funcionalidades utilizadas), e, dependendo da funcionalidade utilizada, dados sensíveis como localização (opcional e com consentimento explícito). O tratamento envolve coleta, armazenamento, processamento, análise, compartilhamento (com terceiros para suporte técnico e analítico) e descarte dos dados. O período de retenção dos dados varia conforme a finalidade e a legislação aplicável, buscando-se sempre as obrigações legais e regulatórias aplicáveis.

Riscos Identificados:

- Vazamento ou acesso não autorizado aos dados pessoais armazenados na plataforma, devido a falhas de segurança ou ataques cibernéticos. (Alto)
- Uso indevido dos dados pessoais para finalidades não autorizadas ou incompatíveis com a finalidade original da coleta, como a venda para terceiros sem consentimento. (Médio)
- Não conformidade com a legislação de proteção de dados (LGPD), resultando em multas, sanções e danos à reputação da empresa. (Alto)
- Falha na implementação de medidas de segurança adequadas para proteger os dados pessoais, tornando-os vulneráveis a ameaças. (Alto)
- Dificuldade em garantir o exercício dos direitos dos titulares dos dados (acesso, retificação, exclusão, etc.) devido a processos inadequados ou falta de recursos. (Médio)
- Compartilhamento inadequado de dados pessoais com terceiros (parceiros, fornecedores, etc.), sem garantias contratuais de proteção de dados. (Médio)
- Coleta excessiva de dados pessoais, sem uma justificativa clara e legítima, aumentando o risco de uso indevido e violação de privacidade. (Médio)
- Falta de transparência com os titulares dos dados sobre as práticas de tratamento de dados, dificultando o exercício de seus direitos e a confiança na plataforma. (Médio)
- Retenção de dados pessoais por um período excessivo, sem uma necessidade legítima, aumentando o risco de exposição em caso de vazamento. (Médio)
- Ausência de um plano de resposta a incidentes de segurança, dificultando a contenção e a recuperação em caso de vazamento de dados. (Alto)

Medidas de Mitigação:

- Implementar medidas de segurança técnicas e organizacionais robustas, incluindo criptografia de dados em repouso e em trânsito, firewalls, sistemas de detecção de intrusão, e autenticação de dois fatores.
- Realizar testes de segurança regulares, como testes de penetração e varreduras de vulnerabilidades, para identificar e corrigir falhas de segurança.
- Implementar controles de acesso rígidos aos dados pessoais, concedendo acesso apenas aos funcionários que necessitam das informações para desempenhar suas funções.
- Obter o consentimento explícito dos titulares dos dados para o tratamento de dados pessoais sensíveis e para finalidades específicas.
- Fornecer informações claras e transparentes aos titulares dos dados sobre as práticas de tratamento de dados.
- Implementar mecanismos para garantir o exercício dos direitos dos titulares dos dados (acesso, retificação, exclusão, etc.), incluindo a disponibilização de um canal de comunicação para solicitações.
- Celebrar contratos com terceiros que tenham acesso aos dados pessoais, exigindo o cumprimento das obrigações de proteção de dados.
- Minimizar a coleta de dados pessoais, coletando apenas as informações necessárias para a finalidade específica.
- Anonimizar ou pseudonimizar os dados pessoais sempre que possível, para reduzir o risco de identificação dos titulares.
- Definir um período de retenção de dados adequado para cada tipo de dado pessoal, eliminando os dados que não são mais necessários.
- Implementar um plano de resposta a incidentes de segurança, incluindo procedimentos para notificar os titulares dos dados e as autoridades competentes em caso de vazamento de dados.
- Realizar treinamentos regulares com os funcionários sobre proteção de dados e segurança da informação.
- Nomear um Encarregado de Proteção de Dados (DPO) para supervisionar a implementação e o cumprimento da LGPD.
- Implementar um sistema de gestão de consentimento para garantir o registro e a gestão do consentimento dos titulares dos dados.
- Realizar auditorias internas regulares para verificar o cumprimento das políticas e procedimentos de proteção de dados.
- Utilizar técnicas de Data Loss Prevention (DLP) para monitorar e prevenir a saída não autorizada de dados sensíveis da organização.
- Implementar um programa de conscientização contínuo para os funcionários sobre os riscos e responsabilidades relacionados à proteção de dados.
- Realizar análises de impacto à proteção de dados (DPIAs) para novos projetos e processos que envolvam o tratamento de dados pessoais.

Score de Risco Residual: 6.10