**Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**

**1. Introdução** Este Relatório de Impacto à Proteção de Dados Pessoais (RIPD) tem como objetivo analisar os riscos associados ao tratamento de dados pessoais no site, considerando a estrutura STRIDE e a metodologia de Torr (2005). O foco será nas funcionalidades de login e dashboard, com a identificação dos riscos e medidas para mitigá-los.

**2. Identificação e Avaliação dos Riscos (Etapa 6)**

### **2.1 Tela de Login**

A tela de login permite o acesso ao sistema por meio de credenciais (usuário e senha). Os riscos identificados são:

* **Repúdio:** Um usuário pode negar ter realizado determinada ação dentro do sistema, criando dificuldades para auditoria e rastreamento.
* **Spoofing:** Um atacante pode tentar se passar por um usuário legítimo, utilizando credenciais roubadas ou forjadas.

### **2.2 Dashboard de Geração de Imagens**

A tela de dashboard permite que o usuário insira palavras-chave para gerar imagens por IA. O principal risco identificado é:

* **Spoofing no Token da API:** Um atacante pode tentar utilizar um token roubado para acessar a API de geração de imagens, comprometendo a segurança do sistema e o controle de uso dos serviços.

A gravidade desses riscos é alta, pois podem comprometer a confidencialidade, integridade e disponibilidade dos dados pessoais.

**3. Identificação de Medidas para Tratar os Riscos (Etapa 7)**

### **3.1 Medidas para a Tela de Login**

Para mitigar os riscos de repúdio e spoofing, serão implementadas as seguintes soluções:

* **Uso de JWT (JSON Web Token):** O token será renovado a cada 1h para garantir que apenas usuários autenticados mantenham acesso.
* **Validação no Banco de Dados:** Cada token será validado no banco de dados para verificar o nível de acesso do usuário e impedir acessos indevidos.
* **Registro de Atividades:** Será implementado um sistema de logs que registrará todas as ações do usuário para evitar repúdio.

### **3.2 Medidas para o Dashboard de Geração de Imagens**

Para mitigar o risco de spoofing no token da API:

* **Renovação Periódica do Token:** O token da API será renovado a cada 1h para reduzir o tempo de exposição em caso de comprometimento.
* **Detecção de Uso Indevido:** O sistema monitorará tentativas de acesso irregulares ao token, invalidando-o e gerando um novo caso um comportamento suspeito seja identificado.

**4. Conclusão** A aplicação da metodologia STRIDE e de Torr (2005) permitiu identificar e tratar riscos de segurança nas funcionalidades do site. As medidas propostas minimizam os impactos negativos sobre a proteção de dados pessoais, garantindo maior segurança e conformidade com boas práticas de segurança da informação.