Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

1. Introdução

Este relatório apresenta uma análise detalhada dos riscos associados ao uso de inteligência artificial no contexto da **cadeia produtiva do café**, dentro do escopo do projeto desenvolvido. O foco está na **transcrição de áudio e geração de música baseada em texto**, tecnologias que podem lidar com informações sensíveis e demandam medidas de proteção de dados.

A análise segue a metodologia **STRIDE**, identificando possíveis vulnerabilidades e sugerindo medidas de mitigação para minimizar impactos à privacidade e segurança dos usuários.

---

2. Identificação e Avaliação de Riscos

A implementação do projeto envolve o uso de **dados de áudio e transcrição de fala**, o que pode levar a riscos associados ao manuseio dessas informações. Os principais riscos identificados são:

- **Coleta de dados sensíveis**: O áudio pode conter informações pessoais ou confidenciais.
- **Armazenamento e vazamento de dados**: O risco de exposição ou uso indevido de áudios transcritos.
- **Uso indevido da IA**: Geração ou modificação de áudios para fins maliciosos.

2.1 Aplicação da Metodologia STRIDE

A análise de ameaças foi realizada conforme a estrutura STRIDE, avaliando os riscos com base em **descrição, impacto, probabilidade e gravidade**:

Categoria	Descrição	Impacto	Probabilidade	Gravidade
Spoofing (Falsificação)	Manipulação de áudios para forjar transcrições.	Uso indevido de identidade digital.	Média	Alta
Tampering (Adulteração)	Alteração maliciosa de arquivos transcritos.	Mudança de informações críticas sem detecção.	Alta	Alta
Repudiation (Repudiação)	Dificuldade em validar a autenticidade de uma transcrição.	Perda de confiabilidade dos dados.	Média	Média
Information Disclosure (Divulgação de Informações)	Exposição de áudios transcritos sem consentimento.	Vazamento de informações privadas.	Média	Alta
Denial of Service (DoS)	Sobrecarga da API de transcrição por múltiplas requisições simultâneas.	Interrupção do serviço.	Baixa	Média
Elevation of Privilege (Elevação de Privilégio)	Acesso não autorizado aos arquivos de áudio e transcrição.	Uso indevido de dados confidenciais.	Alta	Alta

Cada um desses riscos pode impactar a privacidade e a segurança dos usuários, tornando essencial a aplicação de estratégias para mitigar seus efeitos.

---

3. Medidas de Mitigação Sugeridas (ETAPA 7)

Com base nos riscos identificados, algumas medidas **foram sugeridas** para fortalecer a segurança do sistema. Estas incluem:

- **Criptografia de Dados Sensíveis**: Para proteger arquivos de áudio e transcrições contra vazamento.
- **Autenticação JWT**: Implementação de autenticação para restringir o acesso a usuários autorizados.
- **Auditoria e Monitoramento**: Registro detalhado de acessos e transações para detectar padrões anômalos.

- **Remoção Automática de Dados Temporários**: Excluir arquivos de áudio logo após o processamento para reduzir riscos de exposição.
- **Rate Limiting**: Limitação do número de requisições para evitar ataques de sobrecarga (DoS).

Essas estratégias visam garantir que o projeto esteja alinhado com boas práticas de proteção de dados e normas como a **LGPD** (Lei Geral de Proteção de Dados). A implementação de algumas dessas medidas pode ser considerada em futuras iterações do sistema.

---

4. Conclusão

A análise de riscos mostrou que o uso de **inteligência artificial aplicada à transcrição e geração de áudio** pode introduzir desafios significativos em termos de **segurança e privacidade**. Embora o projeto esteja funcional, **a adoção de medidas de proteção de dados deve ser considerada em futuras atualizações** para garantir maior segurança e conformidade regulatória.

Dessa forma, este relatório serve como um **guia de boas práticas**, identificando os principais riscos e sugerindo formas de mitigação para um uso mais seguro da tecnologia desenvolvida.