Relatório de Impacto à Proteção de Dados Pessoais

Identificação e Avaliação dos Riscos

No contexto deste sistema de chat, os principais riscos relacionados à proteção de dados pessoais incluem:

1. **Coleta e Armazenamento de Dados Pessoais:** Caso o arquivo CSV contenha dados pessoais, há o risco de coleta e armazenamento indevidos desses dados pelo sistema.
2. **Processamento de Dados Sensíveis:** O sistema pode processar informações sensíveis sem o devido consentimento ou base legal, especialmente se os dados do CSV forem de natureza confidencial.
3. **Compartilhamento Não Autorizado:** Há o risco de compartilhamento não autorizado de dados pessoais com terceiros, seja por vulnerabilidades no sistema ou por falta de controles adequados.
4. **Armazenamento Inseguro:** Se os dados pessoais forem armazenados sem criptografia ou medidas de segurança adequadas, podem estar suscetíveis a acessos não autorizados.
5. **Retenção Indevida de Dados:** Manter dados pessoais por períodos superiores ao necessário pode levar a violações das legislações de proteção de dados.

Modelagem de Ameaças

Tendo em vista a metodologia de Torr e a estrutura STRIDE, as seguintes ameaças foram identificadas:

1. **Spoofing (Falsificação):** Um agente malicioso pode se passar por um usuário legítimo para acessar dados pessoais.
2. **Tampering (Manipulação):** Alteração não autorizada dos dados armazenados ou em trânsito, comprometendo a integridade das informações.
3. **Repúdio:** Usuários podem negar ações realizadas, dificultando a rastreabilidade e a responsabilização.
4. **Information Disclosure (Divulgação de Informações):** Exposição não autorizada de dados pessoais, seja por falhas no sistema ou ataques externos.
5. **Denial of Service (Negação de Serviço):** Ataques que visam tornar o sistema indisponível, afetando a continuidade do serviço.
6. **Elevation of Privilege (Elevação de Privilégio):** Um atacante pode obter níveis de acesso superiores aos autorizados, comprometendo a segurança dos dados.

Medidas de Mitigação

Considerando as ameaças identificadas, é preciso que sejam adotadas as seguintes medidas para garantir a proteção dos dados:

- Implementar autenticação multifator para verificar a identidade dos usuários.
- Utilizar assinaturas digitais e mecanismos de verificação de integridade para detectar alterações não autorizadas.
- Manter logs de auditoria detalhados e protegidos para rastrear as ações dos usuários.
- Classificar os dados e aplicar controles de acesso baseados em papéis, além de criptografar dados sensíveis.
- Implementar mecanismos de detecção e prevenção de intrusões, além de limitar as requisições por usuário.
- Aplicar o princípio do menor privilégio e revisar regularmente as permissões dos usuários.