MAICON QUERINO JESUS DE SOUZA - 202210115

RELATÓRIO RIPD

LAVRAS

2025

RELATÓRIO RIPD

Relatório de Impacto à Proteção de Dados Pessoais
Disciplina: Sistemas Distribuídos
Professor: André Lima Salgado.

LAVRAS

2025

Introdução

Este relatório tem como finalidade avaliar os riscos associados ao tratamento de dados pessoais no projeto de conversão de texto em fala, garantindo a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). O projeto visa desenvolver um sistema que trabalha com um agentes inteligente, que vai pegar o áudio gravado pelo usuário e transcrever esse áudio permitindo que usuários gravem áudios e tenham uma transcrição exata do que foi falado.

Mapeamento do fluxo de dados

Os usuários inserem textos no sistema, que podem conter dados pessoais identificáveis, os textos são processados por uma IA de conversão de fala em texto chamada Whisper, os audios submetidos e os textos gerados são armazenados temporariamente no servidor para processamento e posterior download pelo usuário, não há compartilhamento de dados com terceiros; os dados são utilizados exclusivamente para a finalidade descrita, após um período definido (por exemplo, 24 horas), os textos e áudios são permanentemente excluídos do sistema.

Avaliação de Necessidade e Proporcionalidade

O tratamento dos dados é necessário para fornecer o serviço de conversão de texto em fala solicitado pelo usuário, O sistema foi projetado para minimizar a coleta de dados, solicitando apenas o áudio necessário para a conversão, a coleta e o processamento dos textos são essenciais para a funcionalidade do serviço oferecido.

Identificação e Avaliação dos Riscos

- Utilizando a metodologia STRIDE, foram identificadas as seguintes ameaças:
- Spoofing (Falsificação de Identidade): Risco de usuários mal-intencionados se passarem por outros para acessar dados alheios.
- Tampering (Manipulação de Dados): Possibilidade de adulteração dos textos submetidos ou dos áudios gerados.
- Repudiation (Repúdio): Usuários negarem ter submetido determinados textos ou realizado certas ações no sistema.

- Information Disclosure (Divulgação de Informações): Risco de exposição não autorizada de textos ou áudios contendo dados pessoais.
- Denial of Service (Negação de Serviço): Ataques que possam interromper o funcionamento do sistema, impedindo seu uso legítimo.
- Elevation of Privilege (Elevação de Privilégio): Usuários obtendo permissões além das concedidas, comprometendo a segurança do sistema.

Ameaças	**Probabilidade**	**Impacto**
Spoofing	Média	Alto
Tampering	Baixa	Médio
Repudiation	Média	Médio
Information Disclosure:	Alta	Alto
Denial of Service	Média	Alto
Elevation of Privilege:	Baixa	Alto

Medidas para Tratamento dos Riscos

Spoofing: Implementação de autenticação robusta para garantir que apenas usuários autorizados acessem o sistema. **Tampering:** Utilização de hashes criptográficos para verificar a integridade dos textos e áudios. **Repudiation**: Manutenção de logs detalhados das atividades dos usuários, com registros de data, hora e ações realizadas. **Information Disclosure**: Criptografia dos dados em trânsito e em repouso, além de políticas de acesso restrito baseadas em permissões. **Denial of Service:** Implementação de mecanismos de detecção e prevenção de ataques DoS, como limites de taxa de requisições e monitoramento de tráfego. **Elevation of Privilege**: Aplicação do princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para suas funções.

Plano de Ação

As medidas serão priorizadas com base na gravidade dos riscos e na viabilidade de implementação, e ainda serão designados responsáveis específicos para a implementação e monitoramento de cada medida, estabelecendo cronogramas claros para a implementação das medidas propostas.

Monitoramento e Revisão

Esses processos foram estabelecidos para monitorar a eficácia das medidas implementadas e revisar o RIPD periodicamente ou sempre que houver mudanças significativas no sistema ou no contexto de tratamento de dados.

Conclusão

Este Relatório de Impacto à Proteção de Dados Pessoais demonstra a aplicação dos conceitos de segurança da informação aprendido na disciplina de Sistemas Distribuídos, além de reforçar o compromisso do projeto com a conformidade à LGPD e a proteção dos dados pessoais dos usuários. As medidas implementadas visam mitigar os riscos identificados e garantir a segurança e privacidade dos dados tratados pelo sistema.