## **1. Introdução**

A geração de imagens utilizando inteligência artificial (IA) tem se tornado uma ferramenta poderosa para designers, artistas e empresas. No entanto, essa tecnologia também apresenta desafios relacionados à segurança dos dados, principalmente no que diz respeito ao acesso e autenticação de usuários. Este relatório aborda os riscos associados ao uso de IA para geração de imagens e vídeos em um ambiente web, propondo soluções para mitigar ameaças potenciais.

## **2. Desenvolvimento**

### **2.1 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, dashboard e geração de vídeo, com a identificação dos riscos e medidas para mitigá-los.

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

##### **2.2 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.

##### **2.3 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.

##### **2.4 Geração de Vídeo a partir da Imagem**

A funcionalidade de geração de vídeo a partir da imagem introduz novos riscos:

* **Manipulação do Conteúdo**: Um atacante pode tentar manipular o vídeo gerado, inserindo conteúdo malicioso ou alterando informações.
* **Violação de Direitos Autorais**: A geração de vídeos a partir de imagens de terceiros pode violar direitos autorais, caso não haja a devida autorização.
* **Deepfakes**: A tecnologia de IA pode ser utilizada para criar deepfakes, vídeos falsos incrivelmente realistas que podem ser usados para difamar, manipular ou prejudicar pessoas.

A gravidade desses riscos é alta, pois podem comprometer a confidencialidade, integridade e disponibilidade dos dados pessoais, além de gerar problemas legais e de reputação.

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

##### **2.5 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.

##### **2.6 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.

##### **2.7 Medidas para a Geração de Vídeo**

Para mitigar os riscos relacionados à geração de vídeo:

* **Assinatura Digital**: Os vídeos gerados serão assinados digitalmente para garantir sua integridade e autenticidade, impedindo a manipulação do conteúdo.
* **Marca d'água**: Os vídeos receberão uma marca d'água com informações sobre a origem e a data de criação, dificultando a utilização indevida e a violação de direitos autorais.
* **Termos de Uso**: O usuário deverá concordar com termos de uso que explicitam as responsabilidades sobre o conteúdo gerado, incluindo a proibição de deepfakes e a necessidade de autorização para uso de imagens de terceiros.
* **Monitoramento e Denúncia**: Será implementado um sistema de monitoramento para identificar e remover vídeos que violem os termos de uso ou causem danos a terceiros. Os usuários também poderão denunciar conteúdos inadequados.

#### **4. Conclusão**

A aplicação da metodologia STRIDE e de Torr (2005) permitiu identificar e tratar riscos de segurança nas funcionalidades do site, incluindo a geração de vídeo. 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.

### **2.8 Código no GitHub**

[Insira aqui o link para o repositório no GitHub]

## **3. Considerações Finais**

Este projeto abordou a geração de imagens e vídeos por IA e os riscos associados à proteção de dados. A implementação de medidas de segurança como a renovação periódica de tokens, a monitoração de acessos, a assinatura digital e a marca d'água permite minimizar riscos e garantir uma experiência segura para os usuários. Futuras melhorias podem incluir a implementação de autenticação multifator (MFA) e a adoção de políticas de segurança mais robustas para acesso à API.

A inclusão da funcionalidade de geração de vídeo a partir da imagem demonstra o potencial de expansão do projeto, oferecendo aos usuários uma ferramenta inovadora e criativa, com a devida atenção aos aspectos de segurança e responsabilidade.