**ComparaDrive**

* **Emilly Mickeli Depine da Silva 23025480**
* **Renan Teixeira Pinheiro 23025274**
* **Fernando José dos Santos 23025299**
* **Gustavo Henrique Santos Araújo 23025397**

**1. Identificar (Identify):**

**1.1. Ativos:**

* **Dados sensíveis do usuário histórico de viagens**

Incluem informações como histórico de viagens, preferências e padrões de deslocamento, exigindo proteção contra acessos não autorizados.

* **Informações pessoais**

Credenciais do usuário, fundamentais para a personalização do serviço e sujeitos a regulamentações de privacidade.

* **Integração com serviços de transporte (Uber e 99)**

Conexão com plataformas como Uber e 99, permitindo acesso a funcionalidades externas e exigindo medidas de segurança para troca de dados.

* **Servidores e bancos de dados**

Infraestrutura essencial para armazenar e processar informações, necessitando de segurança robusta contra-ataques e falhas.

**1.2. Possíveis Riscos:**

* **1.2.1. Acesso não autorizado aos dados**

Ocorre quando terceiros conseguem acessar informações privadas sem permissão, podendo resultar em vazamento de dados e violações de privacidade.

* **1.2.3. Vulnerabilidades dentro do código**

Falhas no desenvolvimento do software podem permitir ataques, como injeção de código ou exploração de brechas de segurança, comprometendo a integridade do sistema.

* **1.2.4. Falhas dentro do servidor**

Problemas no servidor, como instabilidades ou falta de atualizações, podem causar indisponibilidade do serviço e exposição a ataques cibernéticos.

* **1.2.5 Perca de dados**

Erros técnicos, ataques maliciosos ou falhas no backup podem levar à perda irreversível de informações, afetando a confiabilidade e continuidade do serviço.

**2. Proteger (Protect):**

* 2.1.2. Mecanismos de controle de acesso definidos com base nas funções dos usuários.
* 2.1.3. Regras para criação de senhas seguras.
* 2.1.4. Capacitação do time para proteção de possíveis ameaças digitais e hackers

**3. Detectar (Detect):**

* **3.1. Monitoramento:**
* 3.1.1. Mecanismos para identificar acessos não autorizados.
* 3.1.2. Monitoramento de logs de segurança.
* 3.1.3. Análise de comportamento do usuário.
* 3.1.4. Procedimentos para investigação e mitigação de ameaças.
* **3.2. Alertas e Notificações**
* 3.3.1. Avaliação contínua para identificar falhas de segurança no sistema.
* 3.3.2. Testes de invasão simulados para verificar a resistência do ambiente.
* 3.3.3. Uso de ferramentas automatizadas para detecção de vulnerabilidades.

**4. Responder (Respond):**

* 4.1. Elaboração de um plano estruturado para lidar com incidentes de segurança.
* 4.1.1. Atribuição clara de funções e responsabilidades durante um incidente.
* **4.2. Comunicação:**
* 4.2.1. Informar imediatamente os usuários afetados por violações de dados.
* 4.2.2. Manter comunicação com autoridades reguladoras, conforme exigido.
* **4.3. Análise Pós-incidente:**
* 4.3.1. Investigação das causas fundamentais do incidente para evitar recorrências.
* 4.3.2. Implementação de ações corretivas para melhorar a segurança do sistema.

**5. Recuperar (Recover):**

* 5.1. Desenvolvimento de estratégias para garantir a continuidade das operações após eventos inesperados.
* 5.1.1. Estabelecimento de processos de backup automáticos para minimizar a perda de dados.
* 5.1.2. Realização de simulações regulares para testar a eficácia do plano de recuperação em situações reais.
* 5.3.1. Adoção de novas práticas e tecnologias de segurança com base em avaliações pós-incidente.