**Levantamento de riscos, vulnerabilidades e ameaças Pick Your Driver**

**Cibersegurança e Defesa Cibernética**

São Paulo

2025

**INTEGRANTES DO PROJETO e RA’S**

Daniel Baptista Acioli Vanderlei 23025608

Fábio Oliveira Spíndola 22086131

Fabrício Cândido do Nascimento 23025273

Leonardo de Souza Mouzinho 23025627

Sumário

[1. Identificar (*Identify* - ID) 3](#_Toc192270714)

[1.1. Ativos Sensíveis 3](#_Toc192270715)

[1.2. Principais Riscos 3](#_Toc192270716)

[1.3. Principais Vulnerabilidades 3](#_Toc192270717)

[1.4. Principais Ameaças 4](#_Toc192270718)

[2. Proteger (*Protect* - PR) 5](#_Toc192270719)

[3. Detectar (*Detect* - DE) 6](#_Toc192270720)

[4. Responder (*Respond* - RS) 7](#_Toc192270721)

[5. Recuperar (*Recover* - RC) 8](#_Toc192270722)

# Identificar (*Identify* - ID)

# Ativos Sensíveis

**Dados armazenados:** Ponto de partida, destino e valor da corrida.

**APIs de terceiros:** Integrações com serviços de transporte.

**Aplicação e banco de dados:** Servidores, código-fonte e infraestrutura.

# Principais Riscos

**Exposição de dados sensíveis:** Por mais que não utilizaremos um login de usuário, a origem e o destino das corridas podem revelar padrões de deslocamento dos usuários, o que pode ser explorado indevidamente.

**Interceptação de dados:** Se os dados da corrida forem transmitidos sem criptografia adequada, um atacante pode interceptar essas informações.

**Injeção de código:** Se houver campos de entrada de dados como "endereço", a aplicação pode ser vulnerável a ataques como *SQL Injection*.

# Principais Vulnerabilidades

**Exposição indevida de informações:** Certificar que os dados armazenados não fiquem acessíveis publicamente, *endpoints* mal configurados que permitem consulta aberta de corridas armazenadas.

**APIs de terceiros:** APIs de serviços de transporte, certificar que elas sejam seguras e que esteja seguindo as diretrizes de privacidade e uso de dados.

# Principais Ameaças

**Ataques de *SQL Injection***: Se os endereços de partida/destino forem manipuláveis, um invasor pode injetar comandos maliciosos e comprometer o banco de dados.

**Ataques de Negação de Serviço (DDoS):** Um atacante pode enviar uma grande quantidade de requisições ao sistema, sobrecarregando-o e tornando-o indisponível.

# Proteger (*Protect* - PR)

1. Criptografar os dados das corridas no banco de dados;
2. Usar HTTPS/TLS para comunicação segura entre cliente e servidor;
3. Monitorar requisições e bloquear IPs suspeitos automaticamente.

# Detectar (*Detect* - DE)

1. Ativar *logs* detalhados para rastrear requisições suspeitas;
2. Criar alertas automáticos para picos de tráfego ou acessos incomuns;
3. Configurar auditorias de banco de dados para registrar alterações suspeitas.

# Responder (*Respond* - RS)

1. Criar um protocolo de emergência para lidar com ataques e vazamentos;
2. Definir quem deve ser notificado e quais ações tomar em caso de invasão;
3. Criar um plano de comunicação para usuários em caso de falha do sistema;
4. Após um ataque, revisar logs e entender como ele aconteceu;
5. Ajustar medidas de segurança para evitar recorrência.

# Recuperar (*Recover* - RC)

1. Implementar backups automáticos criptografados;
2. Garantir que os backups estejam armazenados em servidores seguros;
3. Usar servidores de backup para restaurar o serviço rapidamente;
4. Após incidentes, documentar falhas e ajustar medidas de segurança;
5. Revisar políticas regularmente para acompanhar novas ameaças.