Nicolás Sanabria 201417265

Juan Camilo Marthá 201423827

1. **1.** Se deben proteger estos datos:

* Estado del vehículo: Es importante porque si alguien conoce en dónde se encuentra el vehículo, podría atentar contra él y así apropiarte de la mercancía que lleve. En caso de que alguien no autorizado pudiera modificar el estado entonces la central no podría tener datos reales y no podría actuar con prontitud en caso de emergencia.
* Rutas existentes: Es importante porque si alguien conoce la ruta del vehículo podría interceptarlo en algún punto y hacer algún tipo de perjuicio. Si alguien no autorizado modifica la ruta puede dirigir la unidad a un destino erróneo y crear retrasos, gastos, problemas con los clientes e incluso peligro para la unidad.

**2.** Vulnerabilidades:

1. Falta de encriptación de los datos al ser enviados por la red. Esta falla concedería a un tercero la interceptación de los datos y un posible spoofing.
2. Falta de comprobación de la identidad de una entidad. Esto provocaría que una fuente no autorizada pueda enviar y recibir mensajes del sistema suplantando una identidad.
3. Falta de encriptación de los datos almacenados. Esto permitiría que si un tercero accede a los datos del servidor pueda leerlos, modificarlos e incluso más problemas.
4. Los datos no son verificados al hacer el procesamiento. Esto permitiría que un interceptador de paquetes pudiera modificarlos y enviar al servidor información errónea sobre las unidades móviles.
5. Vulnerabilidad 1: Para solucionar esta vulnerabilidad se optará por un sistema de cifrado asimétrico. Se tomó la decisión de usar este cifrado porque es más seguro y evitamos el problema de *Man in the middle,* además que asumimos que la central tiene la infraestructura necesaria para soportar la verificación cada minuto de múltiples unidades. De esta manera, los datos quedarán cifrados y pueden ser enviados por la red con tranquilidad.

Vulnerabilidad 2: Para solucionar esta vulnerabilidad se usarán certificados digitales que comprueben la identidad de ambas partes y así evitar la suplantación.

Vulnerabilidad 3: Para solucionar esta vulnerabilidad se usarían algoritmos de encriptación para almacenar los datos, de tal manera que si alguien logra acceder a los datos almacenados no pueda hacer uso de ellos.

Vulnerabilidad 4: Para solucionar esta vulnerabilidad se podría usar un algoritmo de hashing de manera que se pueda comprobar la integridad de la información.