ANEXO II REQUERIMIENTOS TÉCNICOS DE LA SOLUCIÓN TELEMÁTICA

1. DISPOSITIVOS GPS CON CONEXIÓN A SISTEMA OBD Y CANBUS

Los dispositivos embarcados deberán contar con las siguientes características:

- Seguridad:
  - Las interfaces del dispositivo y de la red utilizan autenticación, cifrado y verificación de la integridad de los mensajes, conforme a lo sistemas de diagnosis normalizados según UNE-ISO 14230-1:2015.
  - Cada dispositivo utiliza un identificador único y una clave de seguridad no estática, para dificultar los intentos de suplantación de identidad del dispositivo.
  - Las actualizaciones over-the-air (OTA) emplearán un firmware con firma digital para verificar que provengan de fuentes fiables.
  - FIPS 140-2 validado por NIST (certificado #3371).
- Seguimiento de Vehículos:
  - Notificación de cualquier infracción o forma de conducción brusca no procedente, al conductor mediante alertas acústicas, mensajes de textos u otras aplicaciones de mensajería instantánea.

Cumplimiento de la normativa	FCC, ISED, PTCRB, NOM, HERO/HERF/HERP (referencias seleccionadas), CE, E-Mark, REACH, RoHS, WEEE, RCM, MIC, CITC, IMDA, KCC, NCC, NBTC, UKCA, RAMATEL, ANATEL, BTRC, NTRC, SDPPI, ARTCI, ARTEC, SIRIM, ANRT, NICTA, ARTP
Soporte over-the-air (OTA)	**Actualizaciones de firmware**: para mantenimiento, nuevas funciones y aplicaciones personalizadas **Parámetros**: para activar o desactivar funciones adicionales **Datos de almanaque/efemérides**: para una detección de GPS más rápida
Alerta acústica en cabina	**Salida de decibelios**: >85 dBA a 10 cm **Avisos al conductor**: frenado brusco, aceleración brusca, giros bruscos, exceso de revoluciones, de ralentí y de velocidad, infracciones referentes al cinturón determinadas por el motor (según disponibilidad) y avisos personalizados

	Modo de prueba: pitidos de diagnóstico para validar la conexión GPS e inalámbrica

2. SOFTWARE DE GESTIÓN DE FLOTAS

CARACTERÍSTICAS:

- Seguridad: Medidas adecuadas para evitar que cualquier dato sea leído, copiado, alterado o borrado por partes no autorizadas durante la transmisión o el transporte de cualquier dato hacia y desde el dispositivo:
  - Todos los datos, ya sean directamente desde el propio dispositivo, desde dispositivos de terceros conectados o desde el Gateway Server, están cifrados de forma segura entre el dispositivo y el Gateway Server seguro mediante AES 256º similar. Los procesos de autenticación y cifrado utilizan claves de cifrado individuales, aleatorias y evolutivas que cambian con regularidad.
  - Firmar todo el firmware del dispositivo mediante RSA 2048 o similar. Las firmas se autentican antes de permitir la actualización del firmware en el dispositivo.
  - Ni los datos de GPS ni los de motor contienen ningún nombre del conductor u otros datos confidenciales.
  - Todos los datos enviados entre el Gateway Server y la base de datos se realizan a través de una conexión TLS segura y cifrada.

- Revisiones del cumplimiento de la normativa:
  - Contar con un completo programa que garantice el cumplimiento general de la normativa aplicable a los controles operativos, a través de certificaciones tecnológicas y auditorías internas.
  - La solución está alojada totalmente en Google Cloud Platform (GCP) o similar. Por tanto, se heredan muchas de sus certificaciones, como SOC 2 e ISO 27001.

- Informe SOC 2 de Google a disposición de los clientes, bajo acuerdo de confidencialidad.
- Certificación FIPS 140-2 número 3371.
- Certificación completa FedRAMP PMO Authority To Operate (ATO).
- Certificación ISO 27001.
- Cada una de las certificaciones anteriores requiere documentación y demostración de los controles adecuados para apoyar la concesión y la certificación continua.

- Recuperación de datos en caso de fallo o pérdida:
  - Realizar copias de seguridad de todos los datos alojados en la plataforma a diario, los 365 días del año.
  - Todas las copias de seguridad se confirman, verifican y trasladan a una ubicación física independiente para su almacenamiento.
  - Todos los datos de los que se ha realizado una copia de seguridad están protegidos y su acceso está limitado a empleados específicos y autorizados.
  - Los datos de los que se ha realizado una copia de seguridad se almacenan durante un máximo de 365 días antes de purgarlos.
  - Toda la infraestructura de copia de seguridad cuenta con una redundancia adecuada en caso de fallos de hardware.
  - Todos los datos de los que se realiza una copia de seguridad se almacenan completamente cifrados mediante tecnologías de cifrado de nivel empresarial.
  - Los clientes pueden eliminar los datos almacenados en los sistemas. Se puede pedir ayuda con la exportación y eliminación de los datos a través de un acuerdo de consultoría con tarificación por hora de servicio. Solo se iniciará una purga de datos cuando sea necesario preservar la integridad, fiabilidad y disponibilidad de la plataforma (SaaS). Si se realiza una purga, se conservarán los datos con un mínimo de 365 días antes de la fecha de purga y notificará con antelación a los propietarios de la base de datos. Si se va a realizar una purga de los datos y desea conservarlos durante más de un año,

se pueden recuperar los datos deseados mediante una de las herramientas API que se ofrecen.

- Residencia de los datos:
  - Los datos del cliente se almacenan en los siguientes medios:
    - El dispositivo del vehículo.
    - El ordenador del cliente.
    - Un servidor gestionado por el proveedor (los datos del cliente se separarán por medios lógicos y virtuales).
    - Los datos de clientes se almacenan en los centros de datos europeos.