**Caso 2: Canales Seguros**

**Integrantes:**

* Hugo Santiago Hernández Limas
* Alejandro Gracia Rey

**Solución**

1. **Análisis y entendimiento del problema**
2. Los paquetes que envían cada dispositivo asociado a un carro al servidor:

En caso de que alguien tenga acceso a la información que envía el dispositivo, la empresa podría perder sus clientes y empresas asociadas, lo anterior debido a la fuga de información delicada. Por otro lado, vulnera la seguridad de los conductores y paquetes transportados ya que expone las rutas, puntos de salida y paradas que se van a realizar.

Una mala gestión de los dispositivos de transporte en caso de que se modifique la información de rastreo y/o paquetes asociados al viaje.

1. **Vulnerabilidades**
   1. **Information disclausure:** La comunicación entre el dispositivo y el servidor de manejo de unidades no está protegida.
   2. **Integridad de la información:** La comunicación entre el dispositivo y el servidor de manejo de unidades no está protegida por lo que un atacante podría alterar la información que el dispositivo envía.
   3. **Spoofing:** Al no proteger el canal entre el dispositivo y el servidor de dispositivo es posible ingresar un dispositivo falso.
   4. **Denegación de servicios:** Los dispositivos al no tener un certificado digital es posible suplantarlos y realizar un ataque de denegación de servicios.
2. Soluciones propuestas
   1. **Certificado digital:** A través de un certificado digital en los dispositivos es posible evitar una suplantación y posteriormente un posible ataque de denegación de servicios.
   2. **Hashing:** A través de este método es posible asegurar la integridad de la información que envían los dispositivos con el fin de evitar una manipulación de la información en medio.