

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Grupo 22

Operador: Grupo 22

Encarregado: Lucas Candido

E-mail Encarregado: grupo22@gmail.com

2. NECESSIDADE DE ELABORAR O RELATÓRIO

A elaboração deste RIPD é necessária para demonstrar a compreensão dos princípios da LGPD e a aplicação das melhores práticas de segurança da informação em um projeto de desenvolvimento de software, mesmo em um ambiente acadêmico.

3. DESCRIÇÃO DO TRATAMENTO

3.1 Natureza do Tratamento: Automatizado, em ambiente de desenvolvimento.

3.2 Escopo do Tratamento: Coleta, armazenamento, processamento e eliminação de dados pessoais de usuários simulados para fins de demonstração de um sistema de pedidos online em um restaurante.

3.3 Contexto do Tratamento: Projeto acadêmico desenvolvido na FIAP com o objetivo de aplicar conhecimentos em desenvolvimento de software e segurança da informação.

3.4 Finalidade do Tratamento: Demonstrar a viabilidade técnica e a segurança de um sistema de pedidos online, além de cumprir os requisitos do trabalho acadêmico.

4. PARTES INTERESSADAS CONSULTADAS

- Lucas Candido Pereira da Silva

5. NECESSIDADE E PROPORCIONALIDADE

O tratamento dos dados pessoais é necessário para a realização do projeto acadêmico e é proporcional às finalidades a que se destinam, sendo coletados apenas os dados estritamente necessários para a demonstração do sistema.

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

- **Riscos Identificados:** Vazamento de dados, acesso não autorizado, perda de dados, violação da integridade dos dados, indisponibilidade dos sistemas.
- **Avaliação de Riscos:**

Risco	Probabilidade	Impacto	Nível de Risco	Medidas de Mitigação	Status
Vazamento de dados dos clientes (nome, email, CPF, histórico de pedidos)	Média	Alto	Alto	Criptografia, autenticação forte, controle de acesso, backups regulares	Implementado
Acesso não autorizado aos sistemas	Baixo	Médio	Baixo	Firewalls, IDS/IPS, autenticação multifator	Implementado
Negação de serviço (DoS)	Baixo	Médio	Baixo	Monitoramento de tráfego, rate limiting	Implementado
Injeção de SQL	Médio	Alto	Médio	Validação de entrada, parâmetros preparados	Implementado
Cross-site scripting (XSS)	Médio	Médio	Médio	Saída codificada, sanitização de dados	Implementado
Ataques de força bruta	Baixo	Médio	Baixo	Limite de tentativas de login, bloqueio de IP	Implementado
Perda de dados por falha de hardware ou software	Baixo	Alto	Médio	Backups regulares, redundância de sistemas	Implementado

7. MEDIDAS PARA TRATAR OS RISCOS

- **Medidas Técnicas:** Criptografia, autenticação de dois fatores, firewalls virtuais, backups regulares.
- **Medidas Administrativas:** Políticas de segurança internas, controle de acesso aos sistemas, treinamento dos membros do grupo.

8. APROVAÇÃO

- Lucas Candido Pereira da Silva